SIAS 2015

8th INTERNATIONAL CONFERENCE
ON THE SAFETY OF INDUSTRIAL
AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

8th International Conference Safety of Industrial Automated Systems – SIAS 2015

18-20 November 2015
Königswinter, Germany

– Proceedings –

Published by: Deutsche Gesetzliche Unfallversicherung (DGUV)
Glinkastr. 40
10117 Berlin
Germany
Phone: ++49 30 288763800
Fax: ++49 30 288763808
Internet: www.dguv.de
Email: info@dguv.de

– December 2015 –

ISBN: 978-3-86423-163-6

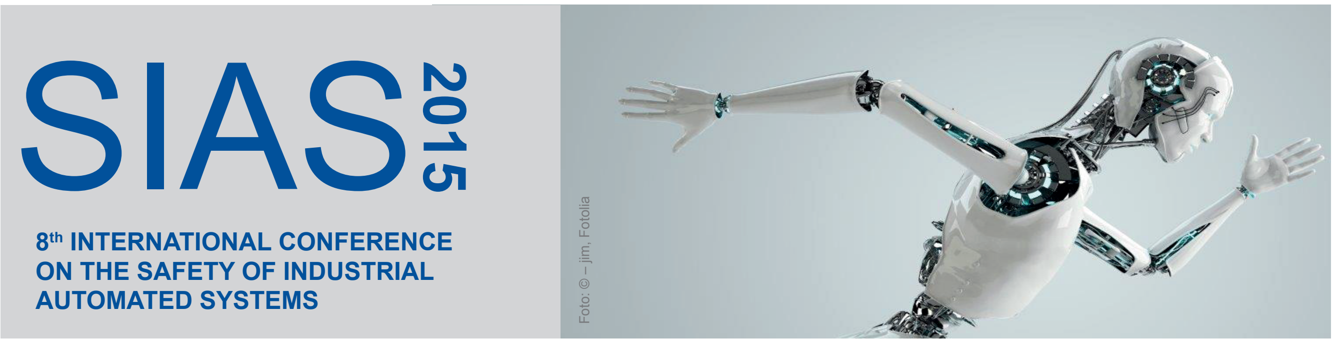

SIAS 2015
8th INTERNATIONAL CONFERENCE ON THE SAFETY OF INDUSTRIAL AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

8th International Conference Safety of Industrial Automated Systems – SIAS 2015

– Proceedings –

Content

Scientific committee

Jean-Christophe Blaise	Institut National de Recherche et de Sécurité (INRS), France
Thomas Bömer	Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Germany
Yuvin Chinniah	École Polytechnique de Montréal, Canada
Marek Dźwiarek	Central Institute for Labour Protection – National Research Institute (CIOP-PIB), Poland
Elie Fadier	Institut National de Recherche et de Sécurité (INRS), France
Michael Huelke	Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Germany
Hiroyasu Ikeda	National Institute of Occupational Safety and Health (JNIOSH), Japan
Timo Malm	Technical Research Centre of Finland (VTT), Finland
Steven Shaw	Health & Safety Executive (HSE), United Kingdom
Denis Turcot	Institut de recherche Robert-Sauvé en santé et en sécurité du Travail (IRSST), Canada

Programme

Wednesday, 18th November 2015

Start	Title, Chair/Speaker
09:00	Registration with coffee
10:15	Opening words *Dietmar Reinert, IFA, Germany*
10:30	Keynote: Human-robot collaboration over the years *Thomas Pilz, Pilz GmbH & Co. KG, Germany*

Session 1: Innovation and the future
chair: Marek Dzwiarek, CIOP-PIB, Poland; Michael Huelke, IFA, Germany

11:15	Upcoming technologies and fundamentals for safeguarding all forms of human-robot collaboration *Roland Behrens, Fraunhofer IFF, Germany*
11:40	Challenges and new ways for the risk assessment of cyber physical systems *Johannes Schubert, AUVA, Austria*
12:05	Functional safety application for collaboration work of machines and persons on the basis of safety levels defined by position and velocity vectors *Yukio Hata, Nagaoka University of Technology, Japan*
12:30	Lunch break
13:30	Application of ICT to smart personal protective equipment for safety management in the working environment *Grzegorz Owczarek, CIOP-PIB, Poland*
13:55	A study of main safety-related functions available to collaborative robotics *Adel Sghaier, INRS, France*

Session 2: Functional safety
chair: Steven Shaw, HSE, United Kingdom; Thomas Bömer, IFA, Germany

14:20	PLCopen: contributing to a safer world via harmonized look and feel of safety finctionalities *Eelco van der Wal, PL Copen, The Netherlands*
14:45	Coffee break
15:10	Relation between functional safety and IT-security on practice: Roosevelt Island *Bernard Mysliwiec, Siemens AG, Germany*
15:40	IFA Matrix Method for development of safety related application software *Michael Huelke, IFA, Germany*
16:05	Security for fail-safe communication in automation *Felix Wieczorek, Beckhoff Automation, Germany*
16:30	Development model for distributed safety function in mobile work machinery site *Ari Ronkainen, Natural Resources Institute, Finland*
17:00	End of day

Thursday, 19th November 2015

Session 3: Risk assessment
chair: Yuvin Chinniah, École Polytechnique de Montréal, Canada; Denis Turcot, IRSST, Canada

09:00	Preventing vehicle-pedestrian collisions: the place of detection systems *Pascal Lamy, INRS, France*

Start	Title, Chair/Speaker
09:25	From risk to requirements – a round robin test *Timo Malm, VTT, Finland*
09:50	Analysis of two risk estimation tools applied to safety of machinery *François Gauthier, IRSST, Canada*
10:15	Ergonomics – A methodology for work analysis to support design (prEN 16710:2015) *Elie Fadier, INRS, France*
10:40	Coffee break
11:10	Keynote: Regulated safety or managed safety *Jean Pariès, DEDALE, France*

Session 4: Safety-related control systems
chair: Hiroyasu Ikeda, JNIOSH, Japan, Steven Shaw, HSE, United Kongdom

11:55	Functional Decomposition from IEC 62061 – How to determine individual safety functions. From requirement to implementation *Derek Jones, Rockwell Automation, United Kingdom*
12:20	Research and consideration of electromagnetic noise immunity of programmable electronic system and common cause failure of safety-related programmable electronic system *Tsuyoshi Toeda, Fuji Electric Co., Ltd., Japan*
12:45	Lunch break
13:45	Improvement of ISO 13849-1 as a result of practical feedback: amendment 1 (2016) *Klaus-Dieter Becker, BG ETEM, Germany*
14:10	Servomotors and power drive systems – Key elements for the safe design of a servopress *Jean-Christophe Blaise, INRS, France*
	The following manuscript was submitted but not presented orally Optimal safety devices in safety-related control systems for low to middle risk applications *Ikuo Maeda, IDEC CORPORATION, Japan*
14:35	Poster session and product exhibition

Session 5: Protective devices and systems
chair: Jean-Christophe Blaise, INRS, France; Thomas Bömer, IFA, Germany

15:55	Optical sensors for person detection – Outdoor use *Martin Wüstefeld, Sick AG, Germany*
16:20	NIR camera based person detection in the working range of industrial robots *Sebastian Sporrer, Bonn-Rhein-Sieg University of Applied Sciences, Germany*
16:45	End of day
19:00	Conference dinner

Friday, 20th November 2015

Session 5: Protective devices and systems
chair: Jean-Christophe Blaise, INRS, France; Thomas Bömer, IFA, Germany

09:00	Real Time Location Systems for monitoring safety of the machine operators *Marek Dzwiarek, CIOP-PIB, Poland*
09:25	Adaptive, material-dependent height-control for protective hoods on panel saws *Norbert Jung, Bonn-Rhein-Sieg University of Applied Sciences, Germany*
09:50	Study on appropriate positioning of emergency stop devices equipped in robot work system *Hiroyasu Ikeda, JNIOSH, Japan*

Start	Title, Chair/Speaker
	Session 6: Practical applications/experiences *chair: Elie Fadier, INRS, France; Timo Malm, VTT, Finland*
10:15	Causes of fatal and serious accidents involving machinery in Quebec *Yuvin Chinniah, École Polytechnique de Québec, Canada*
10:40	Coffee break
11:10	The „Feedback method“, a tool to better understand the real work activities with the contribution of end users of machinery *Fabio Strambi, A. USL 7 Siena, Italy*
11:35	Protective devices with 3D detection zones on machinery: investigations on bypassing safety devices by crawling *Michael Hauke, IFA, Germany*
12:00	Current situation of safety assessor and safety basic assessors (SA/SBA) qualification system: Reduction of accidents achieved by a Japanese company and recommendation by Japanese Ministry of Health, Labour and Welfare *Toshihiro Fujita, NECA, Japan*
12:25	Closing *Dietmar Reinert, IFA, Germany*
12:30	Lunch break
13:30	Technical Tour to IFA (Bus transfer from Maritim Hotel to IFA)
17:00	Return to Maritim Hotel

Poster session

Isolation of energies: Establishing Safe Work Conditions
Jean-Christophe Blaise, Sandrine Hardy, INRS, France

Start up Safety Assessor Qualification to Educate Safety Engineers in Thailand
Patiphon Koompai, Technology Promotion Association, Thailand; Hiroo Kanamaru, Nippon Electric Control Equipment Industries Association, Japan

Camera-Monitor-Systems in Excavators – Using Eye-Tracking to Assess Utilization and Design
Markus Koppenborg, Birgit Naber, Andy Lungfiel, Michael Huelke, IFA, Germany

A Study of a Special Safety-Confirmation Type Washer That Can Detect the Looseness of Tightened Bolts by Way of Leverage-Exerted Displacement Enlargement
Masanobu Chiba, Mizuho Nakamura, Hiroyuki Sasagawa, Polytechnic University, Japan;
Tetuo Sujino, Noboru Sugimoto, School of Science and Engineering, Meiji University, Japan

Setting-up a Virtual Reality Simulation for Improving OSH in Standardisation of River Locks
Peter Nickel, IFA, Germany; Rolf Kergel, UVB, Germany; Thilo Wachholz, Eugen Pröger, Federal Waterways and Shipping Administration, Germany; Andy Lungfiel, IFA, Germany

A Study of Safeguarding Based on Human Body Communication Technology
Kohei Okabe, JNIOSH, Japan

Risk reduction effect of a supporting protective system for an integrated manufacturing system
Shoken Shimizu, Shigeo Umezaki, JNIOSH, Japan

Evolution of the SIAS conference from 1999 to 2012
Denis Turcot, IRSST, Canada; Yuvin Chinniah, École Polytechnique de Montréal, Canada

Investigation of evaluation method for strength of artificial bones by using Finite Element Analysis
Atsushi Yamaguchi, Kohei Okabe, Hiroyasu Ikeda, JNIOSH, Japan

SIAS 2015

8th INTERNATIONAL CONFERENCE
ON THE SAFETY OF INDUSTRIAL
AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

Keynotes

From vision to reality – Human-robot collaboration over the years

Thomas Pilz, Managing Partner Pilz GmbH & Co. KG

Abstract

The classic way to achieve safety in industry is to equip machinery with various safeguards, thus protecting people in the vicinity of potential hazards. Today, many applications that use robots have a very high level of automation. In principle, human intervention in the production process is undesirable. To guarantee safety and availability in such applications, plant and machinery are surrounded by mechanical, physical guards.

In addition to classic, fully enclosed robot cells, there is now an increasing demand for human-robot collaborations (HRC), which can operate without guards where possible. In terms of safety, however, the seemingly unlimited possibilities for HRC applications mean completely new challenges for the safety-related assessment and the technologies employed. The demands on safety technology always depends on the respective application.

The desire for Human Robot Collaboration however is as old as civilization beginning in Ancient Egypt ending today with an increasing number of desirable human-robot collaboration applications in the manufacturing industry. The ability to realize them will depend heavily on innovations in the sensor technology and robotics environment. The first promising step in this regard is to combine intelligent, inter-connected sensors with the control systems that enable the necessary dynamic work processes. Where this path may lead is shown in today’s science fiction movies.

The fascination: Robots – The machine as man's friend

No machine fires man's imagination as much as robots. They are seen to perfect machinery, based on greater degrees of freedom in view of the diversity and scope of their activities. Ultimately, robots symbolise man's quest for machines that participate in human life and help in any situation.

Even in Ancient Egypt and antiquity, human statues and figures were fitted with mechanics. This was mainly to deceive people or to impress, in temples for example. In the centuries that followed and until the Middle Ages, the engineers of the time were especially busy with clocks and glockenspiels with moving figures. Later on the focus shifted to military equipment. In modern times and with the start of the industrial revolution, the economic potential of automated machines and robots was recognised. They were to help people carry out their work, so laying the foundation for the industrial revolution. The first loom controlled automatically using punched cards was built by Joseph-Marie Jacquard in 1801.

People always saw more in robots than just the technical aspect of a machine. At the end of the 18th century, the "Mechanical Turk" was already attracting the world's attention: onlookers had the impression that this machine was playing chess autonomously. In reality, however, there were people inside the machine. Emerging science fiction literature with authors such as Jules Verne continued to inspire the vision of autonomous machinery at the end of the 19th century.

The history: The robot in the 20th century

The actual term "robot" was coined in the 20th century. It comes from the Czech term "Robota", which means forced or compulsory labour. In 1921 the Czech author Karel Čapek published a play about a company that makes artificial people. This was the first time that the term "robot" was used in conjunction with machinery.

This initiated an increasingly critical debate about autonomous machines. The key question was: how can the safety of man and machine be guaranteed when man and machine interact in close proximity? In a short story in 1942, the Russian-American scientist and science fiction author Isaac Asimov described the ground rules for robots as the "Laws of Robotics". These were as follows: 1. A robot may not injure a human, 2. A robot must obey, 3. A robot must protect its own existence (provided this doesn't conflict with law 1 or 2).

The reality: Robots in an industrial environment

Industrial robots are an invention from the second half of the 20th century. The American George Devol heralded this era in the 50s with his patent draft for "programmed article transfer". A robot was used at General Motors for the first time in 1961 with Unimate.

Man and machine were kept strictly separate, to guarantee that workers were protected. The robot was intended to replace manpower and was enclosed in a cell to perform its function. Separate work areas and no direct interaction between man and machine: these principles remained the same for over 50 years. These robot applications failed to meet expectations that man and robot would work closely together. In contrast, science fiction films and series since the 60s have shown this as reality, even the norm. What would Star Wars be without R2D2 and C3PO? Transformer, Terminator, Short Circuit, Irobot, … leave factory planners dreaming of the "friendly robot"

Man's quest for machines that surround him and assist in every situation has now reached the world of standardisation and has obtained its normative framework in the Technical Specification ISO/TS 15066 "Robots and Robotic Devices - Collaborative industrial robots".

The mission: "Get the robot out from behind the safety fence!"

Today, productivity increases and demographic changes with an increasingly older workforce provide the impetus for raising the potential of robot applications. The wish is for man and machine to share a workspace. But always under the premise that the laws of robotics apply.

The key question for human robot collaboration is the same as it was for Asimov: "How can safety be guaranteed?". And this applies for all types of robots, particularly industrial robots with high payload.

The conditions for this are more reliable control systems and intelligent, dynamic sensors, as well as normative foundations. Sensor technology in particular is as yet unable to offer adequate solutions to meet the first law of robotics. That's why the robots familiar from research and science fiction have failed up to now to make a rapid transition to the factory floor. Instead of co-operating with static, permanently defined transfer points between man and machine, in future both partners are to collaborate, flexibly using their respective strengths within a shared workspace.

The basic principles: ISO/TS15066 Collaborative robots

In order to find solutions, the international standards committee ISO/TC 184/SC2 WG3 was commissioned with developing the technical specification ISO/TS 15066 "Robots and Robotic Devices - Collaborative industrial robots". As a member of this international standards committee, Pilz is actively working to shape the specification. The current draft sets out solutions for safe human robot collaboration within an industrial environment. This new standard is groundbreaking and pioneering for human machine collaboration in an industrial environment.

One of the most important points en route to a safe robot application is the production of a risk analysis in accordance with EN ISO 12100. The contents of the risk analysis includes identification of the applicable harmonised standards and regulations, determination of the machine's limits, identification of all the hazards in each of the machine's life phases, the actual risk estimation and assessment, plus the recommended approach for reducing risk. The challenge for the "risk assessment" on robot applications is that the boundaries of the two work areas of man and machine are broken down. The human's movements must be considered in addition to the risks emanating from the robot. However, these cannot always be calculated with a view to speed, reflexes or the sudden approach of additional persons.

The risk analysis is the basis for the subsequent "safety concept" and "safety design", including selection of components. Based on the results from the "risk analysis" and "safety concept", the selected safety measures are documented in the risk assessment and implemented in the "system integration". This is followed by the "validation", in which we take another look at the steps taken previously.

To guarantee the safety of human robot collaborations (HRC) in practice, four different concepts are provided for the system design in accordance with EN ISO 20118-1. These can either be used alone or in combination.

- Safety-rated monitored stop
- Hand guiding
- Speed and separation monitoring
- Power and force limiting

Generally users will opt for safety-rated monitored stop and power and force limiting, or a combination of the two.

The implementation of human robot collaborations in an industrial environment will definitely increase, but their growth will depend heavily on innovations in the sensor technology and robotics environment. The first promising step in this regard is to combine intelligent, inter-connected sensors with the control systems that enable the necessary dynamic work processes in the first place.

Outlook: From vision to reality

In addition to classic, fully enclosed robot cells, there is now an increasing demand for human robot collaborations, which can operate without guards where possible. In terms of safety, however, the seemingly unlimited possibilities for HRC applications mean completely new challenges for the safety-related assessment and the technologies employed. The demands on safety technology always depend on the respective application.

In practice, each application requires its own safety-related assessment. Together, automation specialists, robot manufacturers, integrators and notified bodies such as BG can turn the vision of robot colleagues into reality, step by step, application by application.

Jean Pariès, DEDALE, Paris/France

Regulated safety or managed safety

In terms of safety management, the nemesis intuitively seems to be randomness, and especially the unpredictability of human behaviour. Hence in the currently dominant safety paradigm, safety is seen as the result of a strict enforcement of all rules and procedures. But in most current industrial processes, a total adherence to detailed pre-established action guidelines is both unattainable, incompatible with a reasonable efficiency, and insufficient to keep control under abnormal situations. Further efforts to make the predetermination of behaviours both more extensive and more intensive mainly increase the complexity of the system and the opportunities for deviations, hence the need for more efforts. As a matter of fact, both safety and performance also require human expertise and intelligence, individual and collective capacities to make sense and decisions, even at the operation front line. This implies some degree of autonomy for front line operators, and challenges organizations in their capacity to properly generate and master this autonomy. As it is for the musicians of a symphonic orchestra, the challenge is to nurture the subtle variety of individual rhythms and musical colour needed for a sound interpretation, while reducing the variations that reflect a lack of control and produce false notes. And this challenge not only concerns the design and philosophy of rules and procedures, but also the design of the system itself, the nature of the needed expertise, the design of feedback and learning loops.

SIAS 2015

8th INTERNATIONAL CONFERENCE
ON THE SAFETY OF INDUSTRIAL
AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

Session 1:
Innovation and the future

Upcoming Technologies and Fundamentals for Safeguarding All Forms of Human-Robot Collaboration

Roland Behrens, José Saenz, Christian Vogel, Norbert Elkmann[a]

[a]*Fraunhofer IFF, Magdeburg, Germany*

Abstract

New sensors and robot technologies enable different degrees of human-robot collaboration, ranging from fenceless coexistence to close collaboration. The first part of the paper will introduce different forms of co-work and how they can be characterized using three essential characteristics. Then for each form of co-work, the safeguarding modes from the ISO/TS 15066 which are applicable and make sense will be determined. The second part gives an overview of sensor technologies which can be used for the four safeguarding modes in compliance with the current standards. This overview focuses on recent sensor technologies developed by the authors.

Keywords:

Human-robot collaboration; taxonomy; sensor technologies; biomechanical limit values

Introduction

Human-robot collaboration is a potentially disruptive technology which could be harnessed to counteract social and business challenges such as demographics and an aging workforce. The potential lies in the combination of robot's strength and performance with human dexterity, experience, and cognitive abilities on the shop floor. This will help maintain the physical well-being of human workers and improve productivity, competitiveness especially when manufacturing volatile and highly personalized products with decreasing life cycles.

New sensor and robot technologies enable close human-robot cooperation, ranging from a fenceless coexistence to close collaboration, where humans work hand in hand with robots. The upcoming ISO/TS 15066 will specify the following safeguarding modes for collaborative operation to minimize the risk the human co-worker can be harmed by specific hazards arising from the coworking robot or to eliminate general hazards: [1]

- *Safety-Rated Monitored Stop* – The robot is stopped when a human enters the shared workspace.
- *Speed and Separation Monitoring* – The human and robot are working simultaneously in the shared workspace. Risk reduction is achieved by maintaining a minimum separation distance between human and robot. The robot must stop immediately if the separation distance falls below its minimum value.
- *Power and Force Limiting* – Physical contact between robot and human is allowed. Risk reduction is achieved through complying with biomechanical limit values (force and pressure).
- *Hand-Guiding* – Motion commands given by the human are directly transformed into robot motion. Risk reduction is achieved through an appropriate workplace design, speed limitation and complying biomechanical limit values.

From our perspective we see two reasons why the application of ISO/TS 15066 may be challenging when it is officially available at the end of 2015:

1. The specified safeguarding modes may lead to the assumption that there are only four ways in which a human can work together with a robot.
2. The specifications lack comprehensive information about how particular safeguarding modes can be applied properly. This pertains especially to certain fundamental prerequisites such as limit values and sensor technologies which are currently not available.

Regarding challenge 1: In the following chapter we will show that almost each safeguarding mode of ISO/TS 15066 can be applied for more than one form of cowork. For this purpose a consistent taxonomy will be presented that allows users to determine the exact form of co-work, which can then be used to select an appropriate safeguarding mode depending on the available operational conditions.

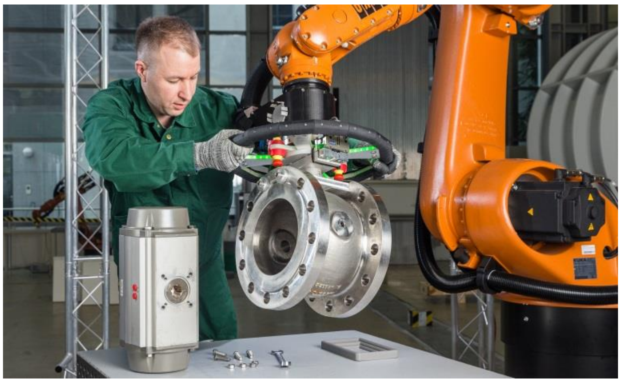


Figure 1: Collaborative scenario (valve assembly)

Regarding challenge 2: We are currently working on different technologies that can be used to implement certain safeguarding modes to their full extent. These technologies range from a projection based monitoring system to tactile sensors, which can be easily applied to any arbitrary industrial robot. Furthermore, we will present two unique studies which focus on the determination of verified limit values for the mode “Power and Force Limiting”. Both will be presented in the third chapter.

The introduced taxonomy, presented technologies and studies will be briefly discussed in the fourth chapter. We conclude our work in the last chapter.

Forms of Co-Work

From a physical perspective, all forms of collaborative operation can be described by three essential characteristics, which will be introduced in the first section of this chapter. Based on these characteristics, a taxonomy consisting of different forms of co-work in context of human-robot collaboration will then be developed. Finally, we will show how the taxonomy can be combined with the safeguarding modes of ISO/TS 15066.

Essential Characteristics

We identified three essential characteristics of collaborative workcells that build upon each other:

Shared Workspace

The human co-worker is intended to carry out a certain task in at least a limited part of the robot workspace. This implies that the workspace is shared by both robot and human. It is important to note that this characteristic describes only a spatial arrangement of both agents (robot and human) and does not consider any time-related conditions.

Simultaneous Co-Work

The human co-worker is intended to carry out a certain task within the shared workspace while the robot is moving to complete its task. It is important to note that robot and human are working separately so that physical contact is not required. In this case, physical contact is considered as an incident with possibly hazardous consequences and should be avoided. As a consequence of this, the space in which the robot is currently moving must be guarded against violation by the human co-work.

Please note that the first characteristic (shared workspace) must be available to realize simultaneous co-work. There cannot be simultaneous co-work without a shared workspace.

Physical Contact

The human co-worker is intended to work hand in hand with the moving robot. Physical contact between both agents is possible and even necessary to complete the common task. As a consequence of this, there is no restricted space in the region where physical contact cannot occur.

The first and second characteristics therefore must be positive to have the characteristic of physical contact.

Determining Forms of Co-Work

Currently the terms coexistence, cooperation and collaboration are widely-used in the robotic community to refer to a case in which a human and a robot are working together in a fenceless environment. In particular, the term “collaboration” is frequently used in combination with a co-working robot. In principle each term has a specific meaning that refers to certain characteristics. Therefore it is highly recommended, especially in a technical setting, to use these terms in a consistent fashion so that misunderstandings and confusion can be avoided. Based on the essential characteristics introduced in the previous section, we can define four forms of co-work as a variation of [2] using [3].

Coexistence

= The state or condition of existing together or at the same time

In a manufacturing context we interpret coexistence as the completion of independent tasks in separate workspaces which are not overlapping. Example: The human is working at a workplace that is close to a workplace of a robot. There is no physical overlapping between both workplaces that due to appropriate distances or separating structures (fences). Actually human-robot coexistence is currently available in most factories with industrial robots.

Sequential Cooperation

= The state or condition of having shared efforts and acting together <u>successively</u>

In a manufacturing context it refers to sequential actions to complete a common task. Example: Robot and human are working successively on the same workpiece in a sequential order. Meaning while the human is working the robot is stopped and while the robot is working the human is not in the shared workspace.

Parallel Cooperation

= The state or condition of having shared efforts and acting <u>simultaneously</u>

In a manufacturing context it refers to simultaneous actions to complete a common task. Example: Robot and human are working simultaneously on the same workpiece within the shared workspace while physical contact between both is not intended or allowed. Physical contact is explicitly excluded.

Collaboration

= The state or condition of acting jointly together to complete something

In a manufacturing context collaboration is the closest form of cooperation and refers to joint actions to complete a common task at the same time. Example: Human and robot are working directly together, hand in hand. Physical contact is needed and therefore included.

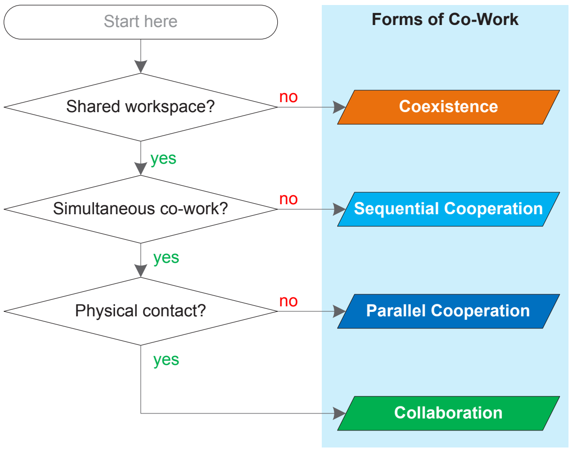


Figure 2: Flowchart to determine the form of co-work

Summary

Since the essential characteristics build upon each other a flowchart can be used to illustrate the introduced forms of co-work and their connection to the characteristics (see Figure 2). It can be used to derive the exact form by going stepwise through the intuitive chart.

Assignment of Safeguarding Modes

We can now extend the flowchart from Figure 2 to a further layer that assigns all possible safeguarding modes depending on the form of co-work. The extension is shown in Figure 3.

As illustrated in Figure 3 the form “Coexistence” can be safeguarded with all modes of ISO/TS 15066 except “Hand-Guiding”. Even separating guards like fences are appropriate, which is why this kind of protection measure was also assigned. All modes can be used without any restrictions as long as surrounding humans are protected against hazardous incidents. For “Sequential Cooperation” we cannot apply separating guards since unobstructed access for humans to the shared workspace is necessary to complete the respective task properly. “Parallel Cooperation” implies the presence of the human within the shared workspace while the robot is working. Then, the safeguarding mode “Safety-rated monitored stop” cannot be applied since this will consequently lead to a stopped robot. Finally, the form “Collaboration” can only be applied if physical contact between robot and human is possible. Depending on the task it must be decided if “Power and Force Limiting” or “Hand-Guiding” is the appropriate safeguarding mode.

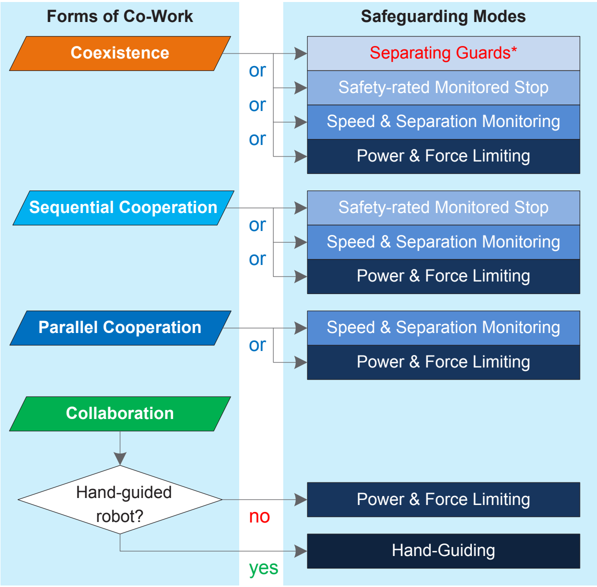


Figure 3: Types of safeguarding modes depending on the form of co-work (not covered by ISO/TS 15066)*

The question “Which of the possible safeguarding modes makes the most sense?” cannot be answered per se. This depends on the specific needs of the end-user. Basically we see that applying “Power and Force Limiting” for a robot is the only safeguarding mode which allows the user to switch between the different forms of co-work, so that the flexible use of the robot in a rapidly changing production is always possible.

Final remark

From our perspective, the presented taxonomy may also help to clarify the meaning of the terms which are frequently used to refer to a collaborative scenario. We have seen quite a bit of confusion surrounding the terms “coexistence”, “cooperation” and “collaboration” when talking about robotics applications within the robotics community and with end-users. Our taxonomy is a good starting point to put the terms in a consistent order and to combine them with the safeguarding modes of ISO/TS 15066.

Upcoming Technologies and Fundamentals

The safeguarding modes of ISO/TS 10566 presume sensor technologies and limit values which are currently not available. In this chapter we address this issue and introduce a couple of upcoming technologies which are specifically tailored to the needs and potentials of certain safeguarding modes. Furthermore, we will present two studies that are focusing on the determination of verified limit values for the mode “Power and Force Limiting”.

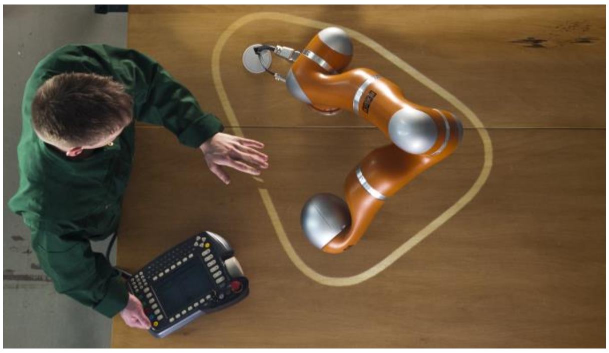


Figure 4: Workspace monitoring with a projection system

Technologies

From our perspective, the currently available sensors cannot take full advantage of certain safeguarding modes and their potentials. In the following sections, we will address three safeguarding modes and present applicable sensor technologies we are currently working on.

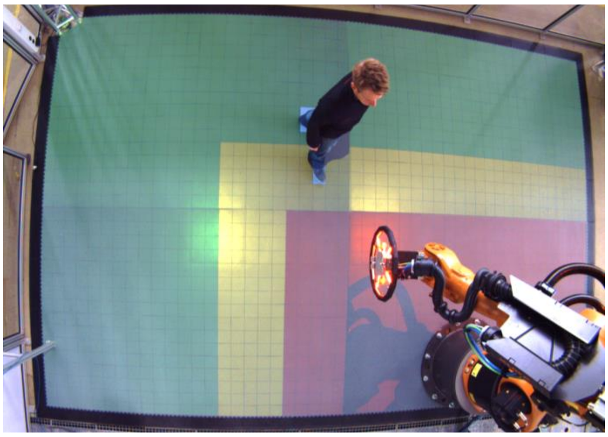


Figure 5: Tactile floor with spatial resolution combined with projectors to display safety zones (view from the ceiling)

Speed and Separation Monitoring

According to ISO/TS 15066 the distance between human and robot must be greater than a certain minimum value otherwise the robot must be stopped. The minimum distance depends on a couple of parameters such as the robot speed, its stopping distance, the moving speed of the human, etc. The ISO/TS 15066 provides an equation to calculate the required distance in real-time. [1] Up to now there are no sensor technologies commercially available which are capable of detecting an overstepping of the minimum distance value as given by the mentioned equation. Currently available sensors like laser scanners lead to safety zones with dimensions that typically exceed the minimum distance value, thereby wasting valuable space around the robot. We recently developed two sensor systems which are capable of establishing and monitoring the required distance stipulated by ISO/TS 15066.

The first system is a combination of a projector and cameras mounted above the collaborative robot. The projector is used to establish a visible area around the robot that satisfies the distance equation of ISO/TS 15066. The area dimensions are adjusted to the robot posture and its moving velocity using state variables (joint positions and speeds) extracted from the control unit. The projected area around the robot is continuously monitored by the cameras. Any violation of the minimum separation distance will cause a shadow in the projected safety zone around the robot and can be easily detected by image processing, which compares the expected image as projected with the actual camera image. Once a violation has been detected, the robot will be stopped immediately. In principle the system allows for adjusting the visible area in exact accordance to the mentioned distance equation. Since the functional principle is based on the projection of visible light, the safety zone is also visible to the human co-worker so that unintended violations of the safeguarded space can be avoided with a high probability. The projection system in a demo scenario is shown by Figure 4. [4-6]

The second sensor consists of industrial floor mats which are provided with a sensitive sub-layer made of tactile cells. The tactile floor can monitor the movement of any person and can be used to establish safety zones around a robot. These safety zones can be easily adjusted in correlation with the robot position and speed according to the distance equation of ISO/TS 15066. The resolution of the tactile floor is such that the averaged foot size of a full-grown person activated two taxels simultaneously. Multiple persons can be monitored at the same time. The tactile floor can be combined with a projection system to make the safety zones visible. This combination is currently tested in the ECHORD++ experiment called SAPARO. An image of a recent demo scenario is shown by Figure 5.

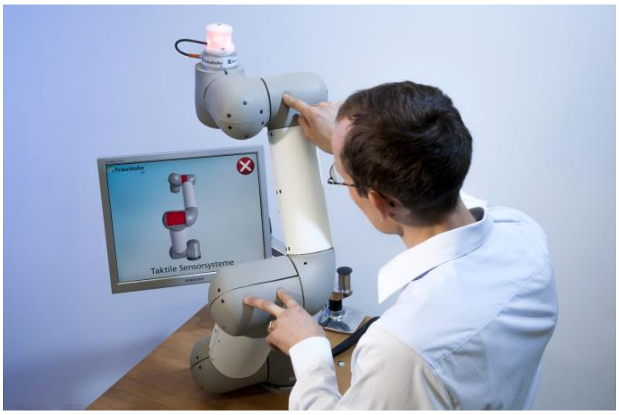


Figure 6: Robot manipulator covered by tactile sensors

Power and Force Limiting

This kind of safeguarding mode is actually in the main focus of almost all robot manufacturers. Force or torque sensors and control techniques are used to realize robots with a sensitive behavior that allows for detecting unintended contact with humans such as a collision. A summary of the commercially available robots with these features can be found in [7].

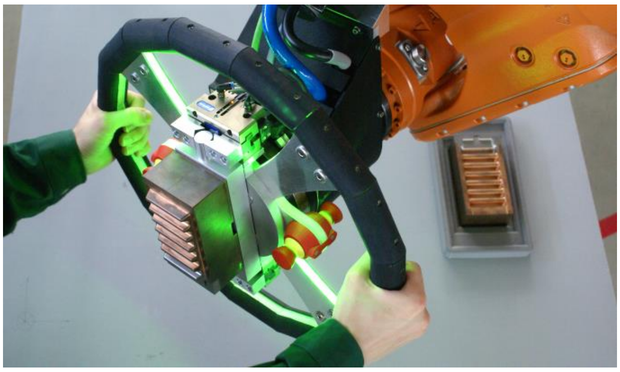


Figure 7: Hand-guiding device with integrated tactile dead-man switch for an unobstructed view of the tool

We propose a different sensor technology that can even be applied to large industrial robots to achieve sensitive behavior. The recently developed sensor is based on the same technology used in the tactile floor. A robot covered with tactile skin can detect any physical contact with the robot and can therefore be used for collision detection. Once an unintended contact has been detected, the robot immediately initiates a safety stop. The shape and material of the sensor can be mounted on or retrofitted to any kind of robot. The sensitive cells are covered with a soft cushioning layer to achieve additional dampening behavior in case of a collision. Through appropriate design of the sensor cushioning, the sensitivity, and the limitation of the robot speed, the robot outfitted with tactile sensors can be made to comply with biomechanical limit values. A standard robot covered with our tactile sensor is shown in Figure 6. [8-11]

Hand-Guiding

The usual way to apply hand-guiding is using a force-torque sensing hand device mounted adjacent to the robot tool. Robots with integrated joint sensors can also be used for hand-guiding when transforming the external forces induced by the operator to robot motions. However, such robots are usually designed to handle smaller payloads in the region of 10kg. [7]

From our perspective a typical hand-guiding device for larger robot in form of a joystick is not appropriate especially when the view of the tool and workpiece must be unobstructed at all times as stated by the ISO/TS 15066. Since a joystick is usually attached at a single location, the view may be hindered by obstacles in certain joint configurations. Furthermore, in our experience we have found that pressing the dead-man switch and moving the robot at the same time is challenging. For this purpose we developed a novel guiding device in a shape of a wheel that can be reached and activated from all sides of the robot. The wheel is mechanically attached to a force-torque sensor that is further mounted onto the tool flange. The outer ring of the wheel is equipped with tactile sensor cells, which function as a dead-man switch. A strong or weak grip of the tactile sensors will not activate the hand-guiding mode. Furthermore, motion can only be initiated if the wheel is gripped at two separate points to ensure both hands of the operator are on the dead-man switch. The guiding device is shown in Figure 7.

Limit Values

The first edition of ISO/TS 15066 will provide verified limit values which must be satisfied by a collaborative robot in safeguarding mode “Power and Force Limiting”. Unfortunately these limit values can only be applied for quasi-static contacts in form of clamping or squeezing. The term quasi-static is used since the robot speed is very low in order to avoid any serious injury to the human. Basically in a collaborative scenario we must take a second contact case into account, namely dynamic contacts like collisions.

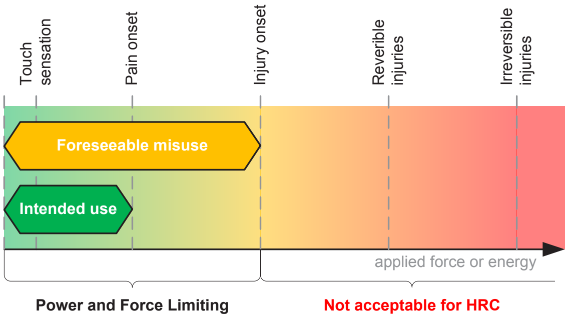


Figure 8: Acceptable severity levels for unintended human-robot contacts [1]

Up to now there are no limit values officially available for this kind of contact, although collisions must be considered as the most frequently occurring case, especially since the possibility of avoidance is significantly lower as it will be for clamping or squeezing.

Furthermore the limit values which will appear in the ISO/TS 15066 will only be applicable for the intended use case. Complementary limit values for unintended contact due to foreseeable misuse currently missing. The maximum allowable consequences due to such contacts are limited to the onset of injury as illustrated in Figure 8. [1] Please note that even slight injuries like bruises or swellings are not allowed since these slight tissue damages are considered to be onset of injury. [12-14]

Limit Values for Pain Onset

The limit values for the onset of pain during quasi-static contacts (clamping and squeezing during intended use) were determined by the University Medical Center of the Johannes Gutenberg University Mainz (JGU Mainz) in a study that was initiated and funded by the German employers' liability insurance association (Expert Committee Woodworking and Metalworking – BGHM). The pain onset of 100 subjects was examined at 29 well-distributed body locations through the use of a pain algometer. The results of the finished study were taken into the upcoming ISO/TS 15066. [15]

The onset of pain due to dynamic contact (collisions during intended use) is currently being determined by the Fraunhofer IFF in a study that was also initiated by the BGHM. We are examining 40 subjects at 21 body locations with a mechanical pendulum, which is an ideal testing device to simulate human-robot collisions (see Figure 9). The parameters mass, collision speed and contact contour can be freely adjusted in a wide range to match those of real robots. The study is accompanied by physicians from different domains, in particular from the Institute for Forensic Medicine and the Clinic for Accident Surgery of the Medical Center of the Otto von Guericke University Magdeburg. Ethical approval for this study was obtained from the Ethical Committee of the Otto von Guericke University in Magdeburg. The study is expected to be finished by the middle of 2016.

Limit Values for Injury Onset

The onset of injury due to dynamic contact (collisions during foreseeable misuse – the most common case for unintended contacts) is currently being determined in a study of the Fraunhofer IFF that is funded by KUKA and Daimler. We are currently examining 30 subjects at five body locations with the same pendulum as used for the pain study. In a previous pilot phase, we had already examined eight subjects and it was shown that the approach and experimental design lead to feasible results. [13] The study is accompanied by physicians from the Institute for Forensic Medicine, the Clinic for Accident Surgery of the Medical Center of the Otto von Guericke University Magdeburg. Ethical approval for this study was obtained from the Ethical Committee of the Otto von Guericke University in Magdeburg. The study will be completed by the end of 2015.

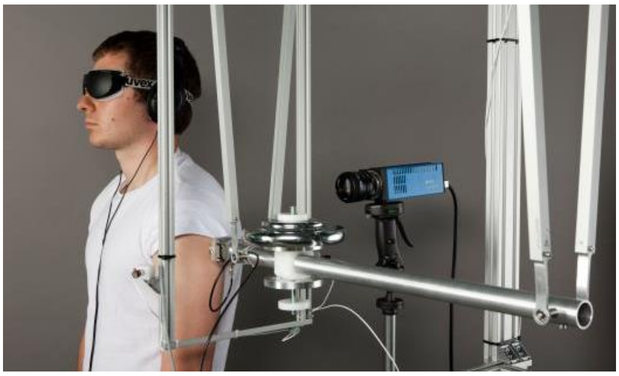


Figure 9: Mechanical pendulum for examining verified limit values of dynamic contacts (collisions)

Discussion

The presented taxonomy will be compared to a different and more comprehensive taxonomy in the next section. In the last section additional remarks will be given and discussed regarding the upcoming technologies and fundamentals.

Taxonomy

In general there are various aspects that can be taken into account for determining the form of a collaborative scenario. In contrast to our taxonomy, which only consists of three characteristics, the author of [2] detailed many more characteristics which can be existent if all possible forms of collaborative scenarios are considered. Altogether, 20 different forms of co-work were defined. However, we found a taxonomy consisting of more characteristics, as used in this paper, cannot be applied easily, especially in combination with the safeguarding modes of ISO/TS 15066. For this purpose we focused only on the essential characteristics that are also relevant for ISO/TS 15066 and are easy to understand and use in practice by systems integrators and end-users.

The field of collaborative robots is rapidly developing and changing, and we do not claim that the proposed taxonomy may be applicable to all possible future scenarios. In general the taxonomy should not be considered as absolute or dogmatically but rather as a supportive means for characterizing the robotic set-up and determining a possible safeguarding mode that is appropriate for the respective workcell.

Safety Technologies and Studies on Limit Values

The presented technologies we are currently working on are still in the prototype phase and will not be commercially available for a couple of years. However, it can be assumed that the release of the ISO/TS 15066 will encourage robot and sensor suppliers to develop new safety products for the next generation of robotics. From our perspective it is absolutely indispensable that future safety sensors be explicitly developed for one certain mode of safeguarding. Especially for the mode “Speed and Separation Monitoring”, in which the human is working beside the robot without any physical contact, we see a tremendous need for tailored safety sensors which take advantage of the possibilities to their full extent.

The safeguarding mode “Power and Force Limiting” is also in a similar situation in that it can only be applied properly when limit values for all kind of contacts and situations are available.

Conclusion

We conclude with the claim that a consistent taxonomy and definitions can help clarify any confusion surrounding terms that are frequently used to describe collaborative robots and scenarios. Furthermore, we showed how a taxonomy based on only three characteristics can be combined with the safeguarding modes of the upcoming ISO/TS 15066.

We showed that certain safeguarding modes can only take advantage of the potential if the used sensors are tailored to the specified requirements and potentials in equal measure. Especially the mode “Speed and Separation Monitoring” can only be applied properly if the sensor system comes up with specific capabilities which cannot be realized by currently available sensors. In contrast to this mode, “Power and Force Limiting” has a sufficient number of technologies are commercially available. However the biomechanical limit values currently available are only suited to very specific set of contact cases and the intended use. The studies presented here regarding the determination of verified limit values are an important foundation for the closest form of human-robot collaboration and will enable new applications in the future.

References

[1] ISO TC 184/SC 2 N, *Robots and robotic devices – Collaborative robots*, ISO/TS 15066, draft as of 4th May, 2015

[2] R. Spillner, *Einsatz und Planung von Roboterassistenz zur Berücksichtigung von Leistungswandlungen in der Produktion* (dissertation only in German language available), Herbert Utz Verlag, Munich (Germany), 2015

[3] “coexist”, “cooperate”, “collaborate”, *Merriam-Webster.com*, http://www.merriam-webster.com, 27th Aug. 2015

[4] C. Vogel, C. Walter, M. Poggendorf, N. Elkmann, *Towards safe Physical Human-Robot Collaboration: A Projection-based Safety System*, 2011 IEEE/RSJ International Conference on Intelligent Robots and Systems, San Francisco (USA), 27th Sep. 2011

[5] C. Vogel, C. Walter, N. Elkmann, *Exploring the possibilities of supporting robot-assisted work places using a projection-based sensor system*, 2012 IEEE International Symposium on Robotic and Sensors Environments (ROSE), Magdeburg (Germany), 16th -18th Nov. 2012

[6] C. Vogel, C. Walter, N. Elkmann, *A Projection-based Sensor System for Safe Physical Human-Robot Collaboration*, 2013 IEEE/RSJ International Conference on Intelligent Robots and Systems, Tokyo (Japan), 3rd-8th Nov. 2013

[7] *Collaborative Robot eBook*, 5th edition, Robotique, 2015

[8] M. Fritzsche, N. Elkmann, *An Artificial Skin for Safe Human-Robot-Interaction*, Humanoids 09, Workshop on Tactile Sensing in Humanoids – Tactile Sensors & beyond, Paris (France), 7th Dec. 2009

[9] M. Fritzsche, N. Elkmann, *RoboTouch – An artificial skin for Human-Robot Interaction*, Sensor+Test Conference, Nuremberg (Germany), 26th-28th May 2009

[10] M. Fritzsche, N. Elkmann, J. Grützner, J. Saenz, *A Tactile Sensor with Cushioning Elements for Enhanced Safety in Human-Robot Interaction*, 2010 15th IASTED International Conference on Robotics and Applications (RA), Nov. 2010

[11] M. Fritzsche, N. Elkmann, J. Saenz, *A tactile sensor for collision detection and human robot interaction on complexly-shaped industrial robots*, 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Workshop "Advances in tactile sensing and touch-based human-robot interaction", Vilamoura (Portugal), 7th-12th Oct. 2012

[12] R. Behrens, N. Elkmann, H.J. Ottersbach, *A Contribution for Standardized Risk Assessment: Examination of Constrained and Unconstrained Human-Robot-Collisions*, 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Workshop "Safety in Human-Robot Coexistence & Interaction: How can Standardization and Research benefit from each other?", Vilamoura (Portugal), 7th-12th Oct. 2012

[13] R. Behrens, N. Elkmann, *Study on meaningful and verified Thresholds for minimizing the Consequences of Human-Robot Collisions*, 2014 IEEE International Conference on Robotics and Automation (ICRA), Hong Kong (China), 31st May 2014

[14] R. Behrens, C. Lerez, N. Elkmann, *KAN study 52: Biomechanical Thresholds*, Kommission Arbeitsschutz und Normung, Jun. 2014

[15] M. Melia, et al., *Measuring mechanical pain: the refinement and standardization of pressure pain threshold measurements*, Behavior research methods 47.1, Springer, 2014.

Corresponding address

The e-mail adresses of the authors are composed as follows: {forename}.{surname}@iff.fraunhofer.de

Challenges and new ways for the risk assessment of Cyber physical systems

Johannes Schubert

Austrian Workers' Compensation Board
Vienna, Austria

Abstract

Cyber-physical systems are distributed interconnected smart objects for networking embedded systems with Internet-based wireless technologies. They are used to record sensor data to help regulate materials, goods, and information flows.

Before placing machinery on the market and/or putting it into service, the manufacturer shall ensure that it satisfies the relevant essential health and safety requirements of the directive (2006/42/EC) on machinery.

This means that the manufacturer must ensure that a risk assessment is carried out, so the machinery must then be designed and constructed taking into account the results of the risk assessment. Therefor the manufacturer shall determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse. At the limits of the machine also temporal and spatial limits must be identified.

It is the question to clarify where the configuration of the machine starts and where it ends und how Cyber-physical systems are part of the whole structure of the machine (or are they partly completed machineries?), especially if these systems are spatially separated from the rest of the machine or connected with each other only through the Internet.

The reliable integration of standard components in cyber-physical systems could be problematic because there are no experiences so far to identify the hazards that can possibly arise and the associated hazardous situations.

Keywords:

manufacturer; limits of the machine; Machinery Directive; risk assessment;

Introduction

The Austrian Workers Compensation Board is the largest accident insurance organisation in Austria with about 4.5 million insured persons. The main focus is on prevention, so there are new themes and modern techniques (for example: developments in production technology) of great interest. The question is to clear there meaning in relation to the risks arising out of the use of machinery. Especially in the field of occupational safety there are many directives of the European Union, which have to be transposed to national laws or decrees.

In this context cyber-physical systems and “Industry 4.0” get a particular significance when manufacturers are using this new technology in the design of their machines.

There are regulations for producers or importers, for instance the Machinery Directive. So every machine which is affected by the directive is marked by the CE sign. The experience shows that accidents can occur because machineries aren't built according to the Machinery Directive and because of violations of the permitted use.

Cyber-physical systems are an essential part of “Industry 4.0”. Industry 4.0 is based on the fundamental recognition that the production is becoming a revolutionary change. It comes, not least, that machinery and products chance into cyber-physical objects and the processes of the production can be networked to the distribution. Many aspects must be considered where some of them are partially recognized in their scope.

The term "Cyber-physical System" is not normatively defined. Following facts usually characterize the details:

> Cyber-physical systems are distributed interconnected smart objects for networking embedded systems with internet-based wireless technologies. They are used to record sensor data to help regulate materials, goods and information flows.

Cyber-physical systems are using so called “Internet of Things techniques” and are usual connected to a cloud structure.

Methods

<u>Machinery Directive 2006/42/EC:</u>

By Industry 4.0 the Internet of Things techniques will becoming part of machineries, so there manufacturers who are going to place them in a member State of the European Community has to comply with the European “Machinery Directive 2006/42/EC". This means that:

- Before placing machinery on the market and/or putting it into service, the manufacturer shall ensure that it satisfies the relevant essential health and safety requirements of the directive (2006/42/EC) on machinery.

- The manufacturer of machinery must ensure that a risk assessment is carried out in order to determine the health and safety requirements which apply to the machinery.

- The machinery must then be designed and constructed taking into account the results of the risk assessment.

By the iterative process of risk assessment and risk reduction, the manufacturer shall:

- determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse thereof,

- identify the hazards that can be generated by the machinery and the associated hazardous situations,

- estimate the risks, taking into account the severity of the possible injury or damage to health and the probability of its occurrence,

- evaluate the risks, with a view to determining whether risk reduction is required, in accordance with the objective of the Machinery Directive,

- eliminate the hazards or reduce the risks associated with these hazards by application of protective measures, in the order of priority established in the Machinery Directive.

ISO 12100 Safety of machinery:

According to the specifications of the harmonised standard EN ISO 12100 risk assessment begins with the establishment of the limits of the machine, including all phases of the life of the machinery.

As we know, a harmonised standard is a non-binding technical specification adopted by a standardisation body (for example the European Committee for Standardisation (CEN)), on the basis of a remit issued by the European Commission. This means that the characteristics and performance of the machine as well as the people, the environment and related products in terms of on the limits of the machine, should be accurately determined.

The risk analysis provides information needed to risk assessment, in turn, using their decisions can be made on whether a risk reduction is required. The Manufacturer of machinery must always consider that the lack of a history of accidents, a small number of accidents or a low harm should not make believe, that the risk is low.

This might be a special problem in terms of cyber-physical systems, since generally no data for the quantitative research is available. It is assumed that an existing hazard on a machine results sooner or later in damage, if no precaution is taken!

According to the ISO 12100 Standard the manufacturer has in the iterative process of risk assessment and risk reduction to determine the limits of the machine, which includes the intended use and any reasonably foreseeable misuse. For cyber-physical systems no serious differences with conventional machinery should occur during the practical approach. The aspects to be taken into consideration, spatial limits are the most difficult factor to handle in connection with cyber-physical systems. Here is the biggest uncertainty in comparison to conventional machines.

The factors referred to spatial limits in the standard EN ISO 12100 usually like as the space of movement, the space of operators, the interaction between man and machine, (E.g. the interface "Man/machine") and the interface "machine/power supply“. These factors have to be expanding by the following additional features regarding to cyber-physical systems:

- A cyber-physical system is characterised by its high degree of complexity.

- Because the data partially, be disclosed beyond the company borders with other business partners, the connection to the Internet is essential.

- Cyber-physical systems arises from the networking of embedded systems through wire or wireless communication networks, where the most important feature is the cloud combined with so-called "big data applications".

- In addition, cyber-physical systems have universal sensors to analyse and to monitor their environment.

- Production-related mass data must be analysed and transferred to a qualified evaluation.

So far, the server of IT-systems is close coupled to production. In Cloud-based systems additional challenges such as latency, and the speed of the network plays an essential role.

Results

Machinery Directive 2006/42/EC:

It is too differentiate whether despite new “Internet of Things techniques”, field bus systems and industrial ethernet networks are used as essential elements of the control architecture. This means that the pure control and regulation tasks are done with classical automation devices.

On the other hand Industry 4.0 allows innovative applications and business models that can be implemented successfully only with special equipment and techniques.Their meaning has to estimate in terms of machine safety.

Especially the connection to several value added networks requires an open and secure communication architecture, whose design determines the entire "safety philosophy" of the machinery.

This assumes, that a synchronous communication over Internet lines is technological possible.

The openness of systems as compared to the classic fieldbus gateways requires high demands on the security concept. This includes authentication, authorization, encryption, and data integrity through digital signatures. At this point the manufacturer has to ensure maximum possible safety.

At the same time the spatial limits are becoming blurred, so that the manufacturer must make a clear statement about where his machinery begins and where it ends. He has specifically to determine how deeply the link between the control technology and above all, the safety-technology of the individual systems should be, especially when several different manufacturers are involved.

There is the need to clarify the question, who then is the manufacturer of the whole new machinery?

The new machinery is the entirety of the individual systems, which can come from different manufacturers and are deeply networked with so-called Internet of Things techniques in connection with the cloud structure to build a production line.

At least it may be also possible for manufacturers to place a component of a cyber-physical system as a so-called "partly completed machinery" to the market.

A “partly completed machinery” means an assembly which is almost machinery but which cannot in itself perform a specific application. A drive system is a partly completed machinery. Partly completed machinery is only intended to be incorporated into or assembled with other machinery or other partly completed machinery or equipment, thereby forming machinery to apply with the European Machinery Directive.

By Installing a cyber-physical system as a partly completed machinery in an existing machine (plant), it becomes an extension with so-called “Internet of Things” techniques. It must be checked out by the manufacturer if a new machinery is placed on the market and how this changes increases the danger.

Conclusion

The knowledge of technical solutions alone is not enough!

Manufacturers in Europe have to note also the legal aspects of new technologies. In case of machines, this concerns above all the European Machinery Directive 2006/42/EC.

This means that a risk assessment and documentation covering all aspects is the basis for a safe and legally compliant machinery.

References

[1] DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery

[2] ISO 12100:2010; Safety of machinery — General principles for design — Risk assessment and risk reduction

[3] Guide to application of the Machinery Directive 2006/42/EC, 2nd Edition, June 2010

Functional safety application for collaboration of machines and persons on the basis of safety levels defined by position and velocity vectors

Yukio Hata, Yuji Hirao[a]

a Nagaoka University of Technology

1603-1, Kamitomioka, Nagaoka, Niigata 940-2188, Japan

Abstract

International standards of safety of machinery require safeguarding and complementary protective measures for collaboration of machines and operators where inherent safety measures are not applicable. However, in order to realize more sophisticated machinery systems, these measures are not sufficient, and it is necessary to apply functional safety to the collaboration for the purpose of enhancement of safety measures. Especially in the case of press machines, simultaneous actuation by machines and operators is possible during the machines' upward process, and a remarkable effect can be anticipated if we apply functional safety.

The aim of this paper is to propose a new functional safety control for the collaboration of press machines and operators on the basis of safety levels defined by the position and velocity vectors, and to evaluate the safety and productivity enhancement of this approach.

Concretely, safety levels are determined by the dynamic safety distance to the hazardous point and the relative speed, which are obtained by monitoring the movements of the press machine and the operator continuously, i.e. obtained by monitoring the position and velocity vectors.The speed of press machines is controlled appropriately so as to keep the minimum distance which corresponds to the safety levels. As a result, it has been revealed that the collaboration work area can be extended even to the press machines' downward area and this increases the work efficiency by 50%.

Keywords:

Press machine, Collaboration, Safe condition, Vector

1. Introduction

The press machine is known as one of the most dangerous machines. The injuries caused during the collaboration with press machines (manually loading a material and manually unloading a product) in the dangerous tool area have occurred far too often.

In this paper, we focus on collaboration with the press machine in the tool area that causes many severe injuries and apply the functional safety for the purpose of keeping the safe condition during the collaboration.The purpose of this paper is to propose the functional safety that enables not only the high performance of the continuous monitoring of the safe condition during the collaboration with the press machine but also the improvement of productivity.

First,we show some issues of single mode in the collaboration of press machines (manually loading a material and manually unloading a product) ,and the necessary functions to solve these issues.

Next, we define the safe condition and the dangerous condition by applying the concept of vectors (the relation of the position and the speed) to the relation of the machine and the operator. We show an example of the greater efficiency when this safety control system of the collaboration of machine and operator is applied to an actual machine and show the “control block diagram and necessary functions” which apply the functional safety to this safety control system.

We go on to evaluate the effect of this system on the safety of the collaboration of the machine and person and show the effect on the safety of collaboration with a press machine and the improvement of its productivity, As a result, we confirmed not only the contribution to the safety of the collaboration of the press machine and the operator of this system and to the improvement of its productivity but also the contribution to the safety of other future production systems. We also show other issues of the future safety control systems of the press machine.

2. The present issues of press machines

The manual operation of the press machine is the operation during the movement by single mode of the press in which the operator loads material into the die and unloads a product from the die by hand. The die area is the hazard area where inherently protective measures cannot be taken.

Access to the die area and manual operation in the die area during the press slide movement, which is the crushing hazard of the press machine, is allowed only when the safe condition (no danger) is confirmed.This access is restricted to allow only single mode and only during the upward process of the slide or in that area (see Fig 1.) after the slide has passed through the dangerous area of the downward process, according to the C standards of the press machine (for example ,EN692[1], ANSI B11.1[2] and so on).

Fig.1 shows the allowed area of the access to work in the die area during the slide movement of the press machine using the single mode. The crank angle of the mechanical crank press machine which is used to convert the crank angle to the linear motion of the slide (the die is attached to the slide) is detected by an encoder, and/or a rotary cam, installed on the crank rotation mechanism. The angle signals set by the use of an encoder and/or cams are used to control the stop at TDP(Top Dead Center), to allow access to the die area during the slide movement and to detect overrun and so on.

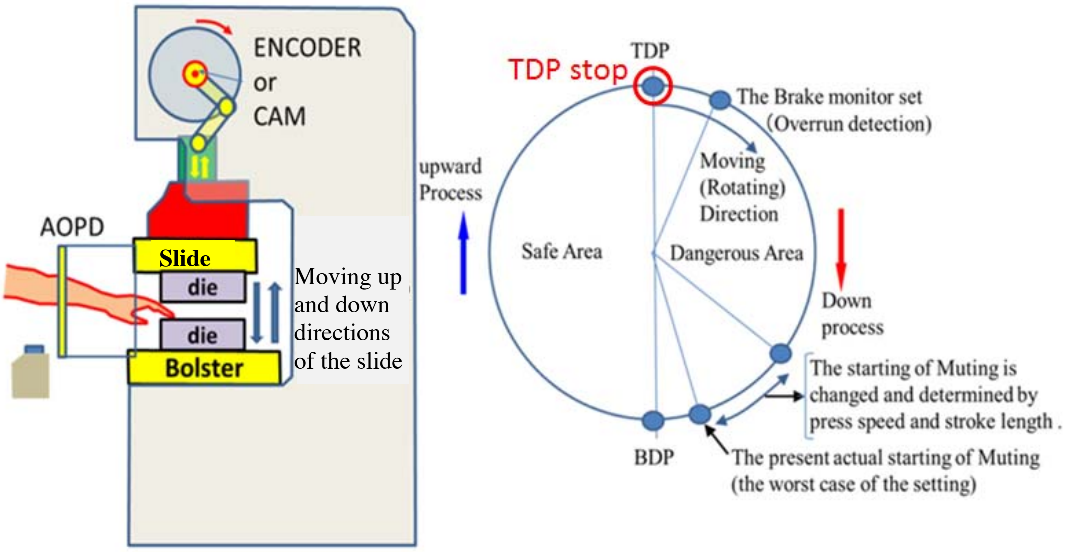

ENCODER
or
CAM
AOPD
Slide
die
die
Bolster
Moving up and down directions of the slide
upward Process
TDP stop
TDP
The Brake monitor set (Overrun detection)
Moving (Rotating) Direction
Safe Area
Dangerous Area
Down process
The starting of Muting is changed and determined by press speed and stroke length .
BDP
The present actual starting of Muting (the worst case of the setting)

Fig1. Single stroke of press machine

But some issues are confirmed in press machine standards, regarding their application to the collaboration of press machines and operators, and to the monitoring function relevant to the safety based on the protective measure of the press machine stop. The following are some of the main issues.

[1] Considering the safety and the productivity of the press machine, the changes of the position and the speed and any changes of setting data need to be continuously refreshed during the press machine movement. This continuous data is vital to the safety of the collaboration, and the safe and reliable system should be established. The safety function relevant to these settings needs an electronic control system which is controlled by the software, and the risk of the safety function of this system shall be estimated, and the functional safety shall be adequately applied.

[2] With the present restriction it is difficult to verify the validity of the setting, because the set data is based on the worst case regarding safety and the allowable operating area, and these set data depend on the operator, and the set data of the worst case makes the productivity lower. Sometimes, this issue may increase the possibility of an accident caused by human error and may decrease the productivity of the machine. Therefore, the continuous automatic optimum setting to which functional safety is applied is required for the setting function relevant to safety, operability and productivity.

[3] The access to the die area in single mode operation without the protective device is usually limited to the restricted area. The Inch Operation by a hold-to-run device which is used for die setting and adjustment is restricted by its one time operation travel distance and the press speed. For these reasons, the safety and the operability are not suitable for the operator. Therefore, the application of the safe condition for all press operation modes by a protective device (for example ESPE using AOPD, and two-hand control devices[4] and so on) relevant to the collaboration of the machine and the operator is necessary to solve this issue.

[4] The characteristic of this function is to detect the overrun of the slide when the slide does not stop at the TDP during the TDP stop process and to make the press stop when the overrun is detected. The overrun position of the mechanical press machine is set by its angle signal, but the detail of how to set and how to control the overrun is not clearly provided by the standards. But the mechanical press machine which has a servo drive but does not have a clutch system has become more common recently and this kind of machine usually uses the stop category 0 but not stop category 1 for the TDP stop control. Therefore the prediction of overrun detection before the overrun occurs becomes crucial; more important than the present overrun detection.

3.The technical proposal to the issues of the present press machine

The target of this proposal is to clarify the necessary safety condition of a press machine control system to solve the safety-related issues of the present control system of press machines shown in chapter 2, and also to propose the safety-related control system to apply to the safety measures of the collaboration of operator and press machine.

3.1 Safety condition of collaboration of machine and operator

Fig.2 shows the dangerous direction and safe direction in the collaboration of press machine and operator, to show the safe condition model by the motion vectors of the press machine and the operator. P(t) and H(t) in Fig.2 are the vector P(t) which has parameters of the press position and the speed and direction of the press movement and the vector H(t) which has parameters of the operator's position and the speed in a horizontal direction: the maximum speed expected toward the hazard .

All of the downward stroke area except the gap which is free from the crushing hazard (refer to the "Safety gap" in Fig.2) is considered a dangerous area from the “machinery safety” point of view , but in this paper all of the downward stroke area from TDP to BDP(bottom dead center) without exception is considered a dangerous area to explain each concept of the safety and the danger as a simple model.

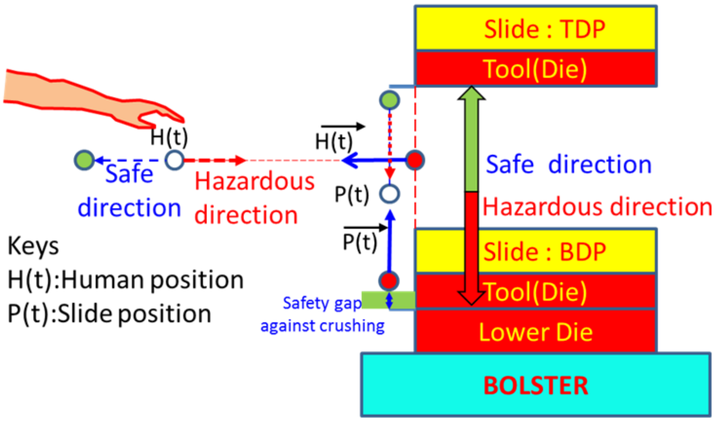


Fig. 2. Safety and Hazard in the Cooperation of Machine and Operator

If the position of the press machine from BDP at time t is P(t) the motion speed at time t is shown as dP(t)/dt. And in this paper, "dP(t)/dt<0" is the downward speed motion vector and ,"dP(t)/dt>0" is the upward speed motion vector. The dangerous condition of a press machine is the situation that an operator accesses the hazardous area while the press machine is moving downward. If the time t1 at time t is defined as the estimated travel time to BDP , the time t1 at time t is shown as equation (1).

$$\mathrm{t1} = \frac{[180-\{\cos^{-1}\{P(t)-r)/r\}]}{\omega} \quad \text{- (1)}$$

And if H(t) is the position that is the minimum safe distance of a person from the hazard area of the press machine at time t, the speed of the operator at time t is shown as dH(t)/dt. In this paper "dH(t)/dt<0" is the speed motion vector toward the hazard and ,"dH(t)/dt>0" is the speed motion vector moving away from the hazard. Since "H(t)=0" is the border point of the position of the operator between safety and danger, and then "H(t)>0 " shows the position of the operator is inside the hazard area and "H(t)>0 " shows the position of the operator is outside the hazard area.

When the operator accesses the machine, the safety condition at time t of the collaboration of the machine and the operator is that the press is in its upward process shown by equation (2), or the condition that a person cannot reach the hazardous area of the press machine during the downward process until the press machine reaches BDP. Therefore the safety condition at time t is shown as equation(3). And H(t+t1) is the expected position at time t when the operator will be expected to move until time t1. The safety condition of the collaboration of press machine and person is maintained by continuous monitoring of equation (3).

$$dP(t)/dt > 0 \qquad \text{-(2)}$$

$$\mathrm{H(t+t1)} = \mathrm{H(t)} - \left(\frac{\mathrm{dH(t)}}{\mathrm{dt}}\right) \times (\cos^{-1}\left((P(t)-r)/_{r}\right) / \ \omega \ \left(= \left(\frac{\mathrm{dH(t)}}{\mathrm{dt}}\right) \times \mathrm{t1}\right) > 0 \qquad \text{-(3)}$$

3.2 The verification of the safety condition of the collaboration of press machine and operator

Fig.3 shows the model of the application example that equation (2) and equation (3) are applied to an actual mechanical crank press machine. The machine specification of this model is as follows: the stroke length is 200mm, the maximum speed of this mechanical crank press is 150spm(strokes per minute: 900 degrees/s), and the operation is the manual loading of a material and unloading of a product.

AOPD which is usually used as the protective device for manual loading and unloading of a press machine is used in this model. The safe distance(Ds) from hazard to AOPD is fixed as "H(t)=350mm" which is detected at AOPD. The access speed of the operator which is used for the calculation of the safe distance is fixed as "dH(t)/dt=2000mm/s" which is provided by ISO13855[3] as the speed the human hand.

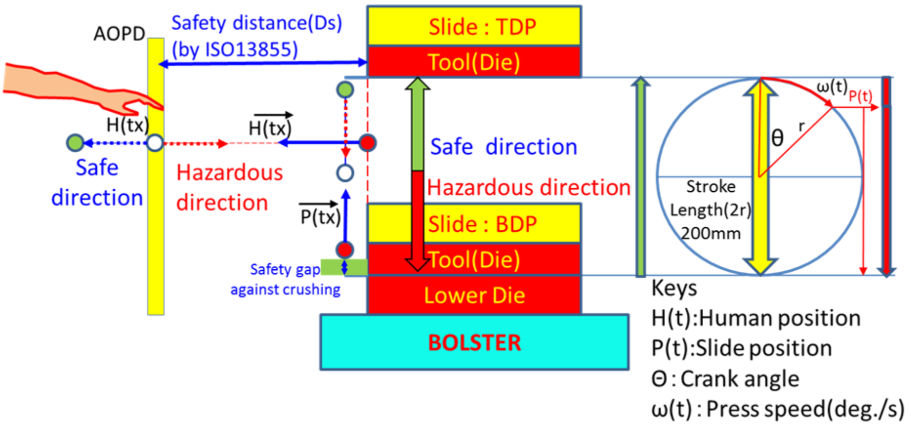


Fig.3 The application model of safety condition to mechanical crank press

If the angular velocity and the crank radius of the mechanical crank press shown in Fig.3 are as ω(t)(deg./s) and r(mm), press position P(t) (mm) and slide speed of the mechanical crank press dP(t)/dt (mm/s) are shown as equation (4) and equation (5). And if the crank angle from BDP of the safety area which is “the allowable area of collaboration of press machine and the operator” at time t is θm(t) (deg.), θm(t) is shown as equation (6) which is decided by the speed of the press machine and the arrival time of the operator at the hazard of the press machine.

$$\mathrm{P(t)} = \mathrm{r} \times (1 + \cos\theta) \qquad - (4)$$

$$\frac{dP(t)}{dt} = \frac{dP(t)}{d\theta} \times \frac{d\theta}{dt} = r\omega\sin\theta \;\; (\theta = \omega \mathrm{t}) \qquad - (5)$$

$$\theta\,\mathrm{m(t)} = \frac{d\theta}{dt} \times \frac{Safety\ distnce}{\left(\frac{dH(t)}{dt}\right)} \qquad - (6)$$

Fig.4 shows the following calculation results:The safety condition area during the downward process by equation (3),and the "safe area and danger area" by equation (2), and the crank angle from BDP of the safety area which is the allowable area of collaboration of the press machine and the operator by equation (6).

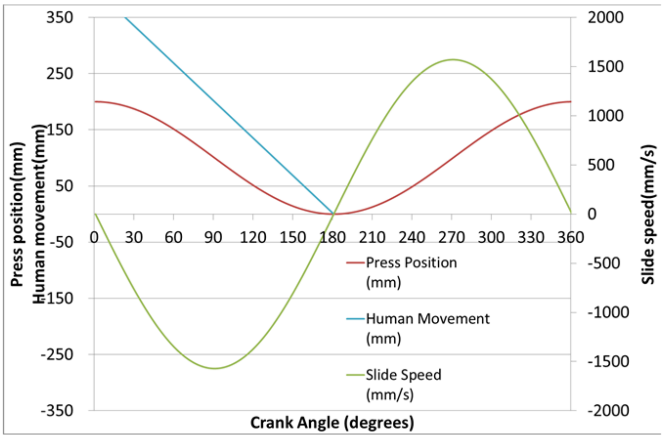
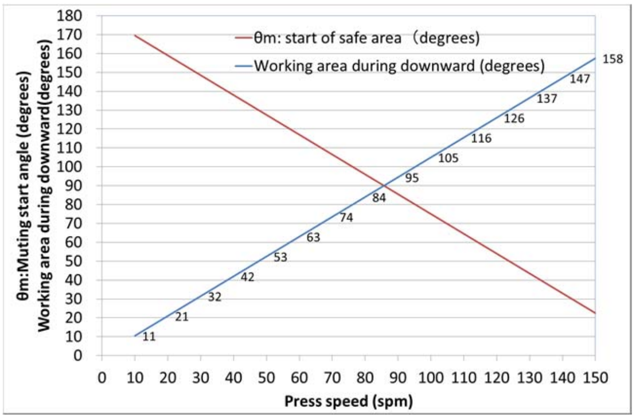


Fig.4 The judgement of the safety condition at each slide position

The safety area shown in Fig.4 is the safety area of the collaboration of machine and operator at the fixed press speed 150spm, but this safety area changes continuously according to the press speed. Therefore the press speed needs continuous monitoring to judge the safety area. Fig.5 shows the start position (angle) of the safety area according to the press speed where access to the hazard area is allowed to start, calculated by equation (6).



Press speed (spm)	θ m: start of safe area (degrees)	Working area during downward (degrees)
10	170	11
20	159	21
30	149	32
40	138	42
50	128	53
60	117	63
70	107	74
80	96	84
90	86	95
100	75	105
110	65	116
120	54	126
130	44	137
140	33	147
150	23	158

Fig. 5. Safety area of the downward stroke based on the press speed

3.3 The application of the safety condition of collaborative work by the functional safety control system

Fig.6 shows the following proposals:The risk estimation to decide the safety level of the safety related control system relevant to the collaboration of the mechanical crank press according to Annex E (refer to Fig.E.1 and Fig.E.2) of IEC61508-5[5], and the example of the control block diagram, and the function blocks of each function. The safety level SIL3 (PLe) shown in Fig.6 shall be required for this safety related control system if the risk level of this safety control system is considered according to the severity of injury, the frequency of the access to the hazard area by hand, and the possibility of avoiding the injury.

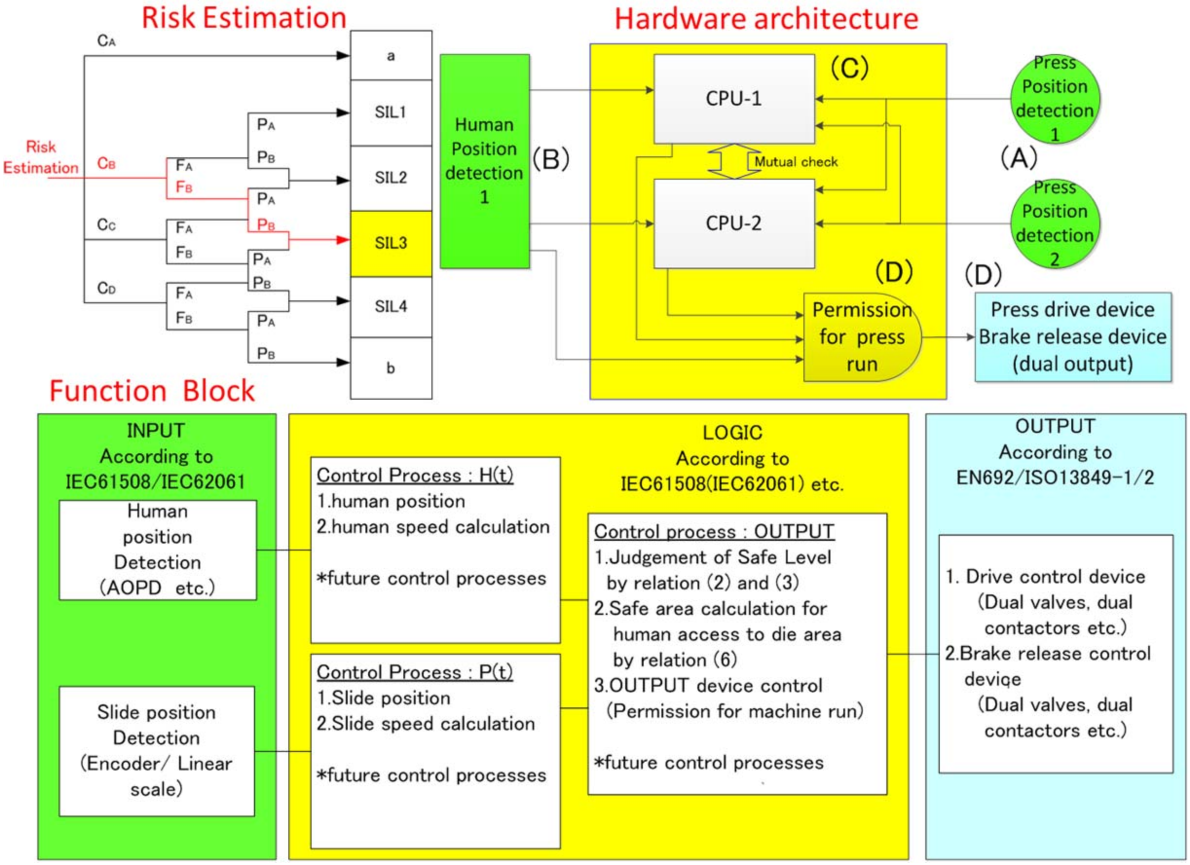

Risk Estimation
CA
CB
CC
CD
FA
FB
PA
PB
Risk Estimation
a
SIL1
SIL2
SIL3
SIL4
b
Hardware architecture
Human Position detection 1
(B)
CPU-1
(C)
Mutual check
CPU-2
Press Position detection 1
(A)
Press Position detection 2
(D)
Permission for press run
(D)
Press drive device
Brake release device
(dual output)
Function Block
INPUT
According to
IEC61508/IEC62061
Human position Detection (AOPD etc.)
Slide position Detection (Encoder/ Linear scale)
LOGIC
According to
IEC61508(IEC62061) etc.
Control Process : H(t)
1.human position
2.human speed calculation
*future control processes
Control Process : P(t)
1.Slide position
2.Slide speed calculation
*future control processes
Control process : OUTPUT
1.Judgement of Safe Level by relation (2) and (3)
2.Safe area calculation for human access to die area by relation (6)
3.OUTPUT device control (Permission for machine run)
*future control processes
OUTPUT
According to
EN692/ISO13849−1/2
1. Drive control device (Dual valves, dual contactors etc.)
2.Brake release control deviqe (Dual valves, dual contactors etc.)

Fig.6 The outline of control system of the safety function of the collaboration work

The following are the main outlines to be considered for FMEA if the functional safety is applied to the control system of the SIL3 collaboration control that is shown from (A) to (D) in Fig.6.

(A) A redundant system should be considered for the input system of the press position detection, or if possible the diversity structure should be considered to eliminate a common cause of failure. And if the redundant or diversity system is applied to the position detection, the common cause of failure by mechanical installation should also be considered.

(B) The ESPE using AOPD which is the type4 of IEC61496[4] is applied as the application example in this paper.

(C) The hardware architecture is the example to apply to the PLe[5]/SIL3[6][7][8][9] safety-related control system of which the hardware architecture is TypeB[8] and hardware fault tolerance 1(HFT=1) and the Safe Failure Fraction(SFF) more than 90%.

(D) It needs to use a redundant output device (e.g. dual valve with the spool monitoring, the use of double contacts with monitoring and so on) for the control system of functional safety level SIL3 and to keep the safe power cutoff and the safe brake control.

4. The necessity of applying functional safety and its effects of functional safety

In this paper, measures for the monitoring of the collaboration of press machine and operator which do not depend on the operator are shown , and functional safety is necessary for the realization of these measures, and the concrete safety conditions for the safety measures and the example of the application of functional safety are shown. It was confirmed that the allowable working area for the collaboration of the press machine and the operator is expanded by applying functional safety to the control of the safety condition .

Fig.7 shows the allowable manual loading and unloading work area according to the press speed, using Fig.5 as the comparison of the productivity when applying this system.

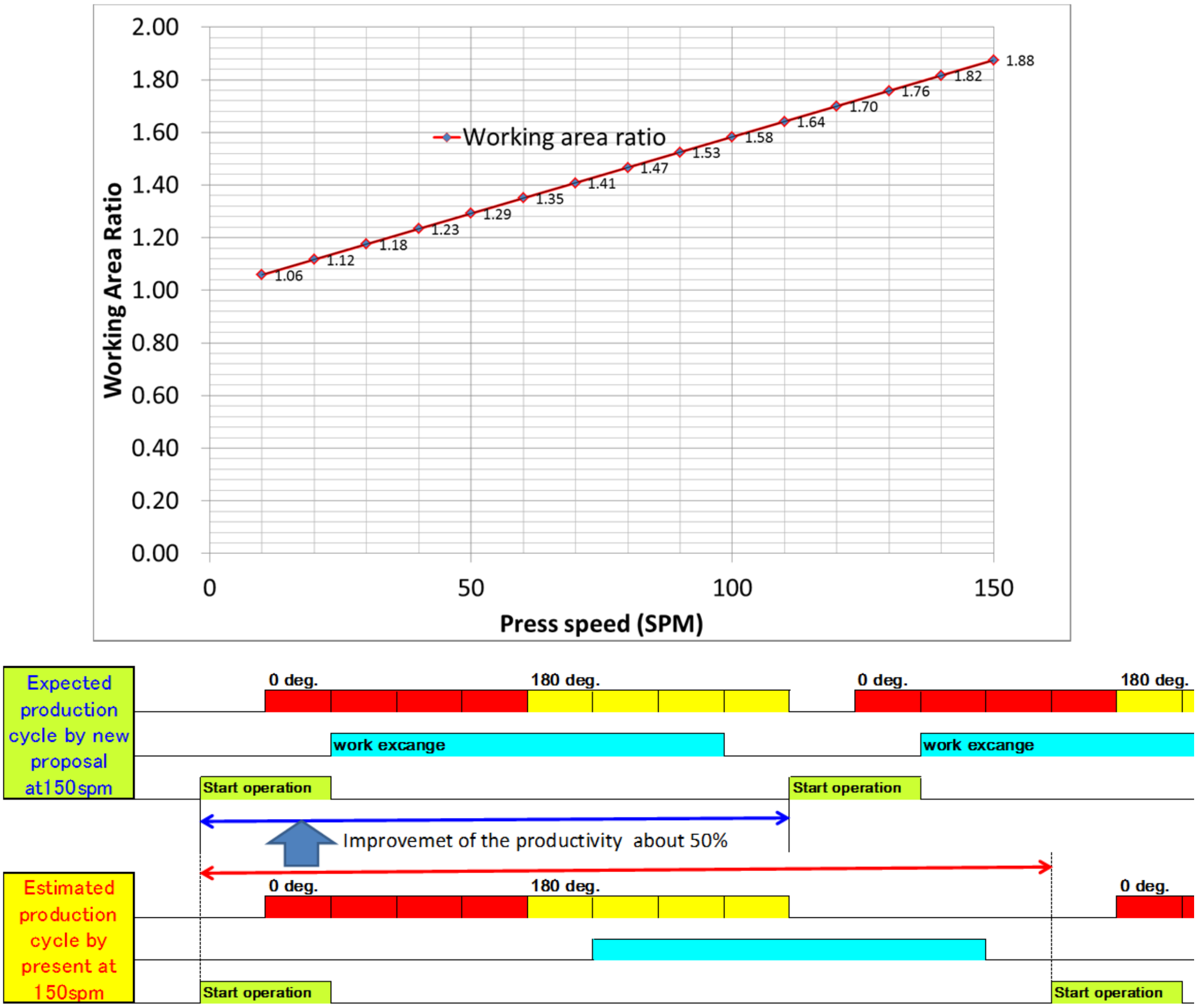


Fig.7 The allowable working area by press speed

Fig.7 shows the calculation result of the allowable working area based on press speed . The press machine specification is that the speed is 150spm and the safety distance 350mm. As a result, the allowable area of the collaboration is expected to be expanded 90% compared to the present press machine. The total production cycle time is expected to be improved by about 50% compared to the present production cycle time., The operator will be free from checking of the press BDP position, especially welcome in the case of high speed production, and as a result, improvements in the operability and the workability are expected.

5. Conclusion

As the results confirm, this proposal will contribute not only to deterministic safety measures but also to the improvement of productivity, especially for high speed production, achieved by applying the safety condition shown in equation (2) for the safety measures of the collaboration of the press machine and the operator and by applying functional safety to equation (2).

The incorporation of the safety condition into the control system of the press machine contributes not only the automatic judgement of the starting position of the collaboration of the press machine and the operator (the same as the muting position provided by EN692 and so on) but also includes overrun detection ,and as a result this proposal will establish the safety control system that does not depend on the operator of the press machine.

The safety condition for the collaborative work in this proposal is not sufficient for the servo press. More consideration of the servo press is needed, including, among other factors, the detection of the presence of the operator, the detection of the dynamics of the press machine, and the reaction time of each.

References

[1] EN692: Machine tools - Mechanical presses – Safety

[2] ANSI B11.1:EN692: Safety Requirements for Mechanical Power Presses

[3] ISO13855: Safety of machinery — Positioning of protective equipment with respect to the approach speeds of parts of the human body

[4] IEC61496-1: Safety of machinery – Electro-sensitive protective equipment –Part 1: General requirements and tests

[5] ISO13849-1: Safety of machinery — Safety-related parts of control systems —Part 1:General principles for design

[6] IEC62061:Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

[7] IEC61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 1: General requirements

[8] IEC61508-2: Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 2: Requirements for electrical/electronic/programmable electronic safetyrelated systems

[9] IEC61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems –Part 3: Software requirements

Central Institute for Labour Protection – National Research Institute (CIOP-PIB)
Ph.D. (Eng.) Grzegorz Owczarek
Ph.D. Agnieszka Kurczewska
Ph.D. (Eng.) Grzegorz Gralewicz

Application of ICT to smart personal protective equipment for safety management in the working environment

Keywords: smart PPE, safety management, augmented reality, radio frequency identification, undergarment microclimate, thermal comfort.

1. INTRODUCTION

This paper provides an overview of the results of three projects related to application of the Information and Communication Technologies (ICT) to smart personal protective equipment (PPE) for occupational safety and health management. Development and application of smart PPE includes integration of sensors, actuators, data transmission and processing units, as well as power sources within the PPE elements. The introduction of ICT to PPE solutions is one of the priorities of several international safety and health organizations. The Central Institute for Labour Protection – National Research Institute (CIOP-PIB) also works on multiple research projects in this field. In this paper, the examples and the results of the selected projects, oriented on the application of ICT to smart PPE for safety management in the working environment are presented. Development of the information support system for welders, based on augmented reality (AR) integrated with eye protection devices and new methods to identify and monitor the time of use of PPE equipped with RFID tags as well as to monitor selected physical parameters of undergarment microclimate for identification of users thermal comfort [1].

The main objective of the information support system for welders is to develop a model of AR system which allows to put the additional pictures and/or security signs in the field of view of welders using helmets with automatic welding filters. The pictures or signs can be useful for familiarizing workers with: welding place, area around the welding place and potential risks. The model of AR system for welders takes advantage of: micro camera recording the area around the user in order to identify the surrounding objects, AR displays integrated with welding helmets, electronic devices allowing for the communication between the camera and the display, sensor module (e.g. electromagnetic field, temperature of welded objects, etc.), defectoscopy module (for non destructive testing of welded objects), databases containing information about objects, manuals, etc., communication systems allowing for radio transmission of the information that can be displayed in the users' field of view. The AR system integrated within the welding helmets is programmed using the original software based on algorithms to identify defects arising during the welding process. Graphical user interface of the AR display provides the following information: actual intensity of welding current, temperature of welded object, actual shade number of automatic welding filter, welding technology (e.g. TIG or TAG), information about potential hazards (e.g. magnetic fields, explosion, objects around welding place).

The concept of the radio frequency identification (RFID) system is to identify and monitor the time of use of PPE equipped with RFID tags. PPE is characterized by a certain "lifetime" associated with the loss of parameters which depends on the degree of their exposure to the environmental agents. Due to the importance of this issue, it is reasonable to search for solutions on how to monitor the time of safe use of the PPE.

The system for measuring the undergarment temperature and relative humidity with data logging and wireless data transmission consists of two main parts: measuring module (temperature and relative humidity sensors with data logger for measuring, data logging and wireless transmission) underwear as carrier of for the measuring module. Designed system allows for data viewing, analysis, and wireless transmission to the computer or to the server through GSM. The system is intended for tests with humans in real conditions.

2. AUTOMATIC IDENTIFICATION AND MONITORING PERSONAL PROTECTIVE EQUIPMENT

2.1. RFID TECHNOLOGY AND PPE

Laboratory examinations conducted in Health and Safety Executive [2] (UK) and the Central Institute for Labour Protection – National Research Institute [3] on both the individual protection equipment withdrawn from use and the new ones subject to accelerated ageing proved that the primary factors effecting in the loss of protective properties are:

- sun radiation,
- high and low temperatures and humidity,
- mechanical interactions, such as friction, cutting, piercing, etc.,
- penetration of dust into the structure of textile materials,
- interaction of aggressive chemicals.

In many cases users cannot detect these changes, and the PPE are applied in the situations of direct threat to life and health. Control and supervision of the PPE can be performed with the use of radio frequency identification (RFID) [4-8]. This technology finds more and more applications in the area of health and security at work. These include e.g. the documentation of data such as [6,8]:

- frequency of use of the emergency evacuation oxygen respirators in mining industry,
- frequency and circumstances of use of the equipment protecting against falling from heights.

Another application of RFID is planning of activities in high-risk areas, such as mines or construction site excavations. The scope of application of RFID technology in the area of occupational safety and health is a subject of studies of the Construction Industry Education and Research Unit of the University of Wuppertal [8]. The project included development of an RFID gateway for automatic control of the PPE. The gateway is installed at the entry to the work area. It allows to check all PPE each time when a user enters the work area. Thanks to the above, the employees have access to the dangerous areas, e.g. the construction sites, only if they possess the appropriate PPE.

2.2. CONCEPT OF AUTOMATIC IDENTIFICATION OF AN AUTOMATIC IDENTIFICATION AND MONITORING SYSTEM

Sustaining the condition of health and safety at work requires supervision and control over the correct selection, use, storage and maintenance of the PPE. These tasks burden mostly the employer and the employee utilizing the equipment. The condition of proper execution of the task is the appropriate control of the PPE. It should be performed on two levels:

- directly before start of work – performed by the employee, who is about to use the equipment,
- periodically (e.g. once a year) – performed by a competent, specially trained person in the workplace or directly by the manufacturer or its authorized service branch.

The tool in the form of an automatic identification and monitoring system for the PPE will improve the usage control processes and observance of the scheduled technical condition reviews. The concept of system operation is based on remote, radio-based reading and recording data with the use of special electronic tags (radio tags) [4,5,7,9] attached to the supervised PPE and a reader connected to a computer. The block diagram of the automatic identification and monitoring system for the PPE is presented in Fig. 1.

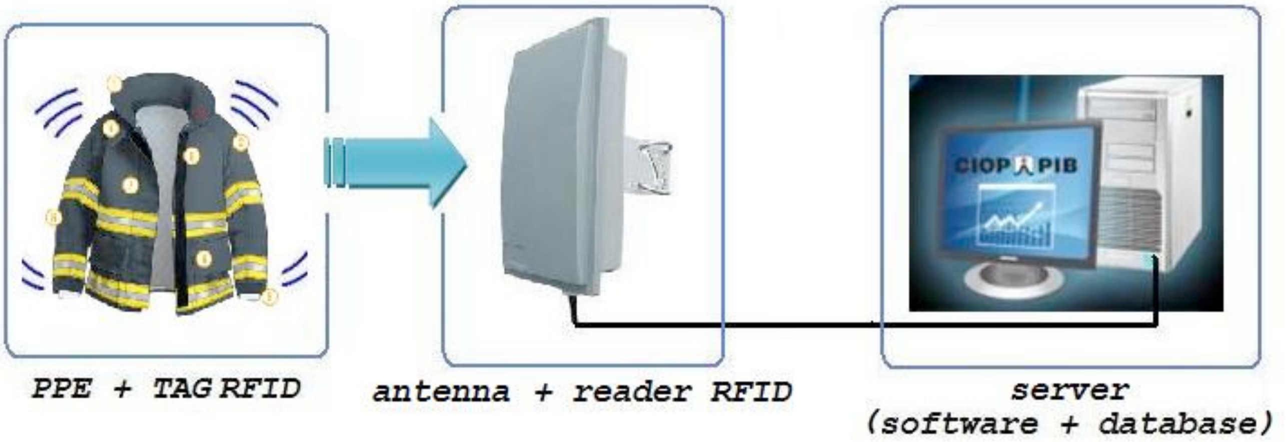


Fig. 1. Block diagram of the automatic identification and monitoring system for the PPE

The system operates with the use of the following components:

- electronic tags attached to the supervised PPE,
- antenna and reading/programming device (reader, terminal) with transmitter and decoder,

- server with software and database.

Information stored in the electronic tags attached to the PPE is read by the reader (and therefore the PPE is identified) and passed to the server, where it is recorded in the database. The collected information enables retracing the life cycle of the PPE. It also allows to improve the security of employees exposed to aggressive work environment factors, as well as to optimize the logistic processes in the workplace and enable keeping statistics and cost planning (generating periodical reports on PPE and statistic wear and tear reports).

Electronic tags. RFID tags is a small communication devices, in which the desired information is stored. The electronic tags can be made of various materials (plastic, paper) in custom shapes, depending on the application. Data transmission can be carried out using the following bands: ultra-high (UHF), high (HF) and low (LF) frequency [7]. First, the scanning antenna puts out the radio frequency (RF) signal. The RF radiation will provide a communication with the tag and provide tag with energy to communicate. When tag pases through the antenna, it detects the activation signal. That activate and transmits the information on tag to the scanning antenna (Fig. 2).

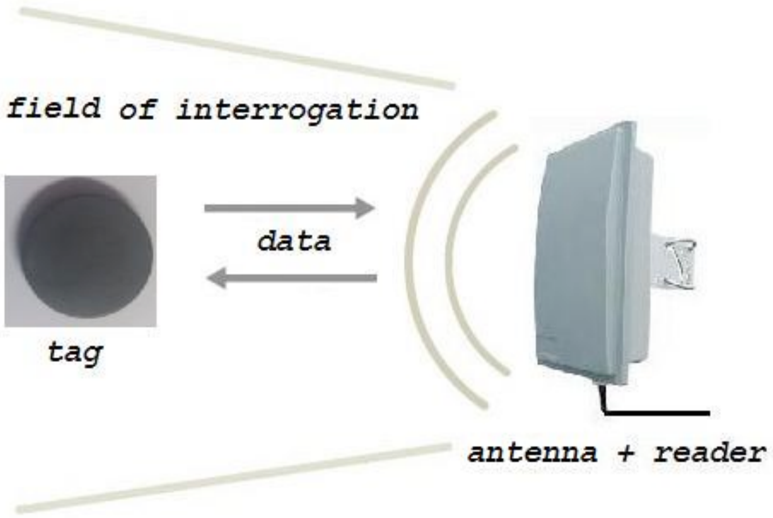


Fig. 2. Activate and transmits the information on RFID tag to the scanning antenna

Electronic tags can be divided into:

- passive (do not have their own power, draw power from the reader),
- active, meaning those that have their own power.

The data stored in RFID tags can be secured through encryption. We distinguish between tags: a secure information during transmission and tags with stored encrypted information.

Electronic tags are attached to PPE. Each tag has a certain amount of internal memory (EEPROM) in which it stores information about the PPE, such as unique ID (serial) number, or in some cases more details including manufacture date and product composition. When these tags pass through a field generated by a antenna RFID, they transmit this information to the reader, thereby identifying the PPE.

While selecting the RFID tag for implementation into the protective clothing (fire brigade clothing, chemical rescue personnel clothing, clothing protecting against cold), the following were taken into account:

- depending on the fabrics comprising the protective clothing,
- resistant to high temperatures (180 °C),
- resistant to repeated washing and also by chemical means,
- safe for delicate fabrics (no sharp edges),
- frequency (proximity tags and long range),
- availability.

For the first stage of works on integration of electronic tags with fabrics used in the protective clothing, the passive tags, i.e. without own power supply, were chosen. Two types were selected (Fig. 3):

- T-BT7700 – tag operating at the frequency of 13.56 MHz (HF) – proximity tag,
- UST 20100-1PC – tag operating at the frequencies of 862-955 MHz (UHF) – tag providing a long range of stored data reading.

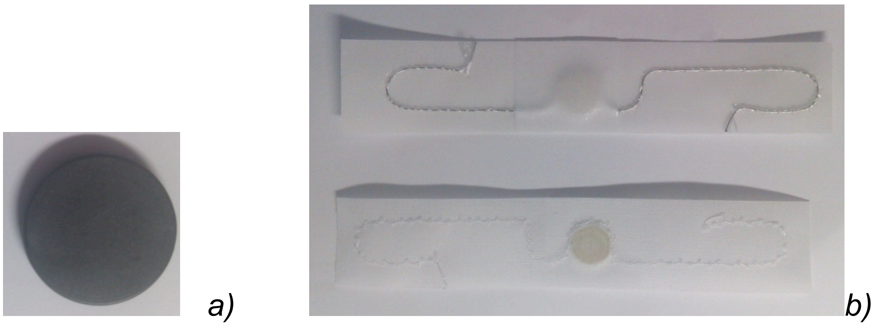


Fig. 3. Selected tag: a) proximity tag T-BT7700, b) tag providing a long range UST 20100-1PC [9]

2.3. IMPLEMENTATION OF ELECTRONIC TAGS ON THE PROTECTIVE CLOTHING Implementation of tags on the protective clothing (fire brigade clothing, chemical rescue personnel clothing, clothing protecting against cold) cannot worsen the protective parameters, must retain the ergonomics of use and should guarantee the appropriate functioning of the identification and monitoring system for the PPE. While selecting the methods of tag implementation into the protective clothing, the following were taken into account:

- type of fabrics comprising the protective clothing (woven cloths, non-woven fabrics, coated fabrics),
- type of electronic tag,
- tag implementation into the clothing (no need to introduce new technological processes to clothing manufacturing),
- no impact of the implementation to clothing usability functions,
- no impact of the implementation to clothing protective properties.

Two methods of implementing electronic tags in classic and coated fabrics used for the protective clothing were proposed:

- sewing in under square fabric fragment with backstitch (proximity tag T-BT7700) and adding terminals under the outer package layer (tag providing a long range UST 20100-1PC),
- pasting in pockets made of the same fabric as the clothing. The pasting of tags directly on the clothing was considered, but the method proved ineffective, as the tag was exposed to work environment factors and damage. The additional layer (pocket) guarantees the tag is protected.

2.4. CHANGES OF THE DATA READING RANGE

Afterwards, clothing packages, used as carriers of electronic tags for reading range research were combined. The prepared station was used to perform test of the impact of specific layers of clothing packages to the changes of the tag data reading range (Fig. 4). The tag reading range was also examined after the clothing was subjected to processes normal for PPE in regular use (i.e. washing, maintenance, exposure to high temperatures). Before the place of introduction of electronic tags in the complete clothing set for fire brigade or chemical rescue teams was determined, the impact of metal elements (i.e. zippers, snap fasteners, shackles) attached to the clothing on the change of reading range was also performed.

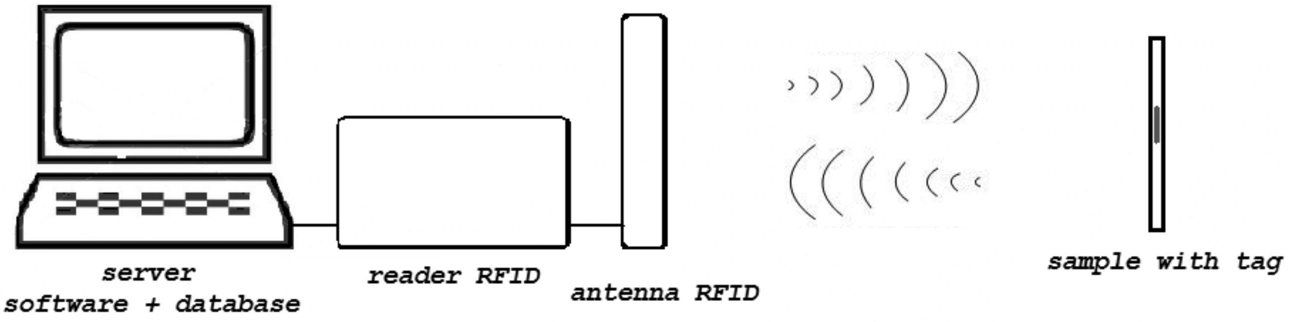


Fig. 4. Station to perform test of the impact of specific layers of clothing packages to the changes of the tag data reading range

To composition of the station to perform test of the impact of specific layers of clothing packages to the changes of the tag data reading range used the following equipment:

- reader: Motorola FX7400 RFID,
- RFID antenna: Motorola AN480-CL66100WR,
- notebook Dell XPS M1330 with software,
- meter stick with a resolution of 1 cm.

The test was performed in accordance with the following procedure:

- the sample packet of material with an electronic tag placed in front of the antenna,
- running a computer with software and RFID reader,
- the software is set to function code read from the tag,
- the sample was uniformly shifted by 1 cm in a straight line toward the RFID antenna,

- at the time code signal from the tag read distance measurements were made with samples from the antenna RFID tag,
- the result of measurements recorded in the card.

2.5. RESULTS AND DISCUSION

Fig. 5 and 6 illustrated selected results test of the impact of clothing (fire brigade clothing, chemical rescue personnel clothing, clothing protecting against cold) to the changes of the proximity tag: T-BT7700 and UST 20100-1PC data reading range. The distance measurements were made with samples from the antenna RFID tag is given in meters.

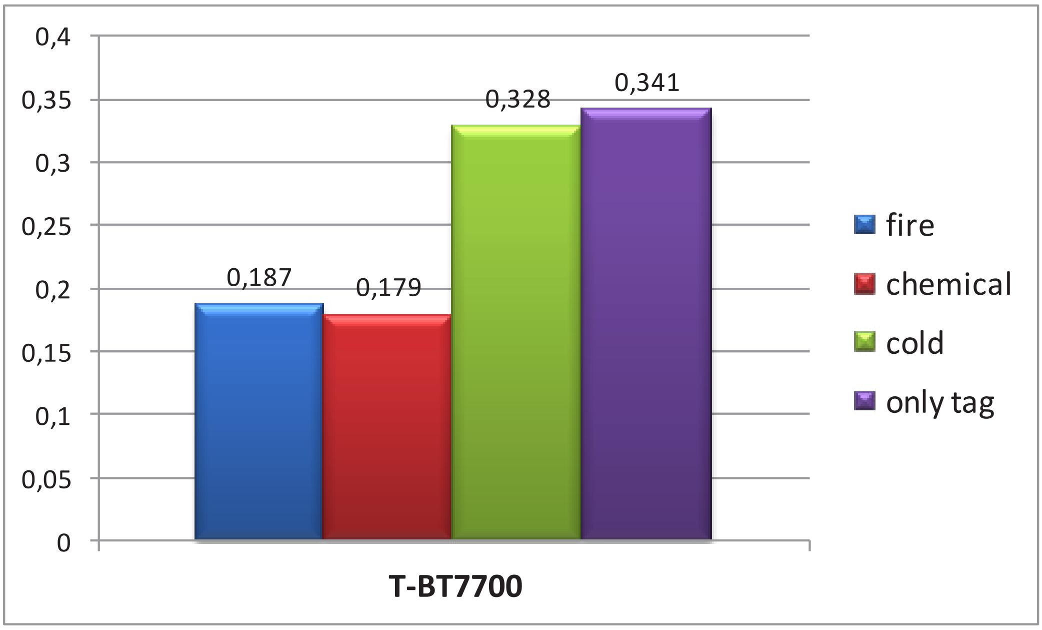


Fig. 5. Results test of the impact of clothing to the changes of the proximity tag T-BT7700 data reading range in meters. Note: fire - fire brigade clothing, chemical - chemical rescue personnel clothing, cold - clothing protecting against cold and only tag - T-BT7700

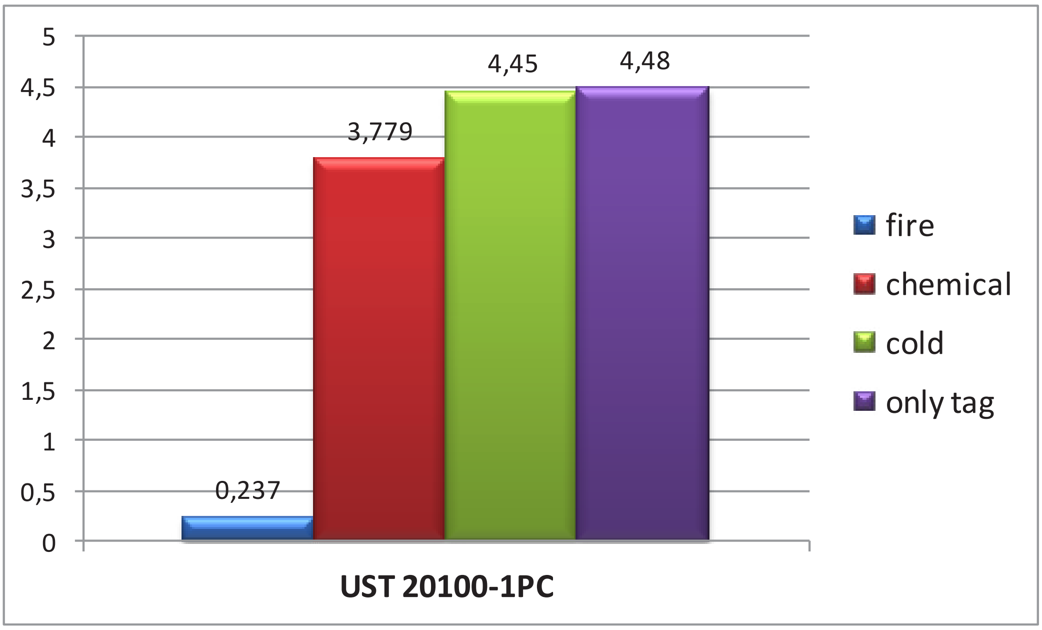


Fig. 6. Results test of the impact of clothing to the changes of the tag providing a long range UST 20100-1PC data reading range in meters. Note: fire - fire brigade clothing, chemical - chemical rescue personnel clothing, cold - clothing protecting against cold and only tag - UST 20100-1PC

The results of the performed tested are as follows:

- fabrics for antistatic clothing reduce the electronic tag data reading range to (0,237±0,003) m. The other layers of the fire brigade clothing package do not impact the reading range,
- coated fabrics used for protective clothing reduce the electronic tag data reading range of 47 % (proximity tags T-BT7700) and of 16 % (tag of long range UST 20100-1PC),
- regular fabrics used for protective clothing do not impact the electronic tag data reading range,
- in the flammability test, proximity tags T-BT7700 placed in the fire brigade clothing were damaged by the flames (+600°C). However, physical damage to the tags did not occur, and what is most important, during and after the test the tags did not pose an additional threat to the clothing user. Tags UST 20100-1PC of long range were not damaged,
- electronic tags placed in the clothing protecting against cold were not damaged after maintenance – 5 laundries (+60°C).
- electronic tags placed in the clothing protecting against cold were not damaged after maintenance – 5 dry cleaning processes.
- single metal elements (i.e. zippers, snap fasteners, shackles) placed in the protective clothing packages do not impact the tag data reading range,
- bigger density of the metal element leads to the decrease of the electronic tag data reading range. This imposes a requirement to keep the distance between the electronic tag and the metal elements, while placing the tags on the protective clothing, which allows to prevent from reading data range loss.

Analysis of the results of tag reading range research place in clothing packages allowed to indicate areas on the protective clothing, where the tag data read range is invariable and where the reading range changes. The proposed concept of the automatic identification and monitoring system for PPE is a tool supporting the execution of employers' obligations resulting from directive 89/656/EEC. The tool enables identification and monitoring of the duration of use of the PPE. It also allows to determine times of technical reviews, repairs and replacement of the equipment, respectively to the extent of wear of the PPE, which improves the safety of employees and reduces the costs borne by the employers. It also optimizes the operation of the employer and the control and supervision bodies through providing instant access to historical data on usage of the PPE in the workplace.

Implementation of the tool (the automatic identification and monitoring system) by the employees will result in:

1. Improved security of the employees exposed to aggressive work environment factors.
2. Support for fulfilling employers' obligations imposed by directive 89/686/EEC.
3. Determining the technical review, repair and replacement periods, respectively to the extent of wear of the PPE.
4. Recording the life cycle of PPE.
5. Analysis of the costs of purchase of PPE, divided into departments/work stations.
6. Keeping statistics and cost planning, with the account of cost centres.

The indicated practical applications of the system directly translate to the improved work safety of the employees utilizing the PPE. The practical applications listed in items 1, 2 and 3 allow for effective improvement of the method of management of the PPE in the workplace. The ability to perform purchase cost analyses (item 4) and keeping cost statistics (item 5) should cause a reduction of costs related to the use of the PPE.

3. AUGMENTED REALITY SYSTEM FOR INTEGRATION WITH WELDING HELMETS

3.1. AR HISTORY

The augmented reality system allows to observe surrounded reality and to put into the field of vision additional information. Tom Caudell is the author of the augmented reality therm. In 1992 he created a system that makes installation of electrical wires easier by using that technology. The augmented reality system described by Caudell is presented in the Fig. 7 [10].

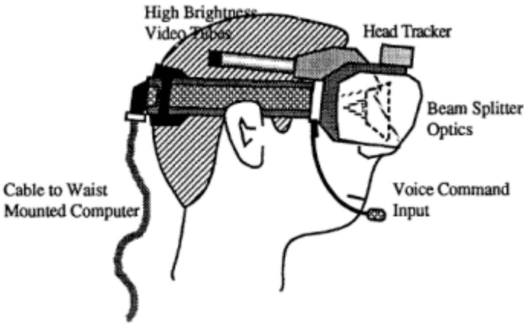


Fig. 7. AR system for installation of electrical wire described by Cudell [10]

The augmented reality system can be divided into two basic groups:

- system that allows, thanks to the special displayers, to display additional and computer generated information directly in front of user's eyes,
- system that displays images/information spatially correlated with the observed reality on traditional displayers.

The system presented in Fig. 7 can be joined to the first group. The second group are for e.g. the augmented reality systems that helps while moving in buildings. Many of GSM operators currently offer applications that allows to display in mobile phones information about objects that are identify by integrated with mobile phone GPRS system. The main distinguishing feature of augmented reality technology is the use of system allowing to display computer generated images or graphic symbols and the fact that it is placed directly in front of user's eyes [11]. The augmented reality system are used mainly during complex activities that need to be done with perceiving and quickly analysing a lot of information [12-14]. This systems need to meet a lot of technical and ergonomic standards that are based on user's comfort and his real need. That is why augmented reality systems are designed mainly according to its use for specially defined future group of users. The workers who operate production machines are generally that kind of group. In this case the augmented reality systems are mainly for generating warning signals made by for e.g. machine failure that are caused by appearance of danger in working environment of the worker [11]. During servicing the augmented reality system delivers to the users information about the order of performed activities. Examples of this kind of use can be find in the automotive industry [15] or during work with hazardous materials [16]. The augmented reality system for medical purposes are currently used during typical surgeries [17], and reconstructive treatments (e.g. jaw surgery [18]). The wide group of the augmented reality system users are also participants of specialist courses. The augmented reality helps in activities that need to be done with remembering many following steps.

3.2. THE POSSIBILITY USE OF AR SYSTEM AT WELDING WORKS

The augmented reality systems can also be used at welding works. During welding (excluding the automatic welding lines) it is necessary to use individual protectors, especially eye's and face's protections. While arc welding the welding helmets are used. Welding helmets can also be used during gas welding or in similar techniques. Every welding eye's protectors contains special filters that protect against harmful optical radiation that accompanies welding. Due to used technology the light transmission factors for welding are from about 0,0004% (filters with signature 13 commonly used at arc welding) up to about 4% (filters with signature 4 used at gas welding). That low values of light transmission factors for welding filters are necessary because of intensive visual radiation that comes with welding. There is especially a lot of light emitted at the arc welding technology. Looking through the welding filters made for arc welding the only thing that can be seen is the welded element. The automatic welding filter can be used in order to allows welder to observe, in a limited way, his surroundings without lifting his welding helmet. The light transmission factor in “the bright stage” is about 8% (welding filter with signature 5). Welding helmets are made of artificial materials by injection method and high quality pressboard or fibre materials. Constructions that are made by injection method characterized by hard/big stiffness what allows integrate additional elements that can be a part of the augmented reality system. This kind of system, containing among others camera, allows to put in a field of vision additional information with saving possibility to observe welded elements trough the welding filter. Basic elements of the augmented reality system for integration with welding helmet are: the augmented reality displayer, camera and modules which register and processing additional information that are put in the welder's field of vision. The additional information can be: an image from the welding surrounding, warning about appearing hazards and also information about welding process.

3.3. MODEL OF AR SYSTEM FOR WELDERS

The conception of the augmented reality system for integration with welding helmet assumes extend functions of currently used welding protectors into additional functions such as:

- observing the welding surrounding,
- informing welder about welding parameters and conditions and about environmental hazards,

- informing welder about material defects.

According to the presented conception the augmented reality system for integration with welding helmet should contains following basic elements:

- micro camera,
- sensor module
- defectoscopy system,
- augmented reality displayer,
- PDA computer.

Fig. 8 presents diagram that schematically shows basic elements of the augmented reality system for integration with welding helmet or with elements of welding equipment.

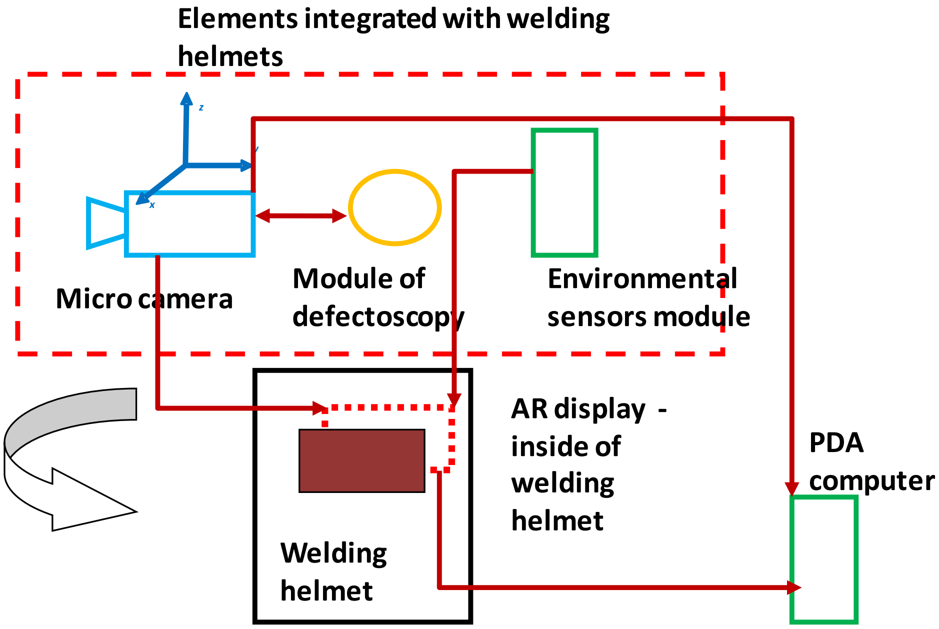

Elements integrated with welding helmets
Micro camera
Module of defectoscopy
Environmental sensors module
AR display - inside of welding helmet
PDA computer
Welding helmet

Fig. 8. Base elements designed for integration with welding helmet

At the assumptions for building the augmented reality system for integration with welding helmet model suggested the method of integration camera with welding helmet according to both construction possibilities and optical system parameters for providing registration of the images form welding surrounding by the camera. An adequate model of graphic interface was designed for information set intended for presenting at the augmented reality displayer. According to the described assumptions the model of augmented reality system for integration with welding helmet was created. The system also contains elements of defectoscopy system and magnetic field sensor. In order to define assumptions for the software that allows an automatic detection of constructional damages there were done the analysis of algorithms and operations done in the defectoscopy system, mainly in the image presenting the defectoscopy tested field of welded constructions (penetration tests).

The integration camera with welding helmet was made so that the image from the welding surrounding at the various welder's head locations could be registered. As an integration spot of camera the surface on the top of the welding helmet (after consulting the final user group) was chosen. The integration of camera allowed the regulation of direction of the optical axis of the lens. In the Fig. 9 and 4 the scheme of camera mounted on welding helmet is presented. The Fig. 10 presents a picture of welding helmet with camera directed to observe welding area.

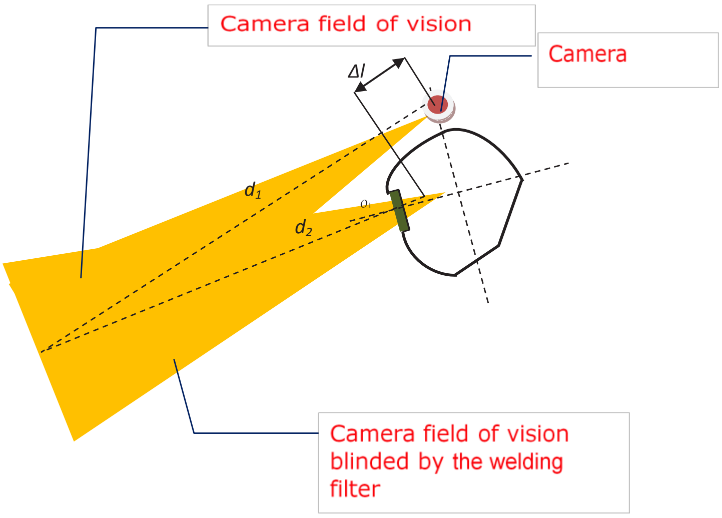
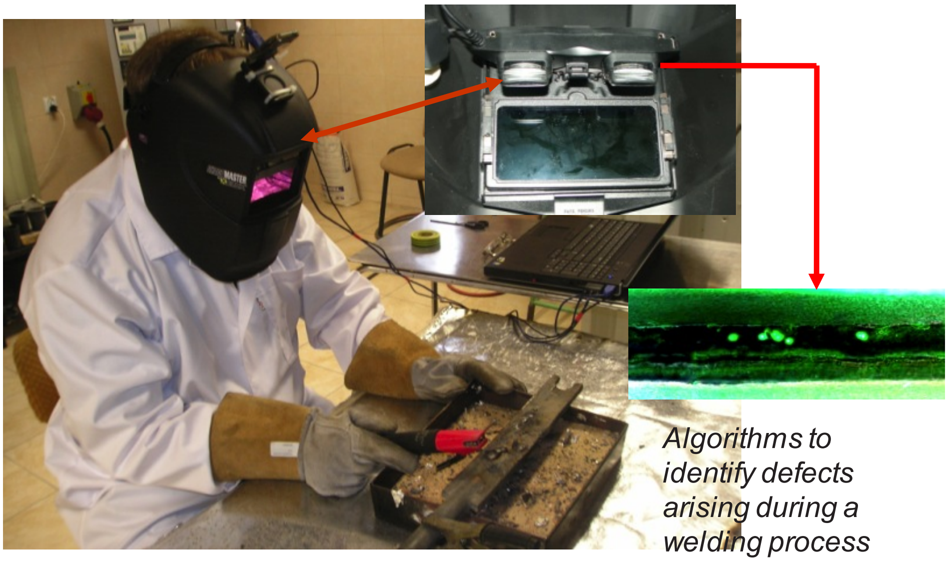


Fig. 9. Camera mounted on welding helmet – diagram *(Δl – distance between eye and camera; d_1, d_2 – distance of eye/ lens from observed object)*



Algorithms to identify defects arising during a welding process

Fig. 10. Observation of welding area using camera embedded with welding helmet

In the situation showed in the Fig. 10 a welded elements can be seen through both welding filter and, by using the camera, on the augmented reality displayer. The size of area displayed on the augmented reality displayer can be regulated by changing the focus of the camera. Mounting camera on the top of the welding helmet allows to observe welded elements. It only needs to direct the optical axis of the lens which goes through the centre of surface of camera image – converter on welded object. Leaning camera back and forward allows to choose proper observation area. During welding there can happen that welder also lean his head to a side what also requires adequate leaning of camera (the opposite direction to the welder's head turning) in order to "equalize" an observed image. Directing camera's lens mounted on welding helmet to the objects that are at the side of the welder we will not escape from situations in which an image would be "turned" due to leaning head. In that case here is recommended to use angel regulation of leaning camera with leaning user's head. These situations are rare. In aforementioned cases there are no problems with covering the camera's field of vision by user's head. The most difficult to make is an observation of objects that are behind the welder. There is no need to lean the camera to a side, but there is a serious problem with covering the camera's field of vision by welder's head, what is presented in Fig. 11.

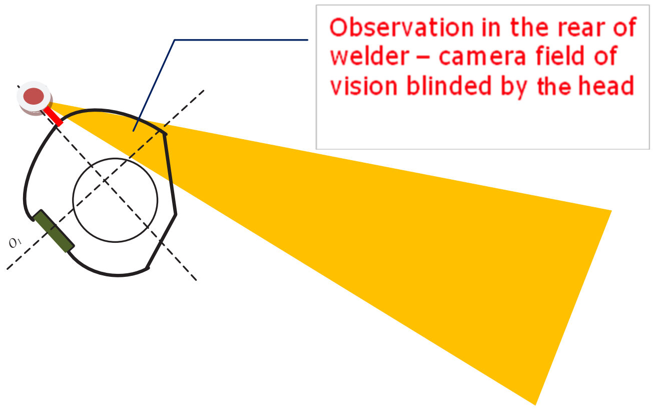

Observation in the rear of welder – camera field of vision blinded by the head

Fig. 11. Camera field of vision blinded by head – observation object in the rear of welder

An observation of objects that are behind the welder's head is limited when welding helmet is leaned down. Even when the camera is on the top of the welding helmet and there is a possibility to lean back the camera the helmet will significantly limit the possibility of observing objects that are behind the welder. Objects that are behind the welder can be observed only when welder's head is lean back or is not lean at all. Analysis of aforementioned cases shows that there are some construction possibilities of mounting the camera on welding helmet. This possibilities are:

- camera mounted on handler that allows to lean camera back and forward,
- camera is mounted on a handler ended with roll,
- camera mounted on a *"self-positioning"* handler.

The first possibility was used for construction of the described model. It is considered that, during observation of welding area, the back and forward regulation depending on the angel of welder's head's lean is enough. The advantage of this solution is simple and flat construction. After mounting the camera on the top of welding helmet there are no elements that significantly protrude over the camera's corpus. The height of protrude elements over the protector's corpus depends on how thick is used camera. In a model, made of elements that can be easily bought for anyone, the camera was 15 mm thick. With this type of mounting there can be done a special technological hole for hiding the camera in the welding helmet after being used. This solution limits the possibility to regulate camera to observe objects that are at welder's side (limited possibilities of "equalizing" an image while welder is leaning his head) and basically unable to observe by the camera objects that are behind the welder. The solution of that problem can be mounting the camera on a roll ended handler. Roll handler (articulated joint) are commonly used in camera tripod and handler for mounting GPRS. The use of roll handler solves the problem of "equalizing" an image during observing objects that are at welder's side. Never the less it does not solve the problem connected with observation objects that are behind the welder. The analysis of observing objects behind the welder shows that, in this case, it is required to mount optic system of the camera in a significant (about 10 cm) height over the welder's head. This solution makes that the length of camera's arm should be longer every time welder is leaning his head forward. Mounting camera on a self-positioning handler, which would enable to save the same plane orientation of image sensor, allows to automatic "equalizing" an image separately form welder's head turning and the welding helmet position. Never the less this solution is not commonly available. The most important advantages and disadvantages of described methods of mounting the camera on welding helmet are presented at table 1.

Tab. 1. Advantages and disadvantages of described methods of integrating camera with welding helmet.

Regulation system	Advantages	Disadvantages
Camera mounted on handler enables "*back and forward"* leaning	Simple construction; possibility of solid and stable integration with welding helmet	Limited regulation of the camera
Camera mounted on roll ended handler	Wide range of camera regulation	Less solid integration with welding helmet
Camera mounted on a "*self-positioning"* handler	Automatically positioning an image separately from the welder's head turning movement	High costs of construction (there are no such devices on the market)

The augmented reality displayer is mounted inside of welding helmet (look at Fig. 12) so that the prisms of displayer were at the line determined by the upper edge of automatic welding filter. In that position an observation through the welding filter and information displayed on the displayer is possible.

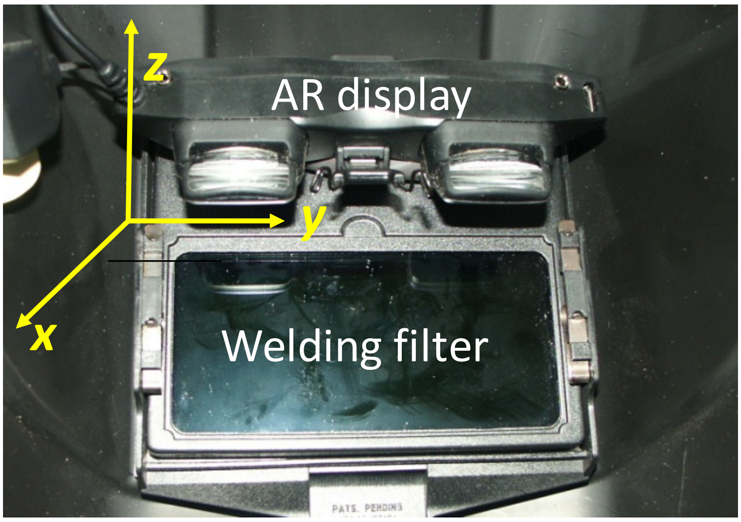


Fig. 12. AR display embedded with welding helmet

Owing to the use of the augmented reality displayer, the observation of registered image, additional information form sensors controlling welding conditions, environmental hazard and defectscopy system is possible. The model of the graphic interface is shown in the Fig. 13.

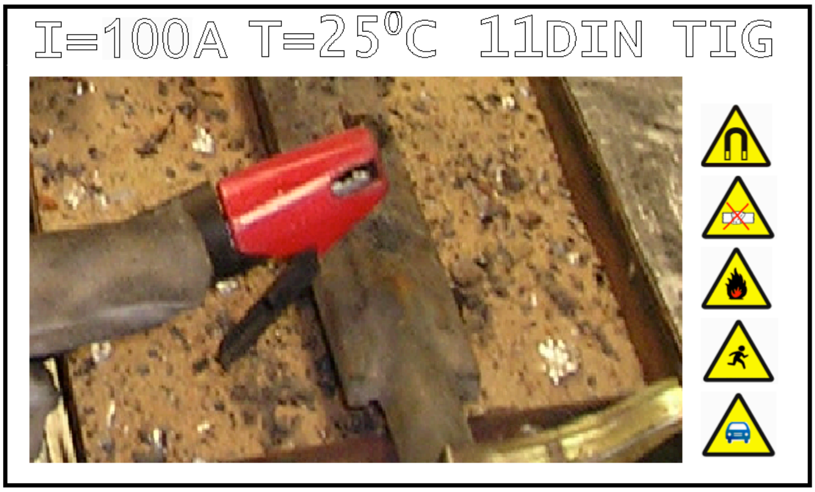


Fig. 13. Graphical interface model

The graphical interface contains four basic elements:

- frame,
- an image registered by the integrated with welding helmet camera,
- upper and side information bar.

The upper information bar contains information about: welding current, temperature at the welding spot, the actual level of shade automatic welding filter and about used welding technology. The side information bar contains ideograms which are displayed when there is a danger of magnetic pole, material defect (after using the defectoscopy evaluation), the dust and smoke hazard and hazards caused by appearing unauthorized persons at welder's area or danger at public traffic (e.g. during welding in an open space or on roads). The important element, considered while developing the concept of augmented reality system for welding, there is a possibility of changing information from hazard sensors (e.g. harmful electromagnetic radiation, chemical's hazard as dust and smoke caused by welding, noise) into a graphic symbols. [19]. In developed model of the augmented reality system for welding the information that need to be changed into graphic symbol is information about magnetic field hazard. The argument considered while making this choice was the fact that the electrical welder is also a strong source of electromagnetic field caused by current through an electrode and wires during welding. The level of workers' exposition to this electromagnetic field depends on used technology, the organization of welding workplace and the method of welding. The most exposed to the magnetic field is welder's hand in which he holds welding handle with electrode. Twisting wires that connect electrode or welding table (welded element) with the welding aggregator and putting them near the worker cause significant increase of danger. The magnetic field is then the sum of every magnetic field caused by every roll of wire [20].

The developed model of magnetic field sensor (look at Fig. 14) is to inform about exceeding the threshold of the magnetic field for range (1000 ± 500 Gauss). The threshold of the magnetic field is defined as a reference value. Sensor model works on a base of comparing measured value to the determined (programmed) value of intensity of magnetic field. The reference value can be programmed by exposing the sensor for a magnetic field exposure, that is as strong as the determined reference value. The signal about detection of magnetic field that is stronger than determined reference value initiates displaying by the graphic interface a symbol – magnetic field. Ultimately the magnetic field sensor will be mounted to the welding handler in which electric welding electrodes are placed.

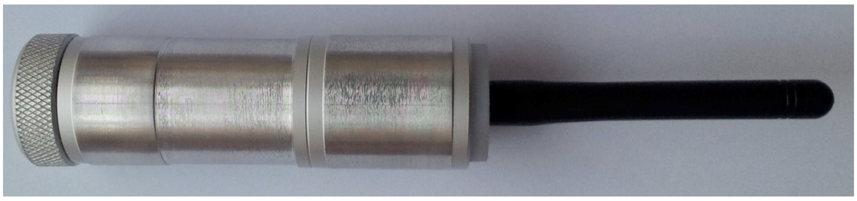


Fig. 14. Magnetic field sensor

Welded constructions during its work transfer constant or various loads and there are exposed for different kinds of damages. That is why the control of welded constructions is so important. The welded elements' control is made only with the use of non-damage methods. In defectospopes using ultraviolet radiation, that are commonly used in the industry, the person who is making the control observe surface of tested elements that are covered with special fluorescent liquid and illuminated by UV radiation [21].

In the solution of using the augmented reality technology the integrated with welding helmet camera can be the observer. Observed elements, as it was in research with using traditional defectoscopes, are covered with special fluorescent liquid. The image of welded element is transferred directly to the augmented reality displayer. Welder has the possibility to observe an unchanged image and an image that has been processed in order to determine discriminatory features showing the damages. In the case of observation a welded element by the camera for an automatic detection of possible damages there were many algorithms, that are able to define criteria allowing to point at the image the spots (defects) of various illumination, tested.

For a fragment of image that presents tested area the following operation were done:

- inversion,
- increasing contrast and brightness,
- increasing contrast,
- threshold,
- filter (e.g. edges detection).

The visual evaluation of images that were treated by aforementioned operations shows clearly the advantage of the increasing contrast method. The algorithm of increasing contrast will be used in in an algorithm allowing the automatic detection of damages. Identified spots of damage can be also taken into a frame. Described conception of designing the augmented reality system was consulted with its final users (welders). A survey was done as a part of consultations. The survey had questions about construction solution (among the others: mounting the camera and the augmented reality displayer), functions that designed system can additionally do, information about welding area and

hazard that may appear and then be displayed on the augmented reality displayer and the methods of its presentation. Welders defined that the one of the most important parameters is to show the temperature of welded element. They also said that it would be useful to display information about persons that are nearby or about approaching vehicles (during road work). Remarks collected as a survey answers and discussion will be included in the next stage of work based on creating prototype of the augmented reality system for integration with welding helmet.

4. SYSTEM FOR MEASURING TEMPERATURE AND RELATIVE HUMIDITY

4.1 CONCEPT OF SYSTEM FOR MEASURING UNDERGARMENT TEMPERATURE AND RELATIVE HUMIDITY WITH DATA LOGGING AND WIRELESS DATA TRANSMISSION

The Directive on Personal Protective Equipment (PPE) 89/686/EEC [22] specifies that such equipment including protective clothing should not only meet the basic protective parameters, but also ensure the greatest possible comfort of use and the lowest possible restrictions on worker movements. The comfort of use of protective clothing is influenced by many factors related to sensory and esthetic perceptions as well as thermal comfort which is particularly significant issue. According to literature data [23-25] to evaluate users thermal comfort in clothing besides the physiological indicators equally important is the undergarment microclimate that is the temperature and relative humidity in the space between the skin and clothing. In CIOP-PIB to assess thermal comfort provided by the clothing, the methodology using the developed system for measuring undergarment temperature and relative humidity with data logging and wireless data transmission has been worked out. The prototype of the system has been developed to measure, record, analyze, and wirelessly transfer the above-mentioned parameters to a computer or to a server through a GSM network. The system may be used in both laboratory tests and the field tests conducted under real-life conditions. A functional diagram of the system is given in Fig. 15.

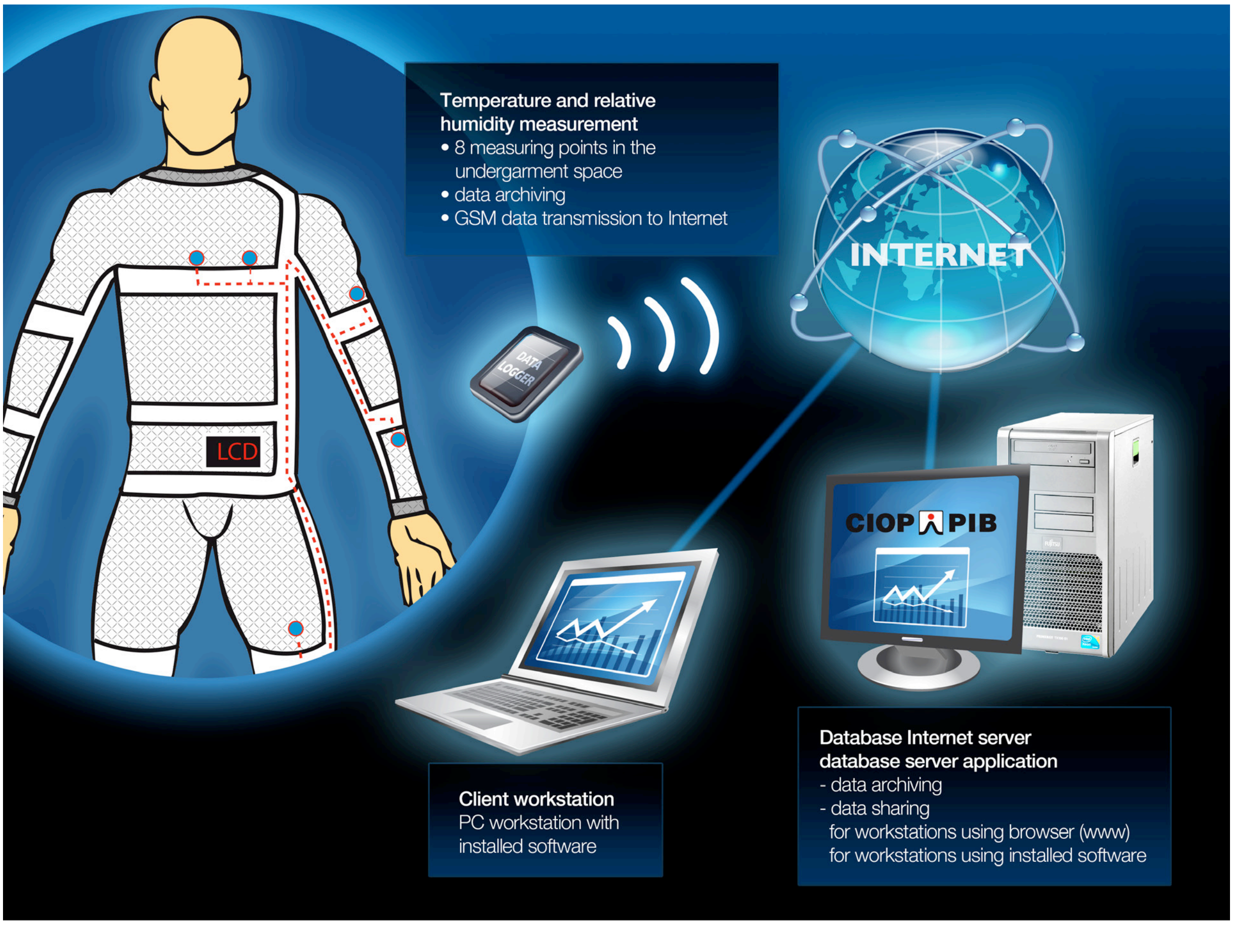

Temperature and relative humidity measurement
• 8 measuring points in the undergarment space
• data archiving
• GSM data transmission to Internet
INTERNET
DATA LOGGER
LCD
CIOP PIB
Client workstation
PC workstation with installed software
Database Internet server
database server application
- data archiving
- data sharing
for workstations using browser (www)
for workstations using installed software

Fig.15. Functional diagram of the system for measuring undergarment temperature and relative humidity with data logging and wireless data transmission – application under conditions of GSM signal availability [26]

4.2 PROTOTYPE OF THE SYSTEM FOR MEASURING UNDERGARMENT TEMPERATURE AND RELATIVE HUMIDITY

The developed prototype of the system consists of a measurement module composed of seven SHT 15 sensors, a device for data measuring, recording and transmitting (a data logger), and underwear in which the measurement module is mounted. Temperature and relative humidity sensors are located in selected places in the underwear. The measurement module is integrated with the underwear, but for conservation purposes may be entirely removed. The underwear in which the measurement module is implemented consists of a long-sleeved T-shirt and long pants. A special knitted material made of a polyester yarn (94%) and an elastomeric yarn (6%) was developed for this underwear. Measurement sensors are housed in casings and placed in the underwear in special “textile pockets” which are located on the inside of the underwear in selected places as presented in table 2. The size of pockets corresponds to the size of sensors in casings. All the sensors are connected with data logger by means of electrical cords implemented in knitted cord tunnels. Arrangement of the sensors in the underwear was designed based on literature data [27] and own research, in places in which the human body produces the greatest amount of sweat.

Tab. 2. Location of sensors in the underwear

SHT sensor symbol	Location
C1	Between the shoulder blades
C2	Arm
C3	Forearm
C4	Chest
C5	Between the breasts
C6	Right shoulder blade
C7	Front part of the thigh

A scheme of the developed system including arrangement of cord tunnels and sensor locations is given in Fig. 16.

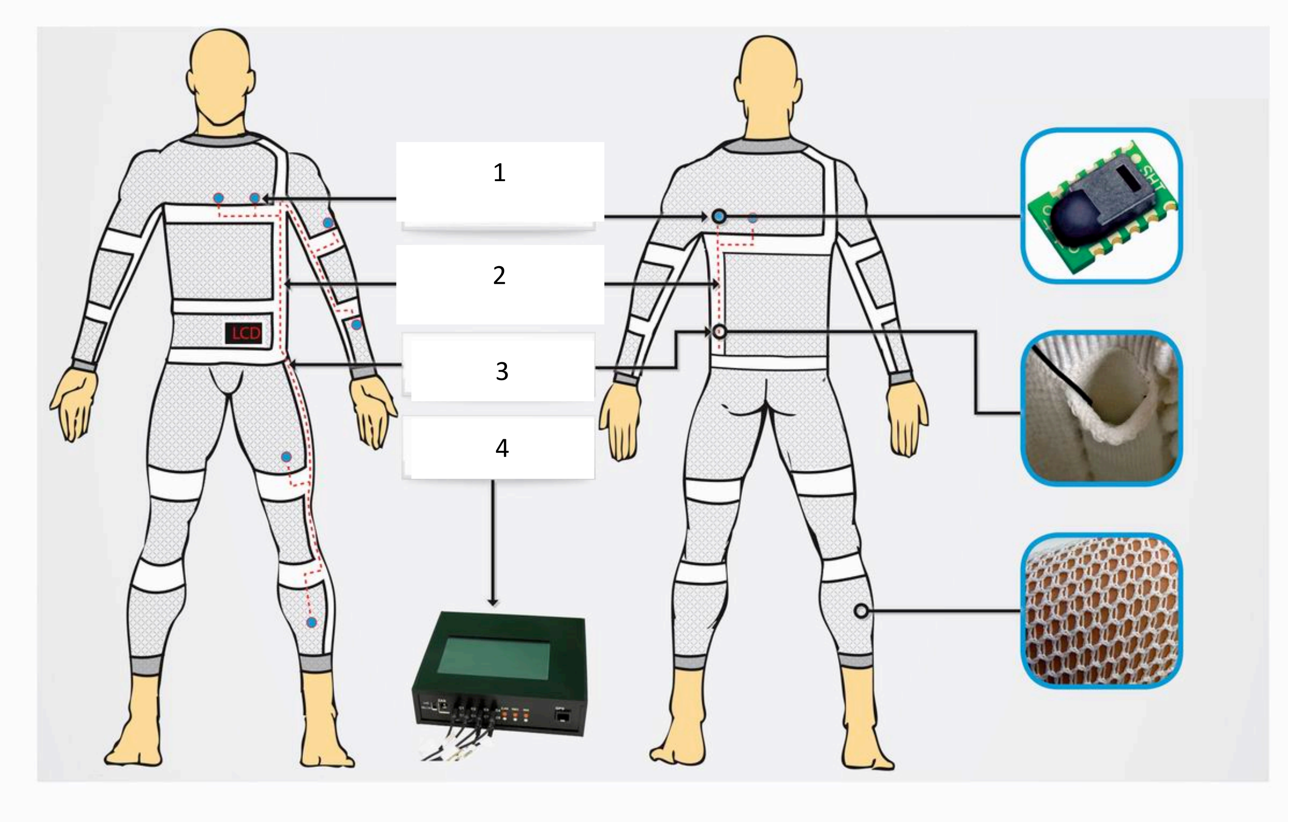


Fig. 16. Scheme of the prototype of the system for measurement of undergarment temperature and humidity with data recording and wireless transmission: 1 – SHT 15 sensors, 2 – cords, 3 – cord tunnels, 4 – data logger [26]

The developed system can be used to conduct tests:

- in laboratory conditions (eg in the chamber microclimatic) - data from temperature and humidity sensors are collected by the Data Logger and transmitted in real time to a computer or PDA (personal digital assistant) so that it can be assessed when doing research – mode: work with the computer,
- in real conditions (eg at workplaces, in the field, during climbing mountain climbing) - data from temperature and humidity sensors are sent via the GSM network to the server, or in the absence of access to the GSM network are stored in the Data Logger and transmitted to the server at the first access to the GSM signal - mode: work with the server.

4.3. METHODOLOGY

In order to assess the developed method with use of the system for measuring undergarment temperature and relative humidity with data logging and wireless data transmission tests on Newton thermal manikin as well as tests with human subjects have been performed [28].

The tests on the thermal manikin. The aim of the tests on thermal manikin was to assess the precision of the developed method in laboratory tests. Tests were performed on Newton, which is a male thermal manikin consisting of independently controllable heating segments

34 (Fig. 17). In tests manikin worked in test mode “Comfort”. In these mode surface temperature of each manikin segment correspond to the temperature of the relevant part of the human body while in thermal comfort.

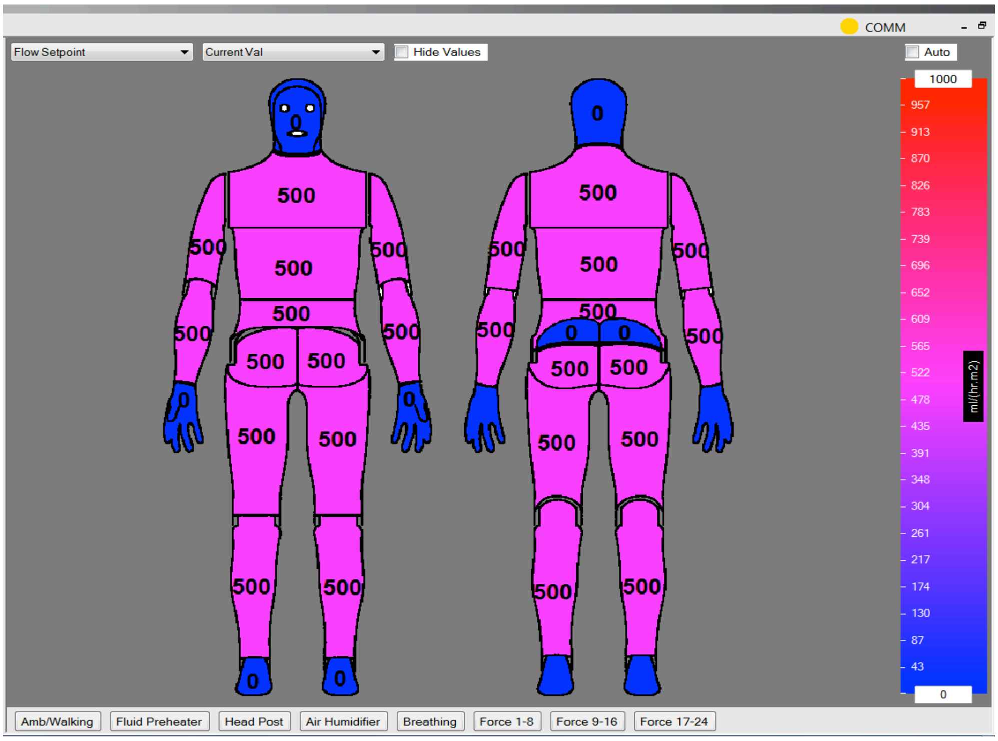


Fig. 17 Schematic of the manikin with marked its segments

The thermal manikin has been selected for tests due to the possibility of obtaining stable, reproducible test conditions. The tests were carried on in hot environment in the climatic chamber, where ambient temperature was (28)°C, and the air movement rate was (0.3 ± 0.1) m/s temperature. At low temperatures, below zero no studies have been conducted to check the operation of the system on a mannequin because of safety of electronics used in the manikin and the lack of stability to maintain its surface temperature. For tests the manikin was dressed in prototype of the system for measuring undergarment temperature and relative humidity with data logging and wireless data transmission (that is, a long-sleeved T-shirt and long pants with an integrated measurement module). On top of that manikin was dressed in the outfit consisting of: cotton long sleeve shirt, cotton trousers, cotton long jacket and cotton socks. Picture of manikin presented on the Fig. 18.

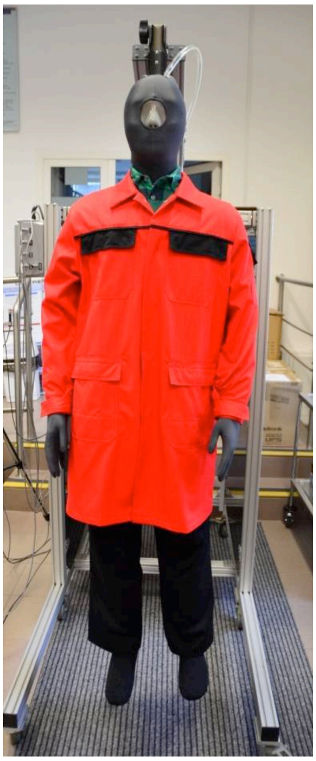


Fig. 18. Picture of manikin dressed in in prototype of the system for measuring undergarment temperature and relative humidity with data logging and wireless data transmission

The test was conducted during 420 min. Using developed system temperature and relative humidity between the surface of the manikin and underwear) has been measured and recorded at an interval of 2 s and then sent to the computer. Measurements started after manikin reached thermal balance state.

Tests with volunteers. The aim of the tests with five volunteers was to assess the accuracy of the measurement as well as ergonomics of use of the system prototype and accuracy of the data acquisition and transmission in the real use conditions. In this paper the accuracy of the measurement of temperature and relative humidity on volunteers is not described. In tests the volunteers at age of 26 dressed the system on and off, walked and rode the bicycle and then completed questionnaire in which they assessed the system functionality, ease of dressing the system, if the software of Data Logger is user- friendly, mechanical effect of the sensors on the volunteers skin, the limitations of the movements, and the mass of the system.

4.4. RESULTS AND DISCUSSION

Tests on the thermal manikin. In each of two test series, the undergarment temperature and relative humidity measurement results obtained using the developed system were divided in two series and each series in six 10 min. intervals. Values from each time interval were averaged and standard deviation calculated. Average values in two series for each of seven sensors with their standard deviation are presented in tables 3 and 4.

Tab. 3. Average test results of 6 undergarment temperature measurements using developed system on thermal manikin, in two series with their standard deviation.

Test results	**Number of sensors**													
	C1		**C2**		**C3**		**C4**		**C5**		**C6**		**C8**	
	Number of series													
	1	2	1	2	1	2	1	2	1	2	1	2	1	2
Average of six measurements	37,2	37,2	36,6	36,3	38,8	39,6	35,1	35,2	36,9	37,1	35,3	34,6	37,3	36,5
Standard deviation	0,19	0,09	0,13	0,05	0,14	0,05	0,17	0,04	0,29	0,12	0,17	0,04	0,15	0,06

Tab. 4. Average test results of 6 undergarment relative humidity measurements using developed system on thermal manikin, in two series with their standard deviation

Test results	**Number of sensor**													
	C1		**C2**		**C3**		**C4**		**C5**		**C6**		**C7**	
	Number of series													
	1	2	1	2	1	2	1	2	1	2	1	2	1	2
Average of six measurement s	32,9	32,9	33,4	33,5	32,6	32,3	34,1	33,9	33,5	33,3	33,6	34,1	33,3	33,7
Standard deviation	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,00	0,01	0,01	0,03	0,01	0,02	0,01

Exemplary results representative for measurement using sensors C1, C2, C3, C4, C5, C6, C8 for undergarment temperature and relative humidity are presented in Fig. 19 and Fig. 20 respectively.

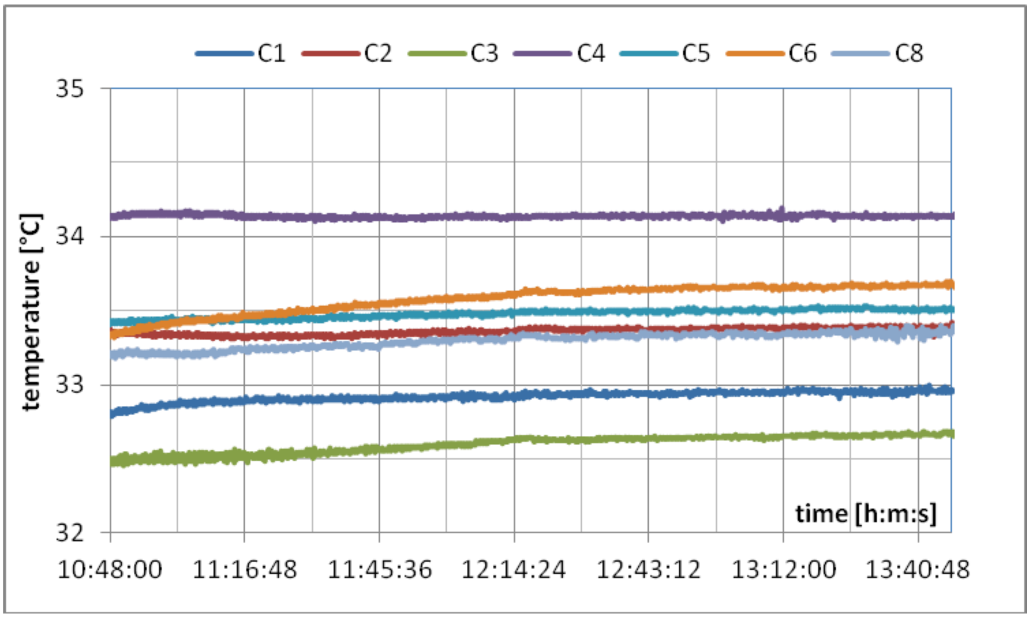


Fig. 19. Test results of undergarment temperature measurement using sensors C1, C2, C3, C4, C5, C6, C8 in time from 10:40 to 13:40.

According to the temperature distribution on a mannequin difference between the lowest and the highest temperature was 1,7°C. Concerning individual sensors their measurements were very stable.

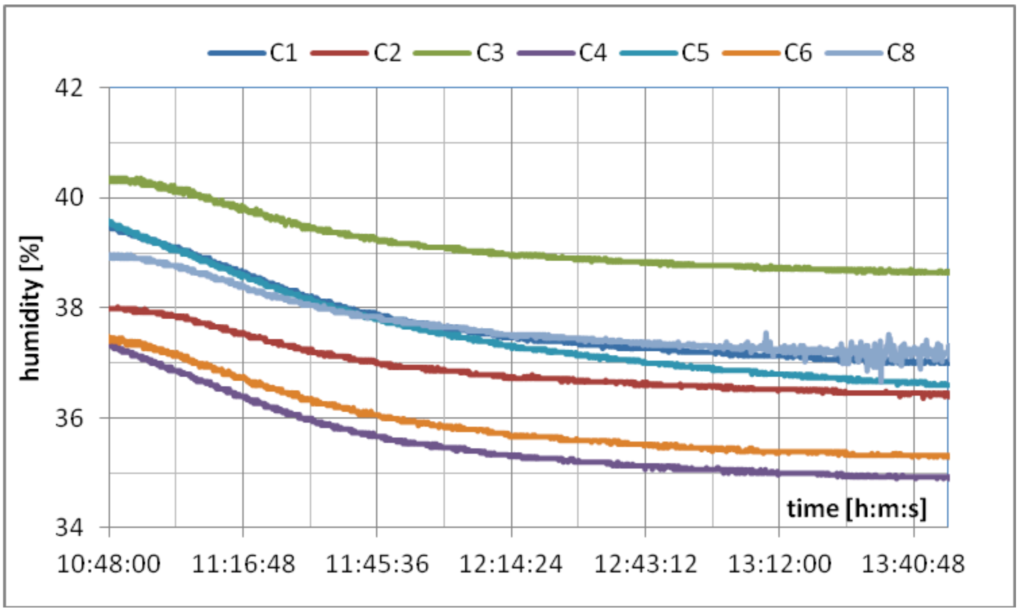


Fig. 20. Test results of undergarment relative humidity measurement using sensors C1, C2, C3, C4, C5, C6, C8 in time from 10:40 to 13:40

Analysing the results of tests on thermal mannequin in the scope of temperature and relative humidity measured using the developed system it was found:

- for the temperature difference between the average of the five values of the measurements for the first and second series of measurements for a given sensor is smaller than the uncertainty of the measurements given by the manufacturer (0.3 ° C
- for measuring the relative humidity of the difference between the average of the five values of the measurements for the first and second series of measurements for a given sensor is smaller than the uncertainty of the measurements given by the manufacturer (2%),

For temperature and the relative humidity measurement very small standard deviation and small differences between the mean in two series were obtained. Based on the results of preliminary testing system on a mannequin in hot climates, it was found that the system works properly.

Tests with volunteers. Based on the analysis of research results (in the scope of assessment of usability, ergonomics, functionality of the prototype, it was found that the system for measuring undergarment temperature and relative humidity with data logging and wireless data transmission works correctly both in the laboratory and field tests.

With wireless data transmission system enables the measurement of physical parameters of undergarment microclimate in dynamic conditions, making it possible to assess the user's thermal comfort in tested clothing and evaluation of the measured parameters in real time. During the evaluation of the system prototype in ergonomic terms, including ease of use, it was found that tests with use of the developed prototype does not impede the performance of physical activities and does not cause discomfort. In addition, the software of Data Logger is intuitive and user friendly. Studies have confirmed the possibility of application of the system to evaluate the users thermal in tested clothing on the workplaces.

The developed test method of measurement of users thermal comfort with use of the described prototype may be complementary to the methodology of assessment of clothing based on determination of its thermal insulation on thermal manikin for the purpose of its selection to work environment. Determination of clothing thermal insulation on a static thermal mannequin and theoretical calculation of the effect of body movement and air movement on the users thermal comfort, may be not sufficient to take into account the real environment conditions, which can give more intensive effect than expected.

The developed system can be also used to assess the user's thermal comfort in special protective clothing as well as sport clothing in mountain conditions, at low ambient temperatures, during the operation of the wind, and for comparison of thermal comfort in various types of clothing. In addition, the system can be used by research institutes or by clothing manufacturers to assess the users thermal comfort, especially when developing new designs of clothing, including protective clothing or specialized sportswear made from advanced materials. Such studies as in workplaces, at low temperatures, with the effect of the wind, can be used to assess the clothing at the initial phase of preparing and designing prototypes of clothing in terms of the selection of a suitable material system.

The publication has been based on the results of Phase II of the National Programme "Safety and working conditions improvement", funded in the years 2011-2013 in the area of research and development works by the Ministry of Science and Higher Education. The Programme coordinator: Central Institute for Labour Protection – National Research Institute.

REFERENCES

[1]. Owczarek G., Gralewicz G., Kurczewska A., "Application of ICT to smart personal protective equipment for safety management in the working environment", presentation on Workingonsafety.net – 7th International Conference, October 2014, Scotland, UK

[2]. Mr. C. Wilson: Assesment of factors that influence the tensile strength of safety harnesses and lanyard webbings. HSL/2002/16.

[3]. Baszczyński K., Jachowicz M., Jabłońska A.: Opracowanie metodyki badań dla potrzeb szacowania dopuszczalnego okresu użytkowania uprzęży chroniących przed upadkiem z wysokości. Sprawozdanie z realizacji zadania 03.5, CIOP-PIB, 2006-2007.

[4]. Roy Watt. „RFID: klucz do automatyzacji świata", Świat Nauki, Nr 2(150),luty 2004.

[5]. Patrick J. Sweeney II. „RFID for Dummies". Wiley Publishing, Inc. 2005.

[6]. Manfred Helmus, Berit Offergeld, "Radio-frequency identification opens up new possibilities in occupational health and safety", KANBrief 3|07.

[7]. E. Walk, D. Buth, Michale. Desch, M. Rodig, F. Neubauer, A. Gauby, A. Hoisl Final Report. Work package 3. "RFID Standards and Radio Regulations". July 25, 2008

[8]. Robert Plum, "The use of auto ID systems for data acquisition: intelligent PPE", KANBrief 3|11.

[9]. www.integer-solutions.com.

[10]. Caudell, T.P. Mizell, D.W. Res. & Technol., Boeing Comput. Services, Seattle, WA, Augmented reality: an application of heads-up display, Print ISBN: 0-8186-2420-5;

[11]. Fundamentals of wearable computer and augmented reality. Edited by Woodrow Barfield and Thomas Caudell, Lawerence Erlabum Associaes, 2001;

[12]. Raport z realizacji zadania badawczego 1.A.06: Badanie percepcji wizualnych sygnałów ostrzegawczych generowanych metodą rzeczywistości wzbogaconej celem ich optymalizacji, CIOP-PIB, Warszawa, 2004

[13]. Dźwiarek M. Holejko K., Nowak R., Czrnecki T.: Koncepcja urządzenia ostrzegawczego z wykorzystaniem systemu rzeczywistości wzbogaconej, Pomiary Automatyka Robotyka 3/2005, str. 6 – 9

[14]. Reinhart, G., A camera-based support system with augmented reality functions for manual tasks in radioactive production environments, Production Engineering Volume: 2, Issue: 2, June 2008, pp. 139 – 147

[15]. Anastassova, Margarita; Burkhardt, Jean-Marie, Automotive technicians' training as a community-of-practice: Implications for the design of an augmented reality teaching aid, Applied Ergonomics Volume: 40, Issue: 4, July, 2009, pp. 713-721

[16]. Reinhart, G., A camera-based support system with augmented reality functions for manual tasks in radioactive production environments, Production Engineering Volume: 2, Issue: 2, June 2008, pp. 139 - 147

[17]. Nicolau, S.A.; Pennec, X.; Soler, L.; Buy, X.; Gangi, A.; Ayache, N.; Marescaux, J., An augmented reality system for liver thermal ablation: Design and evaluation on clinical cases, Medical Image Analysis Volume: 13, Issue: 3, June, 2009, pp. 494-506

[18]. Mischkowski, Robert A.; Zinser, Max J.; Kübler, Alexander C.; Krug, Barbara; Seifert, Ulrich; et. Al, Application of an augmented reality tool for maxillary positioning in orthognathic surgery – A feasibility study, Journal of Cranio-Maxillofacial Surgery Volume: 34, Issue: 8, December, 2006, pp. 478-483

[19]. Bezpieczeństwo I higiena pracy pod redakcją D. Koradeckiej, CIOP-PIB, Warszawa 2009

[20]. Karpowicz J., Gryz K., Zagrożenia elektromagnetyczne przy produkcji wyrobów metalowych i dzialania prewencyjne, CIOP-PIB, Warszawa, 2009

[21]. R. Pakos, Z. Szefner, A. Sajek: Systemy kontroli jakości w spawalnictwie, Materiały Politechniki Szczecińskiej, Szczecin 2004

[22]. Dyrektywa Directive 89/686/EEC on personal protective equipment

[23]. Holmer, I., Protective Clothing and heat stress, Ergonomics, 38 (1), 1995, pp. 166-182

[24]. Holmer, I., Protective clothing in hot environments, Industrial Health, 44,2006, 404-413,

[25]. Marszałek, A., Bartkowiak, G. and Łężak K. Physiological Effects of a Modification of Impermeable Protective Clothing Construction, International Journal of Occupational Safety and Ergonomice (JOSE), Vol. 15, No 1, 2009, 61-73,],

[26]. Source: Agnieszka Kurczewska, Jarosław Dąbkiewicz

[27]. Havenith G., Holmer I., Parsons K., Personal factors in thermal comfort assessment: clothing properties and metabolic heat production, Energy and Buildings, 34, 581-591, 2002

[28]. A. Kurczewska, A. Marszałek, M.Okrasa, B. Włodarczyk, Nowy system do pomiaru temperatury i wilgotności w przestrzeni pododzieżowej z rejestracją i bezprzewodową transmisją danych, Przegląd Włókienniczy - Włókno, Odzież, Skóra, 2014-4

A Study of Main Safety-Related Functions Available to Collaborative Robotics

Adel Sghaier [a], Sabrina Jocelyn[b], Damien Burlet-Vienney[b] and Laurent Giraud[b]

[a]Institut National de Recherche et de Sécurité (INRS)
1, rue du Morvan – CS 60027
F-54519 Vandoeuvre Cedex
[b]Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST)
505, boul. de Maisonneuve Ouest
Montréal (Québec) H3A 3C2

Abstract

Significant developments in robotics and protective device technologies have benefited the field of work equipment. As a result, a new type of machine has appeared in industry: collaborative robots, or "cobots". Standard EN ISO 10218:2011 *respecting industrial robots reflects these developments and specifies requirements for the safe integration of cobots into workstations. Under certain conditions, the operator can enter into the cobot workspace of such a workstation during production, which can be hazardous to the operator's safety. The proximity of the cobot to the operator creates new risks not associated with conventional robotic cells. Robot manufacturers offer technical solutions to the problems of ensuring safe human-cobot collaboration in the form of electronic boards or software modules. With these solutions, appropriate safety-related functions can be implemented to reduce the risks stemming from the operator and the cobot sharing the same workspace. This paper presents a theoretical study that consisted in identifying and analysing the main safety-related functions offered by three cobot manufacturers. Generic families of safety-related functions are identified and recommendations are made to help cobot users and integrators ensure the safety and health of operators.*

Keywords:

robotics, collaborative robot, cobot, safety function

Introduction

Technological and standards-related developments helped the emergence of a new field in industrial robotics: collaborative robotic cells. In this new approach, the operator is allowed, under certain conditions during the production phase, to enter into the robot's workspace in order to carry out operations in collaboration with it. The proximity of the operator and robot arising out of this collaboration creates new risks [1]. The 2011 version of standard *EN ISO 10218* (parts 1 and 2) [2, 3] sets out safety requirements for industrial robots including collaborative operation. As these requirements generally involve use of the control system, they entail the implementation of safety functions. Robot manufacturers are now proposing technical solutions in the form of safety-related modules or boards that enable the implementation of a number of safety functions that are useful for robotic collaborative operation. However, the complexity of the documentation and a lack of experience with this technology constitute major difficulties for integrators and users when implementing collaborative cells.

The work described in this paper is part of a study intended to (1) equip integrators to design collaborative robotic cells and (2) issue safety warnings and identify difficulties needing special vigilance. Providing integrators with this assistance requires conducting an in-depth study of the safety-related functions offered by manufacturers in order to determine the specific technical characteristics that can affect safety. This paper presents a study of the safety-related functions of three robot manufacturers that can be used for implementing collaborative cells.

Method

The main goal of the research presented in this paper was to identify the most common safety-related functions and characterize the specific technical implementation features of these functions. For this purpose, a study of the safety-related functions offered by a sample of robot manufacturers was conducted. The study was based mainly on technical documentation and information obtained from the manufacturers. Three manufacturers were selected for the study on the basis of industry representivity. Only manufacturers that offer collaborative robotics solutions commonly used in industry were chosen. Two manufacturers were studied by the IRSST, while a third was examined by the INRS. For confidentiality reasons, the manufacturers' names have intentionally been omitted from this paper.

The study of the safety-related functions involved several stages:

- **Definitions and detailed specifications**. This stage consisted in (1) identifying the safety-related functions offered by each of the three manufacturers; (2) separating out the collaboration-related functions from the others; (3) cataloguing the technical specifications of each safety-related function in order to reconstitute the theoretical functional chain. This made it possible to highlight, for each manufacturer, the technical differences that may exist between safety-related function names, specifications and uses.
- **Study of whether needs are adequately met**. The specifications and capacities of the functions were compared with the safety needs and requirements described in standard *EN ISO 10218-1*. The purpose was to determine whether the various functions available would enable implementation of the four modes described in the standard.
- **Classification of safety-related functions (SRF)**. The manufacturers offer safety-related functions that can play a variety of roles in collaborative cell safety. They were classified into three generic families based on their functional similarities:
  - Stop SRF. Safety-related functions that cause the robot to stop, with or without removal of power, as a result of an external control, a failure or a fault (e.g., deceleration noncompliant with braking ramp)
  - Monitoring SRF. Safety-related functions that monitor certain robot characteristics to keep the robot stopped with power available or to prevent the characteristics from exceeding preset values (limit violation)
  - General SRF. Safety-related functions that are neither stop-related nor monitoring-related (e.g., brake periodic check)
- **Study of implementation on example cell**. To illustrate the use of the different safety-related functions as an integrator could do, we designed a representative example of a collaborative cell. This cell is a theoretical example that aims to integrate some safety-related functions. Its purpose was not to consider all the risks inherent in human-robot collaboration, but to illustrate the method of using and combining safety-related functions.

Note 1. *In this study we did not favour any manufacturer over another. Our sole aim was to analyse the safety-related functions available on the safety-related electronic boards or modules of the robots studied, in order to be able to provide guidelines for cobot integrators.*

This paper includes an example illustrating the collaborative cell integration process. However, the example does not take into consideration all the risks to which people nearby are exposed, such as the risks created when a person enters the cell. As a result, not all the associated risk-reduction measures are covered.

Results

Table 1 presents the configuration and general specifications of the three robots studied. Data on robot performance and installation are specified. The sample provides an illustration of the different approaches to achieving a collaborative state (e.g., type of robot, integration of controller and safety-related module).

Table 2 presents the safety-related functions of the three robots that the research team identified as contributing to implementing one or more of the four modes of collaborative operation (as described in [2]):

1. Safety-rated monitored stop
2. Hand guiding
3. Speed and separation monitoring
4. Power and force limiting by inherent design or control

These safety-related functions are processed in the safety-related board or module of each robot. The assignment of each of these functions to a specific mode of collaboration was based on our own analysis.

Table 3 shows how safety-related functions offered by the manufacturers can be categorized according to the proposed generic classification.

Table 1 – Configuration and general specifications of the three robots studied

	Robot #1	Robot #2	Robot #3
Type of robot	Designed as collaborative	Conventional converted to collaborative	Conventional converted to collaborative
Number of axis	6	6	6
Payload	>3 kg	>3 kg	>15 kg
Reach	>700 mm	>800 mm	>1,000 mm
Max. speed (axis)	>170°/s	>710°/s	>330°/s
Controller	Robot-dedicated	Uses a compatible controller	Robot-dedicated
Safety-related module/board	Part of original design	To be integrated	To be integrated
SRF compliance (*EN ISO 13849-1:2008* or *IEC 62061:2005*)	Category 3, PLd	– Category 4, PLe: Emergency stop, pendant – Category 3, PLd: Other	Category 3, PLd
Access and changes to safety settings	Password required to authorize changes to safety configuration (position, speed and force limit settings, etc.).		
CE marking (2006/42/EC)	Declaration of incorporation	None	Declaration of incorporation

Table 2 – List of safety-related functions (SRF) by robot and their contribution to human-robot modes of collaboration (✓: contributes, ✗: does not contribute)

			Mode of collaborative operation (*EN ISO 10218-1*)			
		SRF, by manufacturer, available to implement mode of collaboration	**#1**	**#2**	**#3**	**#4**
Robot #1	1	Protective stop (category 2 stop)[1]	✓	✗	✗	✗
	2	Reinitialization following protective stop	✓	✗	✗	✗
	3	Stop monitoring	✓	✗	✗	✗
	4	Tool centre point position limiting	✗	✗	✓	✗
	5	Joint position limiting	✗	✗	✓	✗
	6	Joint speed limiting	✗	✓	✓	✓
	7	Tool centre point speed limiting	✗	✓	✓	✓
	8	Separation monitoring: configurable function, but unavailable as is on the robot	✗	✗	✓	✗
	9	Tool centre point force limiting	✗	✗	✗	✓
	10	Momentum limiting	✗	✗	✗	✓
	11	Power limiting	✗	✗	✗	✓
Robot #2	1	Tool centre point or flange speed limiting	✓	✗	✓	✓
	2	Axis position limiting	✗	✗	✓	✗
	3	Axis speed limiting	✗	✓	✓	✓
	4	Tool centre point or flange position limiting	✗	✗	✓	✗
Robot #3	1	Safe deceleration ramp	✓	✗	✗	✗
	2	Safe stop function	✓	✗	✗	✗
	3	Safe stop function passive monitoring	✓	✗	✗	✗
	4	Axis speed active monitoring	✗	✓	✓	✓
	5	Tool speed active monitoring	✗	✓	✓	✓
	6	Axis angle passive monitoring	✗	✗	✓	✗
	7	Tool space passive monitoring	✗	✗	✓	✗
	8	Axis angle active monitoring	✗	✗	✓	✗
	9	Tool space active monitoring	✗	✗	✓	✗

[1] For stop categories see note 2.

Table 3 – Classification of generic safety-related functions (SRF) found in ISO 10218-1 *and* 2:2011 *respecting human-robot collaboration and those found on the robots studied (✓: SRF present, ×: SRF absent, +: input safeguarding device needs to be added, ?: information not found in documentation)*

Generic SRF families	**Generic names of SRFs**	**Robot #1**	**Robot #2**	**Robot #3**
Stop SRF	Emergency stop	✓	✓	✓
	Safety-rated monitored stop (mode 1)			
	Protective stop (cat. 0)	✓	✓	✓
	Protective stop (cat. 1)	×	✓	✓
	Protective stop (cat. 2)	✓	×	×
	Monitoring of deceleration for cat. 1 or 2 stops	✓	✓	✓
	Hand guiding (mode 2)			
	Emergency stop from hand-guiding equipment	×	×	×
Monitoring SRF	**Safety-rated monitored stop (mode 1)**			
	Monitoring of zero speed of robot	✓	✓	✓
	Monitoring of fixed position of robot	✓	✓	✓
	Hand guiding (mode 2)			
	Monitoring of robot speed < Speed limit	✓	✓	✓
	Speed and separation monitoring (mode 3)			
	Monitoring of robot speed < Speed limit	✓	✓	✓
	Monitoring of robot position	✓	✓	✓
	Power and force limiting by inherent design or control (mode 4)			
	Monitoring of force < Force limit	✓	×	×
	Monitoring of power < Power limit	✓	×	×
General SRF	Deliberate reset from outside the collaborative workspace following a protective stop	✓+	?	?
	Software synchronization	✓	✓	✓
	Brake periodic check	?	?	✓
	Safety-rated monitored stop (mode 1)			
	Detection of presence of an operator in collaborative workspace	✓+	✓+	✓+
	Hand guiding (mode 2)			
	Hold-to-run control operated from equipment's enabling device (releasing the control causes a safety-rated monitored stop)	×	×	×
	Speed and separation monitoring (mode 3)			
	Detection of position of operator in collaborative workspace	✓+	✓+	✓+

Note 2. Standard *IEC 60204-1:2005+A1:2008* [4] defines category 0, 1 and 2 stops as follows (section 9.2.2 – Stop functions):
stop category 0 (cat. 0): *stopping by immediate removal of power to the machine actuators (i.e. an uncontrolled stop – see 3.56)*.
stop category 1 (cat. 1): *a controlled stop (see 3.11) with power available to the machine actuators to achieve the stop and then removal of power when the stop is achieved*.
stop category 2 (cat. 2): *a controlled stop with power left available to the machine actuators*.

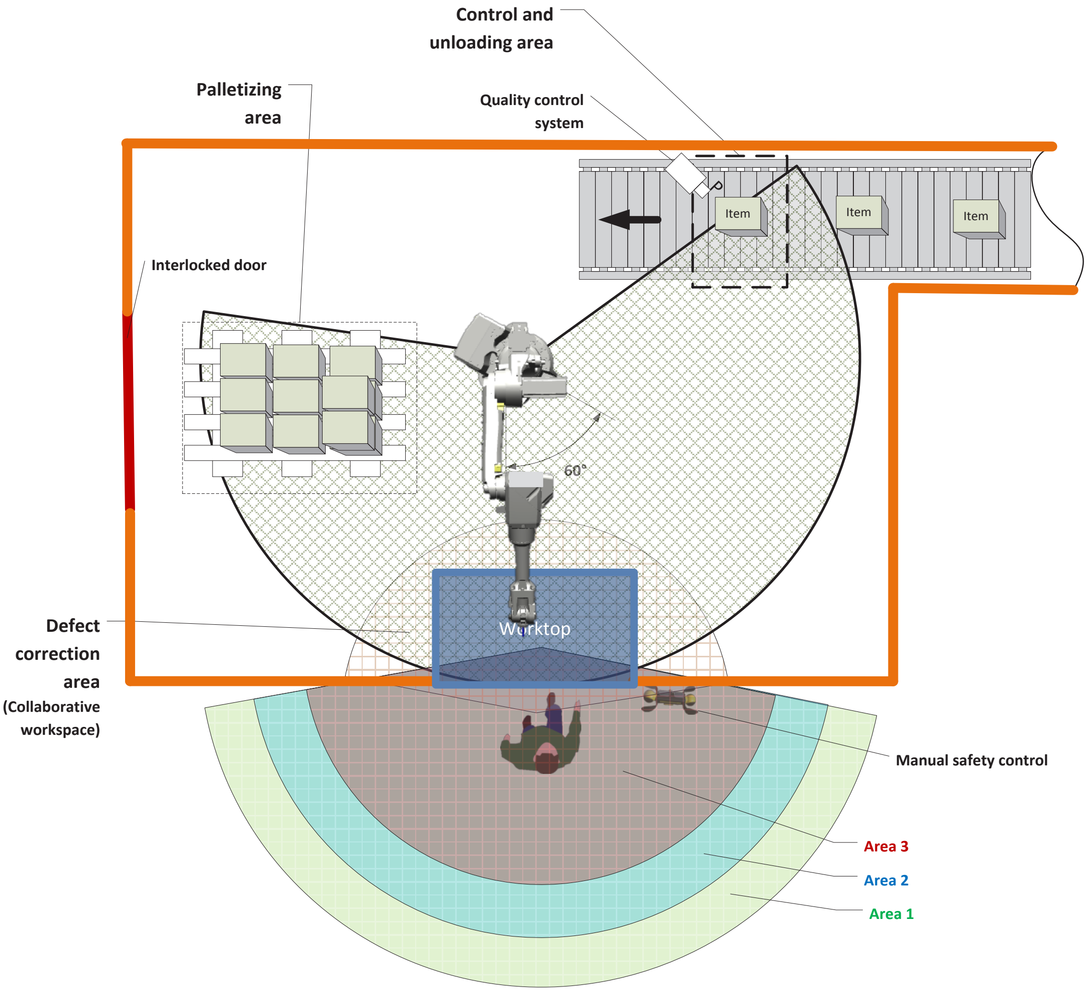


Figure 1 – Example of collaborative cell

Example of Implementation of a Collaborative Robotic Cell

To illustrate how the safety-related functions offered by the manufacturers can be used in the integration process, we designed an example of collaborative cell implementation. This collaborative cell served as a common example for the different manufacturers.

Implementation of a collaborative cell requires different design steps described in the 2010 version of standard *EN ISO 12100* [5]. Following these steps involves adopting an iterative risk-reduction process. As part of implementing the collaborative cell example described below, we assume that the integrator has followed the general design principles described in the standard and, in particular, has gone through the following steps:

- Draw up specifications
- Carry out risk assessment, taking into account tasks planned for the cell
- Choose the combination or combinations of modes of collaborative operations required for the application
- Define the safeguards suggested by the risk assessment and dictated by the safety requirements of standard *EN ISO 10218-1:2011* regarding the chosen modes of collaboration

- Knowing that the safeguards involve use of the control system:
  - Define the safety functions
  - Determine the performance level for each safety function
- Ensure that the safety-related functions available on the manufacturer's boards or modules are adequate to meet the real needs of the application. If safety-related functions are not present in the boards or modules, implement them by external means (e.g., safety-related controller)

The illustrative example we propose concerns a quality control and palletizing workcell (Figure 1). The planned role of this workstation is to perform automatic quality control of items moved mechanically toward a robotic palletizing station. If a defect is found, a manual corrective operation is required before palletization. This defect correction operation requires the robot to hold the item still while the operator acts. This last stage is considered as the collaborative operation.

The robotic cell given as an example consists of three workstations:

1. **A control and unloading area.** This workstation is equipped with a sensor which can detect the presence of an item in order to command the stop of the conveyor. It is also equipped with an item quality control system (visual inspection, for instance).
2. **A palletizing area**. Initially the pallet at this station is empty. It is gradually filled as the items are moved by the robot from the unloading station.
3. **A defect correction area**. This is a collaborative workstation. In some cases, an operator can manually correct the defects in the item (e.g., secure a missing screw) while the robot holds it still. In other cases, the item is removed by the operator.

It is assumed that the first design step (specifications) performed by the integrator leads to the following choices:

- If there are no defects, the robot takes an item from the unloading station and moves it to the palletizing station according to a predefined order (in order to form a full pallet). During this operation, the conveyor stops whenever the following item is at the control and unloading workstation. It remains stopped while waiting for the next operation.
- When a defective item is detected at the quality control and unloading station, the conveyor stops and waits for the robot to move the item to the defect correction station.
- In the case of a defect, the robot picks up the defective item from the conveyor and takes it to the collaborative workstation so that the operator can perform manual operations on it. During this phase, the conveyor brings another item to the quality control and unloading station, and then waits while the defect is being corrected and the palletizing operation is completed.
- During the manual defect correction operation (collaborative operation), the robot is in safe stop mode and keeps hold of the item.
- The end of the defect correction operation is confirmed by the operator by means of an actuating control. Once the operator has left area 3, the robot moves the corrected item to the palletizing station and then resumes its normal cycle.
- In whatever phase the robot is, when the operator approaches the collaborative work area, an audible signal is triggered if the operator is in area 1, then the robot goes into reduced-speed mode (if it is moving) when the operator moves in area 2, and the robot goes into safe stop mode when the operator enters area 3.
- If the operator is in area 3 and the robot has not completed its trajectory to move an item to the collaborative workspace, the operator has a two-hand enabling device to allow the robot to complete its trajectory at reduced speed.
- If the operator decides that the defect in the item cannot be corrected, he or she pushes a button to release the item so that it can manually be removed from the palletizing process. The robot automatically returns to the control station after the operator has validated this operation and has left area 3 (the robot does not go through the palletizing step in this case).

The risk assessment for this cell prompted us to choose a combination of two modes of collaboration described in standard *EN ISO 10218-1: "s*afety-rated monitored stop" and "speed and separation monitoring". This led to the choice of the following safeguards:

- A laser scanner to detect the proximity of the operator to the collaborative workstation.
- A sliding door equipped with an interlock with guard locking. This door is used to secure the entrance to the palletizing area while a collaborative task is undertaken.

- A two-hand enabling device (hold-to-run control) to control the robot manually from the collaborative workstation.

The safeguards described above make use of the control system by means of safety functions (association of safety-related functions). These safety functions are implemented using, among other devices (e.g. safety input components), the safety-related electronic boards or modules provided by the manufacturers. Table 4 presents the safety-related functions from the electronic board or module of each robot that enable implementing the safety functions. Those functions are defined as follows:

- **F1**. Function to reduce speed of robot when operator approaches in area 2
- **F2**. Function to stop robot for collaborative operation (cat. 2 stop): Stop robot when operator is in area 3
- **F3**. Two-hand (hold-to-run) control of robot: move robot at reduced speed pressing the two-hand control, even when operator is in area 3
- **F4**. Cat. 0 or 1 protective stop function triggered by interlock with guard locking device on sliding door
- **F5**. Manual reset function following triggering of interlock with guard locking
- **F6**. Function to release item by pushing a button accessible in area 3

Table 4 – Implementation of safety functions according to the different manufacturers studied

	Robot #1	**Robot #2**	**Robot #3**
F1	Joint speed limiting and/or Tool centre point speed limiting	Axis speed limiting and/or Tool centre point speed limitiing	Axis speed active monitoring and/or Tool speed active monitoring
F2	Protective stop + Stop monitoring + Reinitialization following protective stop	Safe stop	Safe deceleration ramp + Safe stop
F3	Reinitialization following protective stop + Joint speed limiting and/or Tool centre point speed limiting	Axis speed limiting and/or Tool centre point speed limiting	Axis speed active monitoring and/or tool speed active monitoring + Manual control
F4	Protective stop (cat. 0 or 1)	Protective stop (cat. 0 or 1)	Stop (cat. 0 or 1)
F5	Reinitialization following protective stop	External reset	External reset
F6	Protective stop + Tool centre point position limiting	Safe stop + Tool centre point or flange position limiting	Safe stop + Manual control

Discussion

General Specifications

Table 1 distinguishes between robots that are inherently collaborative by design and conventional robots that have been converted to perform collaborative operations. For instance, it can be seen that the joints maximum speed of the robot, that is collaborative by design, is far lower than the joints maximum speeds of the two other robots. The design of this robot is dedicated to collaborative operations, which helps reduce the risks. Similarly, the collaboration-dedicated software modules or electronic boards are integrated into the robot controller by design, limiting the adjustments required and the possibility of error during integration.

Furthermore, it should be noted that manufacturers often exaggerate when using the term “safety” to describe safety-related software modules and electronic boards they market. In reality, those modules and boards can be considered only as a part of the safety since one or more SRFs must be completed by the integrator to meet criteria that bring the system up to the required performance level. It would therefore be more accurate to talk about safety-related modules or boards. The concept of an integrated SRF or of an SRF that needs to be parameterized is discussed in greater detail below.

Lastly, manufacturers consider collaborative robots to be partly completed machinery. According to the user manuals, the integrator is responsible for conducting an appropriate risk assessment and for complying with applicable machinery regulation[2] and standards. However, for partly completed machinery, the manufacturer must always provide a declaration of incorporation (Directive on Machinery, art. 13) [6]. The technical documentation of robots #1 and #3 clearly shows a declaration of incorporation related to the Directive on Machinery.

Modes of Collaboration

It can be seen from Table 3 that the safety-related functions that contribute the most to the implementation of collaboration modes are the monitoring SRF family. Table 3 also shows the generic safety functions according to *ISO 10218* part 1 [2] and part 2 [3] safety requirements. Table 2, on the other hand, lists the safety-related functions found on a robot and the modes of collaboration in which they can be involved. A comparison of the two tables reveals that the Table 2 safety-related functions consist essentially of stop functions and speed, position, force and power monitoring functions. However, the fact that one or more safety-related functions are available for implementing a mode of collaborative operation does not mean that this mode is fully configured on the robot from the outset. Some safety-related functions may be fully implemented on the safety-related electronic board or module and meet the minimum performance level required ("PL$_r$ d," according to standard *ISO 10218-1*). This is the case of the emergency stop functions in our study. Other safety-related functions need to be parameterized (e.g., specify speed or position limits) or input or output component needs to be added (e.g., a light curtain to detect a presence in the collaborative workspace, or a force sensor). The processing part of these functions is already available on the safety-related boards or modules and meets the performance level required. The integrator is responsible for maintaining the performance level of the safety-related function available on the safey-related board or module by choosing an appropriately reliable input or output component. The performance levels stated for cobot safety-related functions are often levels that are attainable, but not implemented at the outset. The stated performance levels are rarely associated with a complete safety function; in many cases, they concern only the processing part of the function. To build a complete safety function, the integrator needs genarally to combine several safety-related functions offered by manufacturers safety-related boards or modules and he also could use external components or devices (as shown in figure 2). The integrator is therefore responsible of maintaining the performance level of the whole safety function.

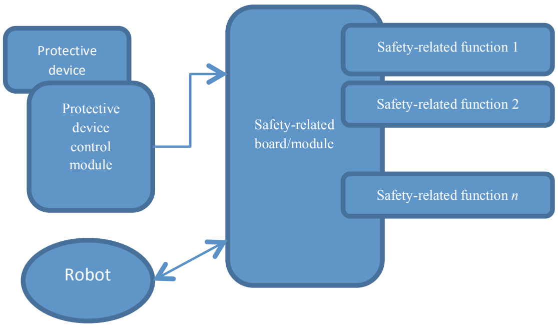

Protective device
Protective device control module
Safety-related board/module
Safety-related function 1
Safety-related function 2
Safety-related function *n*
Robot

Figure 2 – Implementation of a safety function in general

To implement collaboration mode 1 in accordance with *ISO 10218-1:2011* [2], the collaborative robot cell must be able to detect the operator's presence in the collaborative workspace. For robot #1, detection is signalled by the protective device to be installed at the input of the protective stop safety-related function. In the case of robot #2, detection is implemented by means of an enclosure safeguard sensor. For robot #3, a presence in the collaborative workspace is detected by an external detection device connected to the safety-related board. Under the standard, this detection must stop the robot by triggering a protective stop or a cat. 2 stop. In our case, robot #1 does a cat. 2 stop, while robots #2 and #3 do a cat. 1 stop.

Standard *ISO 10218-1* stipulates that for mode 1, any violation (unintended motion or failure) of the deceleration ramp when braking shall result in a cat. 0 stop. This condition is met by all three robots studied. For modes 2 to 4, any violation of the speed or position limit shall, under the standard, generate a protective stop. Section 5.5.3 of the standard stipulates that this stop shall be at least cat. 0 or 1; an additional cat. 2 stop may also be implemented. For modes 2 to 4 in our case, any limit violation causes a cat. 0 stop for robots #1 and #2. For robot #3, it will cause a cat. 0 or 1 protective stop, depending on the configuration chosen at the time of installation.

For mode 2, it can be seen that the only functions available on the three robots are the speed-limiting functions. To satisfy this mode, the following capabilities are missing: the hand-guiding equipment placed near the robot end-effector, as well as the emergency stop and enabling device available on this equipment. An integrator who wishes to install this mode, like any other mode, must ensure that the robot has all the technical capabilities required to host the mode in question.

[2] In Europe, the applicable regulation is directive 2006/42/EC, Directive on Machinery.

Regarding mode 3, all the robots studied have speed-limiting functions for maintaining a safe estimated speed. They also include position-limiting functions that help maintain a certain separation between the robot and the operator. A protective device (e.g., position sensor) for real-time calculation of this separation must be installed and configured in order to implement this mode fully.

Caution must be exercised, however: even if the robots studied can be called collaborative, the speeds they can reach can be hazardous to the safety of their operators. A risk assessment must suggest the appropriate value for the speed, and that value must be restricted and protected from being changed without authorization (hence the need for passwords, mentioned in Table 1). For instance, for robot #3, the (theoretical) configurable speed is greater than 330 °/s for the rotational axis and about 10 m/s for the linear axis. These extreme values seem to be incompatible with collaborative work. It is therefore necessary to exercise vigilance when specifying speeds, so as to remain within ranges compatible with the risk assessment.

With regard to mode 4, the speed-limiting functions contribute to implementing this mode, as by limiting the speed, the kinetic energy released in a human-robot collision, i.e., the power, is also limited. However, the lack of force sensors on robots #2 and #3 makes it impossible to satisfy this mode. In the case of robot #2, the only place where a force sensor could be installed would be at the Tool Center Point (TCP). Thus, the robot will not be stopped following sufficient contact with a human if the person comes into contact with a part of the robot other than the TCP. In the case of robot #1, the faster it moves, the harder it is to stop it with a body part, even if it has safety-related functions other than "speed" allowing power and force to be controlled. The chances of stopping this robot when it is operating at full speed are reduced if it comes into contact with an immobile or slow-moving operator. On the other hand, it is one of the lightest robots, with soft shapes (no sharp edges), so any potential injury is limited intrinsically by the design.[3]

Table 3's General SRF family and the case study show that the integration of a collaborative robotic cell is a complex undertaking. The complexity is due to, among other things, the lack of information (the "?" of Table 3) and the nesting of one mode of collaboration within another (e.g., mode 1 actuated when the enabling handle is released in hand-guiding mode).

Implementation of a Collaborative Cell

One of the main remarks that can be made regarding the implementation of an example collaborative cell is that implementing the complete chain of a safety function (e.g., slow the robot down when the operator is in area 2) may require the use of several functions present in safety-related modules or boards proposed by manufacturers.

The integrator must therefore remain vigilant and select the necessary combination of manufacturers functions, while at the same time paying close attention to possible incompatibilities between these functions. The integrator must keep in mind that a safety function is general and encompasses all elements that affect safety. For instance, the area-monitoring function mentioned earlier, besides making use of combinations of safety-related functions available on the safety-related boards or modules, also requires external elements like a laser scanner. The laser, besides having to meet performance level requirements, often involves use of a control module (PLC) that must be programmed or configured and connected to the safety-related board or module. A safety function must therefore be considered from a very broad perspective.

As was pointed out earlier, the integrator must make an appropriate, informed decision when choosing the external devices (e.g., protective devices) compatible with the general safety function to be implemented. If the function to slow down the robot when the operator is in area 2 is considered to be a safety function, the detection device used must have two detection areas (areas 2 and 3 in the example) compatible with the safety performance level required for collaborative robotics, i.e., "PL_r d." (If the scanner cannot satisfy this condition, another protective device, such as a pressure-sensitive safety mat, must be considered.)

Conclusion

In this paper, we have surveyed three robot from different manufacturers and examined the safety-related functions they offer for implementing collaborative robotic cells. In classifying the functions, we found that most of them fall into two categories: stop functions and monitoring functions. Although the safety-related functions offered by different manufacturers have similarities, there are a number of technical differences between them. These

[3] Note that even though this mode is offered by the manufacturers, implementing it is not possible at this point. In fact, the lack of information about ergonomical and psychological consequences of human-robot contact makes this mode of collaboration very difficult to implement.

technical differences can have repercussions on safety. Vigilance is therefore required when choosing and implementing these functions. In addition, it is important to keep in mind that the implementation of the complete chain of a safety function may require the use of external programming components or devices and parameter-setting, as well as a combination of several board or module safety-related functions.

This research is the first step in our study. The second step will consist, on the one hand, in implementing an experimental collaborative cell in order to run through a concrete example of what an integrator has to do. The purpose of this exercise will be to identify the technical difficulties involved in implementing a collaborative robotic cell, with the aim of writing a guide for integrators. This implementation will be carried out by INRS researchers. On the other hand, we will be making on-site visits at the same time to learn how worker safety is taken into consideration during integration of collaborative robotic cells on the factory floor. These on-site visits will also allow us to document the risks to which workers are exposed when interacting with cobots in the factory, as well as the benefits of this technology. The on-site visits will be made by IRSST researchers.

References

[1] Charpentier, P., and A. Sghaier. – “Industrial Robotic: Accident analysis and Human-Robot Coactivity.” *Proceedings of the 7th international conference on the safety of industrial automated systems (SIAS)*, Montreal, Canada, October 11–12, 2012, 6 p.

[2] EN ISO 10218-1 – *Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots*. Paris: AFNOR, 2011, 43 p.

[3] EN ISO 10218-2 – *Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration*. Paris: AFNOR, 2011, 72 p.

[4] IEC 60204-1:2005+A1:2008 – *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*. Geneva, 2009, 244 p.

[5] ISO 12100 – *Safety of machinery – General principles for design – Risk assessment and risk reduction*. Geneva, 2010, 77 p.

[6] The European Parliament and the Council of the European Union. *Directive 2006/42/EC on machinery*. 2006.

[7] Fryman, J., and B. Matthias. “Safety of industrial robots: From conventional to collaborative applications.” *Proceedings of the 7th international conference on the safety of industrial automated systems (SIAS)*, Montreal, Canada, October 11–12, 2012, pp. 198–203.

Corresponding address

adel.sghaier@inrs.fr

SIAS 2015

8th INTERNATIONAL CONFERENCE ON THE SAFETY OF INDUSTRIAL AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

Session 2: Functional safety

PLCopen: contributing to the world via harmonized look and feel of safety functionalities

Eelco van der Wal

Managing Director PLCopen

Introduction

Safety gets more and more important and more and more complex. PLCopen together with its members provides solutions for this via harmonization of functionalities on an abstract level. With this we can start solving the problems facing us in cooperation of man and robot.

Keywords:

PLCopen, Safety, Motion Control

Examples from the motion control area

There are many changes going on in the industrial machine market, mostly driven by new possibilities in the industrial controls. Servo technology makes mechatronic solutions possible, exchanging a master axis with multiple motors providing local functionalities. With this the mechanical solution is replaced by a software solution and the hard-wired solution with a distributed solution using digital networks. These multi-motor solutions often come with a digital network, of which most are nowadays based on Ethernet.

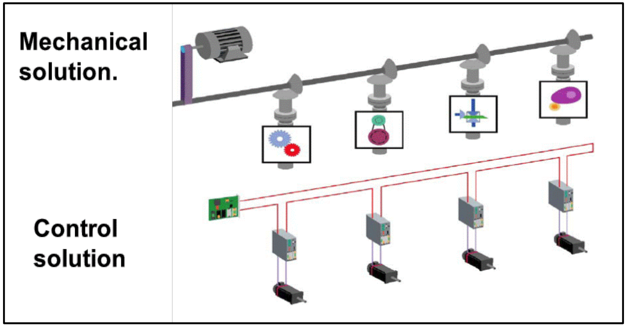


Figure 1: Mechatronic solutions moving to software

These solutions provide many advantages. One of the advantages is the flexibility to change profiles and timings in software. To make the software efficient, standardization is needed on multiple platforms, and abstraction of the underlying technology makes the application programs hardware independent.

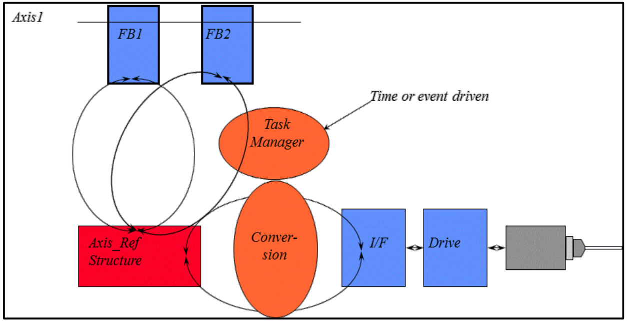


Figure 2: Abstraction via function blocks

Effect on safety

With the availability and acceptance of digital networks with safety functionality built-in, one inherently moves from hardwired safety functionalities to software solutions: the emergency function moves from a hardwired solution to a software solution via the network.
Via abstraction one can make the software independent from the hardware, supporting different platforms and (network) architectures with the same philosophy, reducing training and increasing reuse.

Further challenges

Additional forces facing the machine building industry include:

- The availability of many safety standards, including IEC 61508 and IEC 62061;
- Additional governmental requirements increasing the liability issues;
- The increasing importance of safety related issues regarding personnel and machines.

Solution as provided by PLCopen

The solution includes standardization of the safety functionality on the software level, and integrating this in the development environment. This combination helps developers to integrate safety related functionality with more ease in their systems, even from the beginning of the development cycle. Also, it contributes to the understanding of safety aspects, as well as to reducing the certification time and costs by relevant organizations.

Based on this, the international association PLCopen, together with its members, has specified the basic safety functions on the software level. In a later stage they have extended this to include specific application area like presses, where additional requirements need to be fulfilled.

The common basic requirements of a safety application for machine builders within all applicable safety standards are:

- Distinction between safety and non-safety functionalities;
- Use of applicable programming languages and language subsets;
- Use of validated software blocks;
- Use of applicable programming guidelines;
- Use of recognized error-reducing measures for the lifecycle of the safety-related software.

Example emergency stop

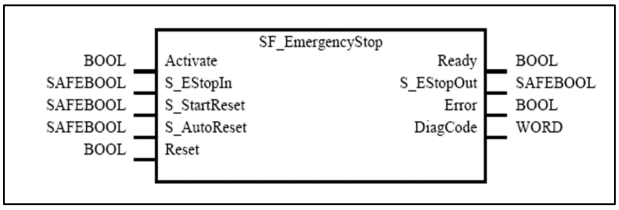


Figure 3: Example of the graphical representation of the emergency stop functionality

As an example we look at the functionality for the emergency stop. Above the graphical representation with the function block name on top, the inputs with corresponding datatype on the left, and the outputs on the right. Via the dedicated dataype SAFEBOOL a distinction between the safety application and the functional application is provided, reducing the functionalites for the safety application to the relveant ones, creating the safety program quicker and with less errors.

The emergency stop functionality in a small program with 2 motors is shown hereunder. First a normal stop functionality is done. If that one is not resulting in the stopping of the motors in the applicable time frame, the SafeStop functionality takes over. Of course one can create a dedciated stop functionality per motor, making it different from a mechanical master-axis approach.

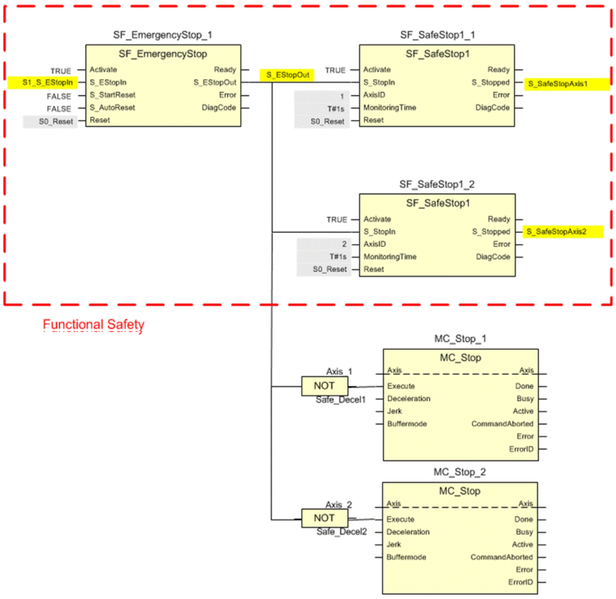


Figure 4: Example of a software program for emergency stop controlling two motors

Example for press applications

Presses can be very dangerous for the operating personnel so special safety functions have to be installed. To show the combination of the different functionalities, an example for a power press is shown hereunder. The press in the center is seen from the top.

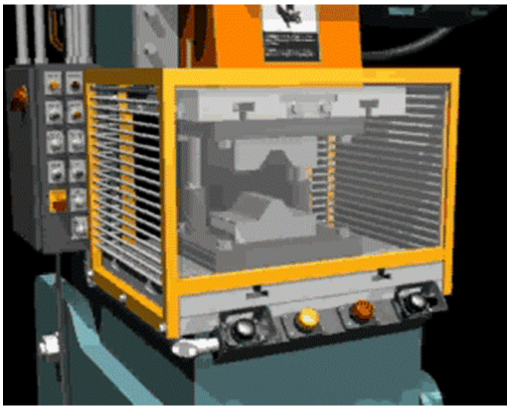


Figure 5a: Example of a press

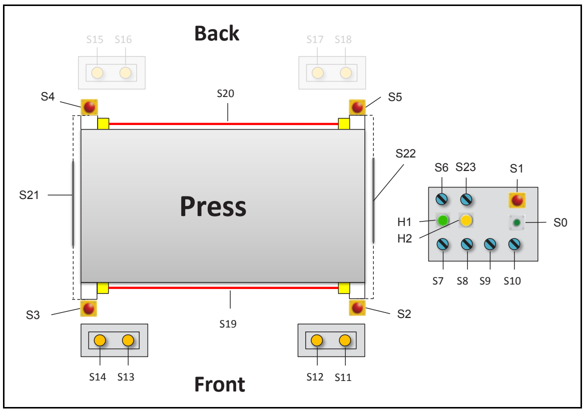


Figure 5b: and the related safety aspects with multi operator modes

The operator sides are on the top and bottom of the picture. They are protected by both two hand controls (S11-S18) and/or a light curtain (S19 and S20), one on the front side and back side. The two hand control devices are selectable.

Access from the left and the right side of the press are protected by interlocked guards (S21, S22)

On every corner of the press there is an emergency stop button installed.

The operator panel is located on a central position. It contains a mode-selector, and additional emergency stop functionality, the pre-selection for the 4 two-hand-control devices, and a switch for backward move. It also contains a reset button and two indicators (lamps) for status information.

This functionality can be programmed with the following defined functionalities, depending on the power source.

SF_EmergencyStop	SF_SingleValveMonitoring
SF_FootSwitch	SF_SingleValveCycleMonitoring
SF_ESPE	SF_DoubleValveMonitoring
SF_GuardLocking	SF_ValveGroupControl
SF_GuardMonitoring	SF_TwoHandMultiOperator
SF_Mode_Selector	SF_CamshaftMonitor
SF_TwoHandControlTypeIII	SF_CamMonitoring
SF_TwoHandControlTypeIIIC	SF_PressControl
SF_Cycle Control	

Overview of the applicable PLCopen Safety Function Blocks

With these canned functionalities the creation and certification of apllication programs goes much quicker and in a more transparetn way.

Future aspects

The next step will be focused to safe motion. This means not only harmonize the look and feel for the different function towards or in the drive, but also the motion of linked axes, e.g. in areas where the kinematics is involved, like in robotics. That extends the scope of the current functions to levels in line with Industry 4.0 and other initiatives, as well as interactions of a person and a robot, like expected in the fast growing area of service robots. And this interaction means that the robot will become part of the human workspace and not separated with a safe fence.

This is not a simple area since it involves aspects that were not considered some time ago. The current solution with slow moving robots can be improved with appropriate safety solutions, going far beyond Boolean expressions and fixed values to multi-axes systems with kinematic transformations. This is a real challenge for the future.

For more information and to download the specification check www.PLCopen.org	PLCopen® safety

Bernard Mysliwiec, Siemens AG, Nuremberg/Germany

Relation between functional safety and IT-security in practice: Roosevelt Island

The term Functional Safety is now well established as well in Factory as in Process or other industrial sectors. Dedicated user standards allow to satisfy the necessary safety requirements. Most of the control systems are now connected to Ethernet or Internet to exchange information together, to field devices or to monitoring systems. This brings new hazard possibilities related to IT-Security. These aspects are defined and explained in new and coming standards. The question is now, what has to be done in machines and plants, are complementary requirements to be considered to make a plant safe and secure. Machine Safety Experts considered these aspects. The presentation will show, how to perform the risk analysis and which normative or legal regulations-have to be considered. A pragmatical way will explain how system integrators can satisfy the requirements of Functional Safety and of IT-Security. An example based on ropeways (New-York Roosevelt Island Tramway) will show different use-cases.

IFA Matrix Method for development of safety related application software

Michael Huelke[a] **, Norbert Becker**[b]

[a] Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), Sankt Augustin, Germany
[b] Bonn-Rhein-Sieg University of Applied Sciences, Sankt Augustin, Germany

Abstract

Manufacturers of machinery are increasingly using application programming of safety controls in order to implement safety functions. The EN ISO 13849-1 and EN 62061 standards define requirements concerning the development of software employed for safety functions. The IFA began addressing the subject of safety-related application software many years ago. Between 2011 and 2013, Project FF-FP0319 concerning standards-compliant development and documentation of safety-related user software in machine construction was successfully completed at the Bonn-Rhein-Sieg University of Applied Sciences in conjunction with numerous partner bodies from the machine construction sector and with funding from the DGUV. For this purpose, a procedure – the IFA matrix method – was developed, and evaluated and documented with reference to examples from industry, for implementation of the requirements concerning the development of software for machine safety functions. This paper provides insights into both the IFA matrix method and the new IFA report on the subject, and with information on what further tools are planned.

Keywords:

Safety of machinery; safety-related parts of control systems; application software; cause and effect table

Introduction

Manufacturers of machinery are increasingly using application programming of safety controls in order to implement safety functions. In the past, EN 954-1 defined the requirements concerning the implementation of safety functions. By the end of the 2000s however, this standard had ceased to reflect the state of the art, and was replaced by EN ISO 13849-1 [1] and EN 62061 [3], either of which can be applied. The new standards include definitions of requirements concerning the development of software employed for safety functions. The requirements are intended to prevent hazardous systematic errors in the application software employed for a machine. How these new requirements are to be implemented in detail remains unclear to the software developers of safety functions. This is partly because by their nature, requirements in standards are formulated only in very general terms, and up to now virtually no examples of implementation have been published. This situation prompted the German Social Accident Insurance (DGUV), at the IFA's instigation, to fund the project described below.

DGUV research project FF-FP0319

In DGUV project FF-FP0319 (Norm compliant development and documentation of safety related application software in manufacturing system engineering) [6] (2011-2013), the project partner, Professor Dr Norbert Becker and his team at the Bonn-Rhein-Sieg University of Applied Sciences, developed several specific procedures for implementing the requirements set out in the new standards concerning the development of safety-related application software for machinery, and evaluated and documented these procedures with reference to industrial examples. The aim was to describe both the procedures and their application in a research report, which was then to be presented to the public as part of a new IFA Report [7].

Two committees were formed for evaluation of the project results during the project term:

- A user group consisting of local industrial companies
- The research support group, comprising representatives of control product manufacturers, accident insurance institutions, the IFA, the VDMA, TÜV Rheinland Akademie, KAN and users

In addition, the method was presented and discussed at a number of industrial companies.

The project was divided into the following tasks: development of a method and subsequent evaluation of the method by the user group and the research support group.

Several methods for specification of application software were studied:

- Description of application software as a finite state machine
- Specification by means of checklists
- Specification by means of tables

Describing the application software of an actual machine as a finite state machine in which all operating states are considered is generally a very complex process. Subsequent programming of the application software in a graphical or text-oriented programming language is also completely different. This particularly applies to safety-related software, for which the use of certified function modules is common. Procedures in which finite-state machines are described are not common in machine construction. Finite-state

machines are used in the specification of complex safety-related function modules (library modules) [4], which however was not the primary topic of this research project.
A checklist-based method was also developed. The safety functions are described in this method by forms based upon checklists. These forms are progressively refined in the course of further specification. Following presentation in the user group and the research support group, it soon became evident that the checklist-based method was also unsuitable for the development and documentation of safety-related software in an industrial context.
Many companies are however already documenting and specifying safety-related software in the form of tables. Based upon this activity, a matrix-based procedure for specifying and documenting safety software was developed. This met with much greater acceptance when presented to industry.
This procedure, described below as the "IFA matrix method", was positively received by the user group and the research support group. The discussions resulted in numerous improvements to the presentation. Several examples were integrated into this form of presentation in order for as many cases relevant to practice as possible to be described. In addition, a more comprehensive example of a machine tool was implemented in order to demonstrate the IFA matrix method's suitability for describing larger installations.

The IFA matrix method was presented to the public as an interim result of the project at the VDMA workshop on functional safety application software, held on 8 November 2012 in Frankfurt. It was subsequently presented on several occasions to companies and to test bodies. These presentations and publications [10] met with a largely positive reception and resulted in further constructive suggestions.

The IFA matrix method

Research project FF-FP0319 has been published in the form of a research report and ten examples illustrating the matrix method. These publications are available online [6].

The essential characteristics of the matrix method are:

- The V model of EN ISO 13849-1 can be simplified and broken down into two small V models (figure 1). One V model is used for the development of safety-function software, the other for the development of project-specific function modules.
- Definition of documents (captions see figure 1: A, B, C, D, V or AM, BM, CM, DM, VM) for execution of the V models. Many of these documents should already be present in the project implementation.
- Breakdown of the software into a pre-processing level, a de-energization logic to be specified, and a post-processing level (example see figure 2).
- This enables the de-energization logic to be specified by a cause and effect (C&E) table (figure 3). The test coverage can be completed by additional test lines in the C&E table.
- Integration of test and verification fields into the documents.
- The quality of the software in accordance with the specifications is assured by the test steps of verification, code review and software validation.

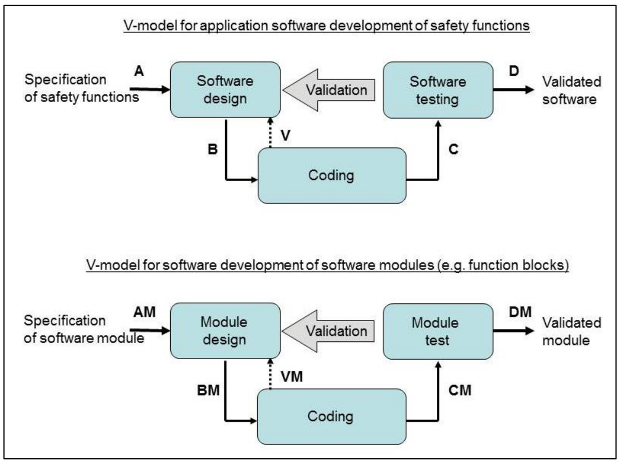
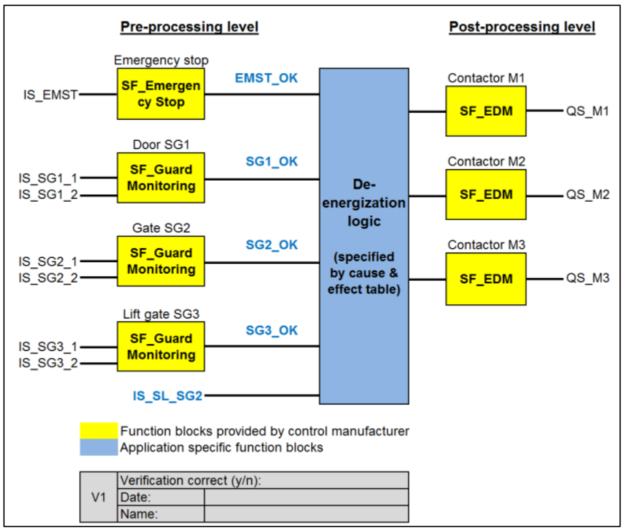

V-model for application software development of safety functions
Specification of safety functions
A
Software design
Validation
Software testing
D
Validated software
B
V
C
Coding
V-model for software development of software modules (e.g. function blocks)
Specification of software module
AM
Module design
Validation
Module test
DM
Validated module
BM
VM
CM
Coding

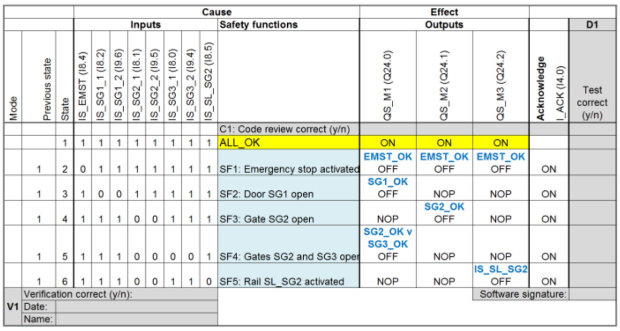
Figure 1: Simplified and seperated V-models



🟨 Function blocks provided by control manufacturer
🟦 Application specific function blocks

V1	Verification correct (y/n):	
	Date:	
	Name:	

Figure 2: Module architecture of application software



			Cause									Effect				
			Inputs								Safety functions	Outputs				D1
Mode	Previous state	State	IS_EMST (I8.4)	IS_SG1_1 (I8.2)	IS_SG1_2 (I9.6)	IS_SG2_1 (I8.1)	IS_SG2_2 (I9.5)	IS_SG3_1 (I8.0)	IS_SG3_2 (I9.4)	IS_SL_SG2 (I8.5)		QS_M1 (Q24.0)	QS_M2 (Q24.1)	QS_M3 (Q24.2)	Acknowledge I_ACK (I4.0)	Test correct (y/n)
											C1: Code review correct (y/n)					
		1	1	1	1	1	1	1	1	1	ALL_OK	ON	ON	ON		
	1	2	0	1	1	1	1	1	1	1	SF1: Emergency stop activated	EMST_OK OFF	EMST_OK OFF	EMST_OK OFF	ON	
	1	3	1	0	0	1	1	1	1	1	SF2: Door SG1 open	SG1_OK OFF	NOP	NOP	ON	
	1	4	1	1	1	0	0	1	1	1	SF3: Gate SG2 open	NOP	SG2_OK OFF	NOP	ON	
	1	5	1	1	1	0	0	0	0	1	SF4: Gates SG2 and SG3 oper	SG2_OK v SG3_OK OFF	NOP	NOP	ON	
	1	6	1	1	1	0	0	1	1	0	SF5: Rail SL_SG2 activated	NOP	NOP	IS_SL_SG2 OFF	ON	
V1	Verification correct (y/n):													Software signature:		
	Date:															
	Name:															

Figure 3: Cause & effect table for specification of logic

In order to describe the matrix method and its boundary conditions, this paper makes reference to the highly detailed presentations found in the freely available literature [6] [7] and to the SIAS presentation slides, which are also available.

IFA Report on safety-related application software for machinery

It was intended from the beginning of research project FF-FP0319 that its results would subsequently be formulated and published in an IFA report [7] on the topic. Besides presenting the development method itself, the IFA report will provide the target group with further essential information and interpretations regarding the normative requirements to be met by application software. The changes in the EN ISO 13849 series of standards, Parts 1 and 2 [2], will also be considered with regard to their relevance to application software.

The project examples are presented in a data format suitable for automated handling by future development tools, such as SOFTEMA, the IFA tool described below. The report is to be published in PDF format at the end of 2015, firstly in German and later in English. The revised examples will also be available for download.

This new IFA report thus supplements the familiar BGIA Report 2/2008, "Functional safety of machine controls" [5], which is focused more upon the reliability of the control hardware and upon calculation of its probability of failure.

The IFA SOFTEMA tool

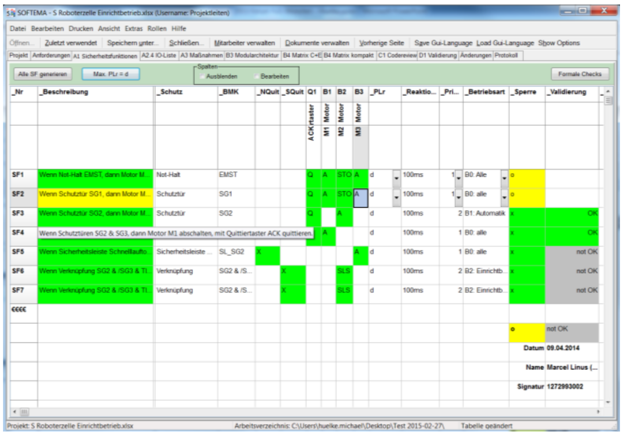
In order for the IFA matrix method to be implemented efficiently and with assured quality, the IFA is developing the SOFTEMA software tool (refer to the project information page of IFA Project 5137 [8]). Like IFA's SISTEMA tool, SOFTEMA will be available for download free of charge in the future. This chapter provides only an overview of the tool's planned features and functions. Further information and assistance for users will be made available separately in the future on the SOFTEMA download site.

The examples using the IFA matrix method that are available for download can be viewed in SOFTEMA (figures 4 and 5). Users can also use SOFTEMA to create and edit their own projects. SOFTEMA opens a project-specific file for specification and documentation of an application program. Multiple instances of SOFTEMA can however be opened in order for multiple projects and application programs to be worked on simultaneously.

SOFTEMA uses the Microsoft Excel worksheet (*.xlsx) format for its project files. The files can be edited either in SOFTEMA or in Microsoft Excel itself, as preferred. All tables can be edited freely in Excel. In SOFTEMA, the content is write-protected by the user management function. The specialized SOFTEMA functions described below are available only in SOFTEMA. In Excel however, additional table worksheets can be added and used for development and documentation, for example for hardware engineering.

SOFTEMA will initially support the following functions:

- Automatic updating of tables following modification of input data
- Formal verification of tables (for missing, conflicting or double entries)
- Management of project members
- Role-based user permissions
- Support during verification, validation and testing
- Support with modifications
- Dedicated editors for the different forms of cell content
- Management of documents and changes
- Specific print functions and reports



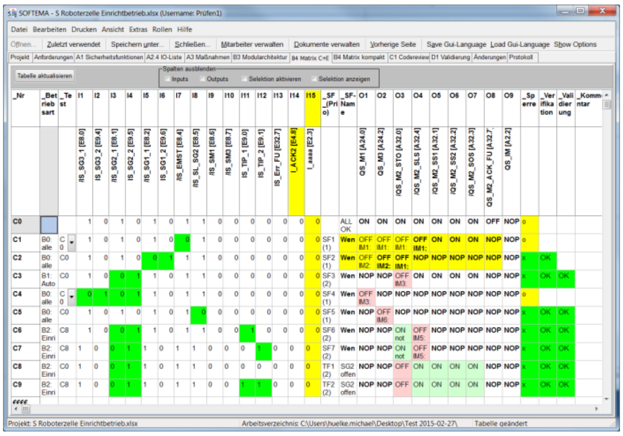
SOFTEMA - S Roboterzelle Einrichtbetrieb.xlsx (Username: Projektleiten)

Datei Bearbeiten Drucken Ansicht Extras Rollen Hilfe
Öffnen... Zuletzt verwendet Speichern unter... Schließen... Mitarbeiter verwalten Dokumente verwalten Vorherige Seite Save Gui-Language Load Gui-Language Show Options
Projekt Anforderungen A1 Sicherheitsfunktionen A2.4 IO-Liste A3 Maßnahmen B3 Modularchitektur B4 Matrix C+E B4 Matrix kompakt C1 Codereview D1 Validierung Änderungen Protokoll
Alle SF generieren
Max. PLr = d
Spalten
Ausblenden
Bearbeiten
Formale Checks

_Nr	_Beschreibung	_Schutz	_BMK	_NQuit	_SQuit	Q1 ACKrtaster	B1 M1 Motor	B2 M2 Motor	B3 M3 Motor	_PLr	_Reaktio...	_Pri...	_Betriebsart	_Sperre	_Validierung
SF1	Wenn Not-Halt EMST, dann Motor M...	Not-Halt	EMST			Q	A	STO	A	d	100ms	1	B0: Alle	o	
SF2	Wenn Schutztür SG1, dann Motor M...	Schutztür	SG1			Q	A	STO	A	d	100ms	1	B0: alle	o	
SF3	Wenn Schutztür SG2, dann Motor M...	Schutztür	SG2			Q		A		d	100ms	2	B1: Automatik	x	OK
SF4	Wenn Schutztüren SG2 & SG3, dann Motor M1 abschalten, mit Quittiertaster ACK quittieren.						A			d	100ms	1	B0: alle	x	OK
SF5	Wenn Sicherheitsleiste Schnellaufto...	Sicherheitsleiste ...	SL_SG2	X					A	d	100ms	1	B0: alle	x	not OK
SF6	Wenn Verknüpfung SG2 & /SG3 & TI...	Verknüpfung	SG2 & /S...		X			SLS		d	100ms	2	B2: Einrichtb...	x	not OK
SF7	Wenn Verknüpfung SG2 & /SG3 & TI...	Verknüpfung	SG2 & /S...		X			SLS		d	100ms	2	B2: Einrichtb...	x	not OK
€€€€															
														o	not OK
														Datum	09.04.2014
														Name	Marcel Linus (...
														Signatur	1272993002

Projekt: S Roboterzelle Einrichtbetrieb.xlsx Arbeitsverzeichnis: C:\Users\huelke.michael\Desktop\Test 2015-02-27\ Tabelle geändert

Figure 4: Table of safety functions (SOFTEMA preview)



SOFTEMA - S Roboterzelle Einrichtbetrieb.xlsx (Username: Prüfen1)

Datei Bearbeiten Drucken Ansicht Extras Rollen Hilfe
Öffnen... Zuletzt verwendet Speichern unter... Schließen... Mitarbeiter verwalten Dokumente verwalten Vorherige Seite Save Gui-Language Load Gui-Language Show Options
Projekt Anforderungen A1 Sicherheitsfunktionen A2.4 IO-Liste A3 Maßnahmen B3 Modularchitektur B4 Matrix C+E B4 Matrix kompakt C1 Codereview D1 Validierung Änderungen Protokoll
Tabelle aktualisieren
Spalten ausblenden
Inputs
Outputs
Selektion aktivieren
Selektion anzeigen

_Nr	_Betriebsart	_Test	I1 /IS_SG3_1 [E8.0]	I2 IS_SG3_2 [E9.4]	I3 /IS_SG2_1 [E8.1]	I4 IS_SG2_2 [E9.5]	I5 /IS_SG1_1 [E8.2]	I6 IS_SG1_2 [E9.6]	I7 /IS_EMST [E8.4]	I8 /IS_SL_SG2 [E8.5]	I9 /IS_SM1 [E8.6]	I10 /IS_SM3 [E8.7]	I11 IS_TIP_1 [E9.0]	I12 IS_TIP_2 [E9.1]	I13 IS_Err_FU [E32.7]	I14 I_ACK2 [E4.8]	I15 I_aaaa [E2.3]	_SF_(Prio)	_SF-Name	O1 QS_M1 [A24.0]	O2 QS_M3 [A24.2]	O3 /QS_M2_STO [A32.0]	O4 /QS_M2_SLS [A32.4]	O5 /QS_M2_SS1 [A32.1]	O6 /QS_M2_SS2 [A32.2]	O7 /QS_M2_SOS [A32.3]	O8 QS_M2_ACK_FU [A32.7	O9 QS_IM [A2.2]	_Sperre	_Verifikation	_Validierung	_Kommentar
C0			1	0	1	0	1	0	1	1	0	0	0	0	0	0	0		ALL OK	ON	ON	ON	ON	ON	ON	ON	OFF	NOP	o			
C1	B0: alle	C0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	SF1 (1)	Wen	OFF IM1:	OFF IM1:	OFF IM1:	OFF IM1:	ON	ON	ON	NOP	NOP	o			
C2	B0: alle	C0	1	0	1	0	0	1	1	1	0	0	0	0	0	0	0	SF2 (1)	Wen	OFF IM2:	OFF IM2:	OFF IM1:	NOP	NOP	NOP	NOP	NOP	NOP	x	OK		
C3	B1: Auto	C0	1	0	0	1	1	0	1	1	0	0	0	0	0	0	0	SF3 (2)	Wen	NOP	NOP	OFF IM3:	ON	ON	ON	ON	NOP	NOP	x	OK	OK	
C4	B0: alle	C0	0	1	0	1	1	0	1	1	0	0	0	0	0	0	0	SF4 (1)	Wen	OFF IM3:	NOP	NOP	NOP	NOP	NOP	NOP	NOP	NOP	o			
C5	B0: alle	C0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	SF5 (1)	Wen	NOP	OFF IM6:	NOP	NOP	NOP	NOP	NOP	NOP	NOP	x	OK	OK	
C6	B2: Einri	C8	1	0	0	1	1	0	1	1	0	0	1	0	0	0	0	SF6 (2)	Wen	NOP	NOP	ON not	OFF IM5:	NOP	NOP	NOP	NOP	NOP	x	OK	OK	
C7	B2: Einri	C8	1	0	0	1	1	0	1	1	0	0	0	1	0	0	0	SF7 (2)	Wen	NOP	NOP	ON not	OFF IM5:	NOP	NOP	NOP	NOP	NOP	x	OK	OK	
C8	B2: Einri	C0	1	0	0	1	1	0	1	1	0	0	0	0	0	0	0	TF1 (2)	SG2 offen	NOP	NOP	OFF	ON	ON	ON	ON	NOP	NOP	x	OK	OK	
C9	B2: Einri	C8	1	0	0	1	1	0	1	1	0	0	1	1	0	0	0	TF2 (2)	SG2 offen	NOP	NOP	OFF	ON	ON	ON	ON	NOP	NOP	x	OK	OK	
€€€€																																

Projekt: S Roboterzelle Einrichtbetrieb.xlsx Arbeitsverzeichnis: C:\Users\huelke.michael\Desktop\Test 2015-02-27\ Tabelle geändert

Figure 5: Cause & effect table (SOFTEMA preview)

Plans are for the beta version of SOFTEMA to be available for download on the IFA's website from the spring of 2016 onwards. The tool is to be available for use free of charge following registration.

Conclusion

This paper and the SIAS presentation slides describe a pragmatic and transparent method of meeting the requirements of EN ISO 13849-1 concerning safety-related application software for machinery. The method is based upon the results of a project funded by the DGUV [6] and forms the basis of the future IFA report [7] on the subject. The basic concepts and an example of the method have already been included in the existing draft of ISO/IEC 17305 [9]. The IFA matrix method also forms the basis of IFA's SOFTEMA tool [8], currently under development.

The IFA matrix method presented here can be used for standards-compliant specification, validation and documentation of the application software of safety functions. The procedure is non-proprietary and not specific to a particular programming language or Performance Level. Provided the procedures are followed, it can be assumed that the safety-related application software satisfies the relevant requirements of EN ISO 13849-1 [1].

Besides this procedure, other equally valid methods doubtless exist by means of which the requirements can be met. The IFA matrix method therefore lays no claim to be the only means of satisfying the requirements of the standards.

References

[1] EN ISO 13849-1:2007 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (7/2007). Beuth, Berlin 2008

[2] EN ISO 13849-2: Safety of machinery – Safety-related parts of control systems – Part 2: Validation (2/2013). Beuth, Berlin 2013

[3] EN 62061: Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems (10/2005). Beuth, Berlin 2005

[4] PLCopen – Technical Committee 5 – Safety Software Technical Specification, Part 1: Concepts and Function Blocks Version 1.0 – Official Release, 2006

[5] BGIA Report 2/2008 – Functional safety of machine controls – Application of EN ISO 13849, DGUV, 2008. Currently undergoing revision and adaptation to the second edition of EN ISO 13849-1

[6] Project page FF-FP0319, Norm compliant development and documentation of safety related application software in manufacturing system engineering. DGUV, Sankt Augustin 2014. http://www.dguv.de/webcode/ep54444

[7] Project page IFA5133, IFA-Report Sicherheitsbezogene Anwendungssoftware von Maschinen. IFA/DGUV, Sankt Augustin 2014. http://www.dguv.de/webcode/dp89985

[8] Project page IFA5137, SOFTEMA – Tool für sicherheitsgerichtete Anwendungsprogrammierung an Maschinen. IFA/DGUV, Sankt Augustin 2015. http://www.dguv.de/webcode/dp102081

[9] ISO/IEC 17305: Safety of Machinery – Safety Function of Control Systems, Working draft, 2014.

[10] Becker, N.; Eggeling, M.; Huelke, M. SPS-Software für fehlersichere Steuerungen - Normgerecht entwickeln und dokumentieren. atp edition - Automatisierungstechnische Praxis 57, Nr. 4, S. 34-47. Deutscher Industrieverlag, München 2015.

Corresponding address

Dr. Michael Huelke, DGUV, Alte Heerstrasse 111, 53757 Sankt Augustin, Germany

Security for Fail-Safe Communication in Automation

Felix Wieczorek[a], Frank Schiller[a], Jan Wolf[a]

[a] Beckhoff Automation GmbH & Co. KG

Abstract

Specific protocols for fail-safe communication via regular communication systems enable the control of critical applications. However, with the growing number of attacks on automation systems, security is an important issue. Safety measures and security measures apply different algorithms to achieve different goals, and their interaction may lead to mutual interference. In a first step, safety function and operation function are distinguished in order to assign security goals separately. This distinction is the base of an efficient combination of safety algorithms and security algorithms for their application in communication for automation. We propose different views on communication enabling efficient analysis of the interference between safety algorithms and security algorithms. The analysis leads to a suitable architecture, where security algorithms do not affect the existing fail-safe communication error models. The part of the security measures, which have to be included in the certification process under safety criteria can be designed to be minimal.

Keywords:

Information Security; Industrial Communication; Functional Safety; Fail-Safe Session; Error analysis

1 Introduction

The goal of safety in general is to decrease the risk of harm to humans and environment to an accepted degree. Solutions to safety critical applications in automation are often developed according to the principle of fail-safe systems. Those systems ensure all subsystems to be in a safe state. The safe state is met either if no error occurs, or if the system reacts in a safe way in case of an error.

The goal of security in general is to decrease the risk from malicious actions by attackers. Commonly considered risks are loss of confidentiality, integrity, or availability.

In the past, safety standards did not demand security means. Nevertheless, more and more safety systems are in the focus of security considerations because of e.g. increasing interconnection of automation systems. Until recently, isolation of those safety systems has been postulated.

Combinations of safety and security goals and corresponding measures are a topic in current research.

Safety systems are usually certified according to relevant standards i.e. [1, 2]. Those standards assume specific models for communication errors like the Binary Symmetric Channel (BSC), that may become invalid if security measures are not applied carefully.

This issue is treated in current research by not considering the impact of security measures to the assumed error models or by even trying to solve safety goals by means of security measures:

Åkerberg [3], claims to solve some safety problems with security measures. This approach would require to prove the security measures under safety aspects, which takes considerable effort, if feasible at all. Moreover, whenever the security system changes, a renewed safety proof is required.

Bock et. al. [4] provide security requirements for safety related communication in railway automation. Their approach is to separate security requirements from safety requirements by means of an infrastructure of zones and conduits. The authors consider the secure conduits as black channel in the safety analysis, but the consequences of this choice are not fully analyzed.

Wieczorek et. al. [5] provide an architecture for secure integer and confidential fail-safe message transmissions. However, important aspects like sequence integrity are left open and are discussed in this contribution.

2 Distinction between Operation Function and Safety Function

Usually, the automation tasks can be divided into operation function and safety function (see Figure 1).

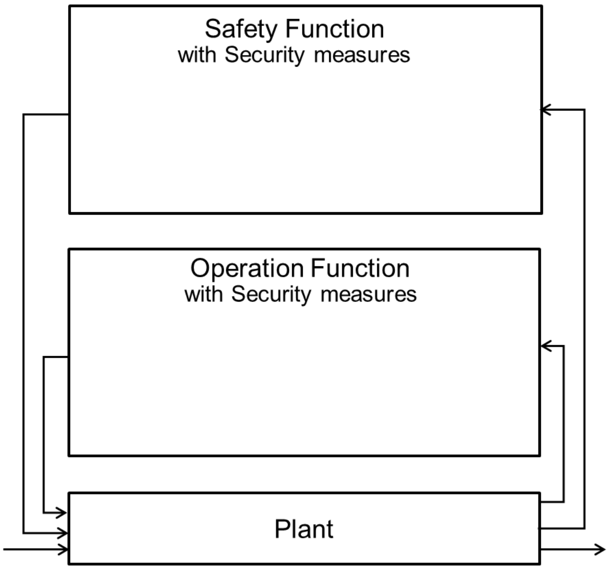


Figure 1: General Structure

2.1 Characteristics of Operation Function and Safety Function

The operation function achieves the economic added value of the plant. On the other hand, the safety function enforces the safety goal with sufficient probability and therefore needs to overrule the operation function if necessary. This is ensured by maintaining a safe operation or initiating a transition into another safe state. This state is allowed to decrease the availability of the operation function. The safety function is considered available after such a transition, since its goal is still maintained.

Obviously, plants need a high degree of availability of the operation function as well as a high degree of availability of the safety function. However, safety functions can often be designed to be less complex if the availability of the operation function is not taken into account. There, the safety can often be proven with less effort. Sometimes, only this approach enables affordable safety of plants.

2.2 Security Goals of Operation Function and Safety Function

The general goals of security are confidentiality, integrity, and availability. The importance of each goal depends on the specific application only.

- *Integrity* ensures the correctness of information or the functionality of a system, providing changeability to authorized parties only.

Integrity is ensured in safety with the focus on accidental transmission errors, which requires different methods than protection against manipulation by attackers.

- *Availability* ensures that authorized parties can use information and functionality of a system as specified.

The security goal availability is commonly reached by restricting the resources to authorized parties only or the system is designed to be usable even in case of attacks.

- *Confidentiality* is the protection against unauthorized disclosure of information. Confidential information must only be accessible in a defined manner for authorized parties.

The defined manner of access is accomplishable through encryption with the use of a secret key. This is one of the classic goals in cryptography.

Authenticity is often mentioned as a further goal. It can be solved with a Public Key Infrastructure (PKI) in combination with key-exchange protocols (see e.g. [6]) which bind address data to secret keys. Thus integrity can also ensure authenticity.

Many other goals like freshness or non-repudiation can be reduced to the fundamental goals confidentiality and integrity.

The general security goals are adapted to operation function and safety function separately in the following (cf. Figure 2):

- *Security-Integrity for Operation* demands to avoid economic loss caused by manipulation of data and functions.
- *Security-Integrity for Safety* means that manipulation of safety-related data and functions is avoided or detected.

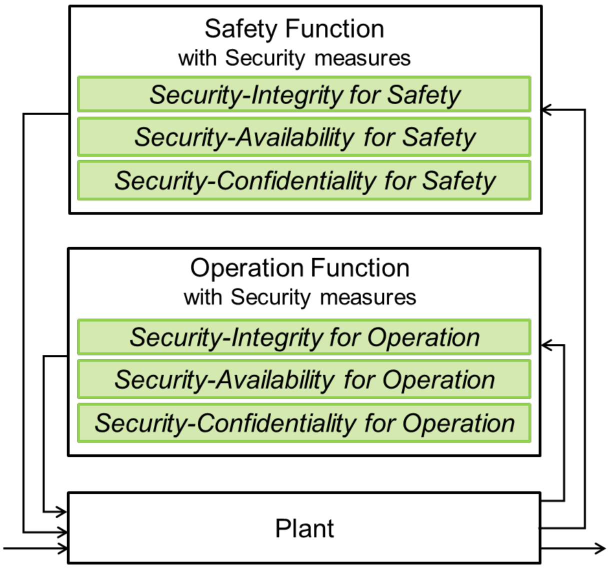

Safety Function
with Security measures
Security-Integrity for Safety
Security-Availability for Safety
Security-Confidentiality for Safety
Operation Function
with Security measures
Security-Integrity for Operation
Security-Availability for Operation
Security-Confidentiality for Operation
Plant

Figure 2: Mapped Security Goals

The reaction to a detected manipulation of Security-Integrity for Safety has only to keep safety, regardless of the economic impact. Vice versa, the violation of the Security-Integrity for Operation must not affect the safety at all.

- *Security-Availability for Operation* means to provide the operation function and data whenever needed. Amongst others, the safety-related transition to a less-productive state should be avoided if possible.
- *Security-Availability for Safety* addresses the capability of the safety function to avoid hazards and accidents.

In a safe state, the availability of the operation function can be reduced. Therefore the Security-Availability for Safety can affect the Security-Availability for Operation tremendously.

- *Security-Confidentiality for Operation* prevents unauthorized inference about sensitive information to avoid economic loss.
- *Security-Confidentiality for Safety* prevents unauthorized inference about sensitive information to avoid hazards and accidents.

Interlaced confidentiality dependencies between the operation function and the safety function occur if the same confidential information is used in the operation function as well as in the safety function. The same information can be represented differently and might not be recognizable at first glance (e.g. operational and safe sensors measuring the same physical variable). In such cases, the information has to be protected accordingly to both Security-Confidentiality for Operation and for Safety in all representations.

This concept has an impact on the design of security measures for fail-safe communication in automation.

3 Fail-Safe Communication

3.1 Goals

The general goal of fail-safe communication is to detect errors and to initiate a safe reaction. Fail-safe communication solutions mainly focus on random errors:

- The algorithms aim to detect bit errors in transmitted messages with high probability. The corresponding indicator is the residual error probability (P_{re}).
- An additional goal is the detection of specific error patterns in the messages (deterministic criteria).
- Fail-safe communication demands not only measures for data integrity in messages but also further safe detection of sequence errors and session errors (see Table 1, which is inspired by [2]).

Table 1: Mapping of the safety errors of IEC 61784-3 to views in this paper

Communication Errors	Message related	Sequence related	Session related
Corruption	x	x	x
Unintended repetition		x	x
Incorrect sequence		x	x
Loss		x	x
Unacceptable delay			x
Insertion		x	x
Masquerade	x	x	x
Addressing error			x

3.2 Session Concept

Typically, communication is organized by a layer architecture [7]. Fail-safe communication provides properties of a session layer and often uses standard automation communication protocols as the transport layer, see Figure 3.

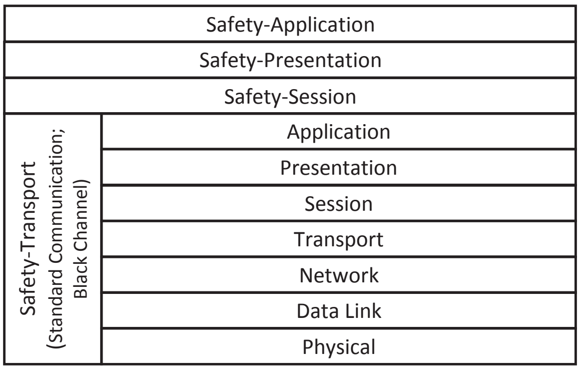


Figure 3: Layer architecture

A session includes the measures to ensure that the sender knows about the reception of all transmitted data and that the receiver knows about the completeness and correct order of the transmitted data.

Sessions between sender and receiver are established and terminated. Therefore, a session is either established or non-existent at every point in time. During a session, a sequence of messages is transmitted and the sender is informed about the reception of all messages by means of acknowledgements. A sequence is an ordered tuple of messages (see Figure 4).

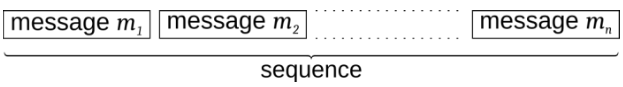


Figure 4: Sequence of messages

The maximum allowed time interval without new received messages defines Δt_{live}. If there was not received any message in this time interval, the session would be terminated by the receiver. Additionally, Δt_{ack} is defined by the maximum allowed time interval for the reception of the corresponding acknowledgement after sending a message. If no acknowledgement for a specific message was received during the time interval between sending the message at t_s and receiving the acknowledgement at $t_s + \Delta t_{ack}$, the session would be terminated by the sender (see Figure 5).

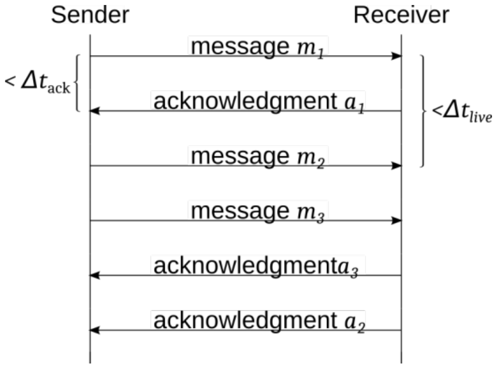


Figure 5: Illustration of a session

Obviously, a session concept is already being applied in fail-safe communication. However, it has not been necessary to treat it as a separate concept. But this concept is very helpful in the context of security considerations.

3.3 Error Model

The typically used error model in fail-safe communication is the Binary Symmetric Channel (BSC). This model assumes that

- the bits are corrupted independently,
- each bit is falsified with same probability (bit error probability), and
- the falsification from 0 to 1 occurs with same probability as from 1 to 0.

Apparently, the assumptions of the BSC do not completely apply. There are errors that might occur with higher probabilities than they would determined based on the BSC.

For instance, the probability of complete inversion of a message is very low according to BSC since each bit is corrupted with the bit error probability. But inversion can be the effect of hardware faults of much higher probability.

Therefore, in addition to the probabilistic criterion, so called deterministic criteria are to be met by the error detection algorithm. They include the detection of

- completely inverted messages,
- messages consisting only of 1-bits,
- messages consisting only of 0-bits,
- slack errors,
- burst errors, and

- bit errors smaller than a required minimal Hamming Distance (HD).

In general coding theory, the minimal HD describes the minimum number of bits necessary to transform at least one valid code word into another.

In communication, HD means more specifically how many bits are at least to be falsified in order to potentially achieve an undetectable erroneous message. For instance, a HD of 6 means that all 1 up to 5 bit errors are detectable. This characteristic — like the other deterministic criteria — does not depend on the assumption of the BSC. Therefore, the analysis of the deterministic criteria is also reasonable and often required.

3.4 Common Solutions

Error Detecting Codes

To detect transmission errors in data ($data$), a checksum, called frame check sequence (fcs), is concatenated, such that the message becomes $m = data \parallel fcs$. After transmission, the consistency between the $data$ and corresponding fcs is checked. The correctness of $data$ is assumed whenever consistency holds.

There are various techniques for error detection. An efficient and common coding technique is the Cyclic Redundancy Check (CRC). There, a low residual error probability can be assured with a relatively short fcs. A generator polynomial is the main parameter, which has remarkable impact on the quality of error detection [8, 9, 10].

In general, the residual error probability P_{re} is calculated by

$$P_{re} = \sum_{i=HD}^{n} A_i \cdot p^i \cdot (1-p)^{n-i}, A_i \leq \binom{n}{i}$$

where A_i denotes the number of undetectable error patterns of i bits of a n bit message, and p denotes the bit error probability according to the BSC.

A typical curve of P_{re} as a function of p is depicted in Figure 6. There, the CRC applies the generator polynomial $x^{24} + x^{23} + x^{19} + x^{18} + x^{16} + x^{15} + x^{13} + x^9 + x^7 + x^4 + x^3 + 1$ or 18DA299 in hexadecimal notion, respectively. This specific generator polynomial of degree 24 is proper for 428 bit of data, i.e. it causes a maximum P_{re} of 2^{-24}.

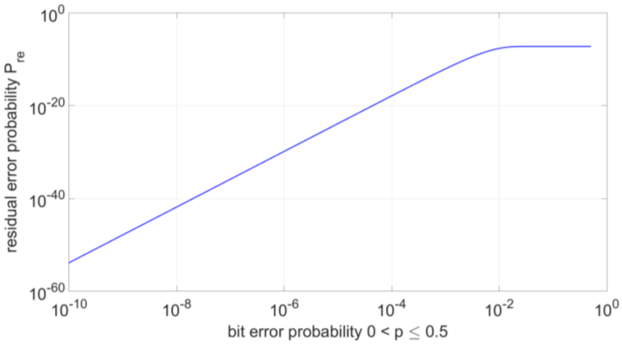


Figure 6: Residual Error Probability of CRC-24 (18DA299h, 428 bit of data, assumption of BSC)

Besides the residual error probability of CRC, its compliance with the deterministic criteria can be assured [11].

Sequence Error Detection

Many existing solutions solve sequence errors by error detecting codes on message level by maintaining a shared state in sender and receiver, e.g. stateful CRC. This state is treated as additional input data for the calculation of the fcs. The shared state is either sent (e.g. sequence numbers) or not sent (as implicit data, cf. [2]).

Therefore, all sequence errors can be detected and treated in the same way like regular errors in safety-related messages. (Remark: All safety justifications have to be rethought.)

Session Error Detection

The remaining session errors are detected by timers and acknowledgements. Often addresses are included in safety-related messages and therefore, addressing errors can be detected by means of error detecting codes, too.

4 Secure Communication

The security goals for safety (cf. Section 2.2) have to be derived for applicability in fail-safe communication.

4.1 Derived Goals

Integrity for fail-safe communication means that the session is either correct or detectably incorrect. Correctness of a session means that all messages in the transmitted sequence are correct and the sequence start and end are correct, i.e. identical in sender and receiver.

Availability for fail-safe communication means, that either a session is fully functional or the session is detectably broken down.

Confidentiality for fail-safe communication is given if no unauthorized third party can infer confidential information, which is transmitted without the knowledge of involved secret keys.

With respect to security requirements, an attacker has to be considered.

4.2 Attacker Model

An attacker is assumed to possess the capabilities to

- read all transmitted messages,
- manipulate all transmitted messages,
- drop all transmitted messages and
- transmit any messages to each communication party.

An attacker is assumed not to have direct access to relevant secret keys.

Common attack goals are to

- infer confidential information,
- undetectably insert or manipulate information, or
- force one or more communication parties into stopping communication.

4.3 Common Solutions

Ciphers

Output of ciphers aims to be not distinguishable from uniformly randomly distributed data without knowledge of the key. They can be classified as outlined in Figure 7.

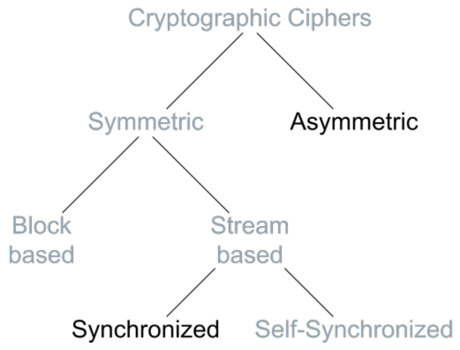


Figure 7: Classification of ciphers

Asymmetric cryptography bases on trapdoor functions, where one operation is easy and the related inverse function is assumed to be hard to compute without the knowledge of a secret (e.g. encryption can be made with the public key, but the decryption is only feasible with the corresponding private key). Asymmetric cryptography scales well for a large number of communication parties, since a system consisting of n parties requires $O(n)$ key pairs.

Symmetric cryptography uses the same shared secret key for encryption and decryption. Symmetric cryptography is faster than asymmetric cryptography, but does not scale well for a large number of communicating parties. If each participant has to reach the security goals with each other in a system, a system consisting of n participants requires $O(n^2)$ secret keys.

Symmetric ciphers are categorised into block ciphers and stream ciphers.

Block ciphers split the data into blocks of equal length. Each block is processed depending on the key and possibly on an internal state [12, p. 228 ff]. A design aspect is the strict avalanche criterion which was introduced by [13]. It states, that each change of the input block (e.g. also only one input bit) affects each bit of the output block (cf. Figure 8). If block chaining or a similar encryption mode is used even the following blocks will be affected. That means, each input data error causes an unpredictable data error after decoding.

Assuming a uniformly randomly chosen key, the blocks of output data are uniformly distributed for each input data.

For comparison: this result is equivalent to a uniform distribution caused by a bit error probability of 0.5 in the BSC, although BSC is not valid since all bits in one block depend on each other.

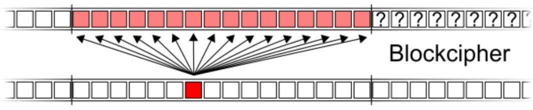


Figure 8: Propagation of one bit error in block cipher decryption

Stream ciphers use the key for initialization and then produce a pseudorandom stream. This stream is used in synchronous stream ciphers to overlay the data by exclusive or. The avalanche criterion does not apply here. The stream cipher ensures that the only one corresponding output bit is affected (cf. Figure 9). Stream ciphers are usually more performant, but the experience in design and analysis of schemes may not be as high as with block ciphers.

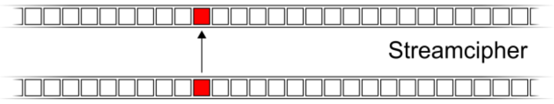


Figure 9: Propagation of one bit error in stream cipher decryption

Encryption Schemes

In many cryptographic protocols, a hybrid approach is used to reach the speed of symmetric ciphers and the scalability of asymmetric ciphers [6]. In these protocols, a secret key is exchanged privately using asymmetric cryptography. The information is later secured with a symmetric algorithm employing the exchanged key.

Embedded and real-time systems often use encryption schemes facilitating stream ciphers. There they can be used in synchronized mode, where the stream is produced independently of the input data or the ciphertext, and a synchronized state is maintained in all participants. Alternatively, there is also a self-synchronized mode of stream ciphers, where a limited number of the processed ciphertext bits influence the output of the stream, so that the stream resynchronizes after a fixed length of processed ciphertext [12, p. 199 ff].

In the following, we focus on real-time constraint communication, where synchronous stream ciphers are a good choice. Regarding the safety error model, this is also recommended by [5]. We will assume that secret keys are already known to each party. Though the essential key exchange will not be discussed in this paper.

Sessions in Security

The common solution to secure communication is the Transport Layer Security (TLS) protocol [6] which among others provides secure sessions. TLS satifies the goals message integrity, sequence integrity, and confidentiality.

Nevertheless, security solutions do not fulfill all required safety goals and are only usable with adaptation for fail-safe communication.

5 Interference of Safety Algorithms and Security Algorithms

In this section, we analyze the interference between safety algorithms and security algorithms.

Potential interference can occur between each of the algorithms of safety and security. Detrimental interference among security algorithms are assumed to be well analyzed and mastered. The same is assumed for safety algorithms here.

The security algorithms taken into consideration are those gaining security-integrity and security-confidentiality. The safety algorithms to be analyzed are those aiming at safety-integrity and safety time expectations of communication.

Security-availability on transport level is not in the focus of this contribution, because it is only solvable if several transport routing options are possible.

The safety time expectations are not affected by security algorithms except for an integer time base for time measurements, which has to be provided with security-integrity. The runtime of the security algorithms is not relevant w.r.t. safety, as they can be treated as any other transport delay from safety perspective.

Therefore, the interference between integrity algorithms of safety and security are further analyzed, as well as the interaction between security-confidentiality and safety-integrity.

If chosen carefully, the security-confidentiality can be achieved not affecting the safety-integrity [5]. There the layered approach without sessions is proposed (cf. Figure 13).

5.1 Message Integrity

Weak Manipulation Detection by Safety Algorithms

The fcs on base of CRC must not be used as security-integrity information, since an attacker could superimpose every multiple of the generator polynomial of the CRC without detection. Even for stored data sets with known fcs, not only consistency but the identical fcs can be achieved easily by manipulation [14].

Especially, the deterministic criteria (cf. Section 3.3) are contradicting the required feature of seemingly uniform random output (cf. Section 4.3). They are easily to be identified, and the success probability to generate undetectable error patterns increases, since the possible search space is tremendously reduced.

Insufficient Random Error Detection by Security Algorithms

The message authentication code (mac) prevents attackers from forging messages, which leads to the basic idea that random errors could also be detectable with the mac scheme. For this reason, the mac is analyzed under the assumption of the BSC (cf. Section 3.3) in the following. The Message Authentication Code Algorithm (MAC) is used to calculate the mac depending on a secret key, an internal state, and the $data$. Note that the mac is assumed to be equally distributed according to its construction principle:

$$P(\mathrm{MAC}(data_1) = mac) = P(\mathrm{MAC}(data_2) = mac)$$
$$\text{where } data_1 \neq data_2, \qquad mac \in \{0,1\}^{|mac|}$$

The MAC is deterministic according to its design criteria. The message $data \parallel \mathrm{MAC}(data)$ with the error pattern e leads to the erroneous $data$

$$\big(data \parallel \mathrm{MAC}(data)\big)' = \big(data \parallel \mathrm{MAC}(data)\big) \oplus e$$
$$= data' \parallel \big(\mathrm{MAC}(data)\big)'$$

If e affects the mac only, such that

$$\big(data \parallel \mathrm{MAC}(data)\big)' = data' \parallel \big(\mathrm{MAC}(data)\big)'$$

holds, the error is always detected.

If the error is affecting $data$, then the probability that the error is not detected is equal to $2^{-|mac|}$. This probability is independent of the falsification of the mac since all $macs$ are equally probable. Therefore, the overall probability of undetectable errors is

$$P_{re} = 2^{-|mac|} \cdot \big(1 - (1-p)^{|data|}\big)$$

where p is the bit error probability according to the BSC. The second factor describes the probability of the occurrence of any error in the $data$. An example with $|mac| = 60$ is depicted in Figure 10.

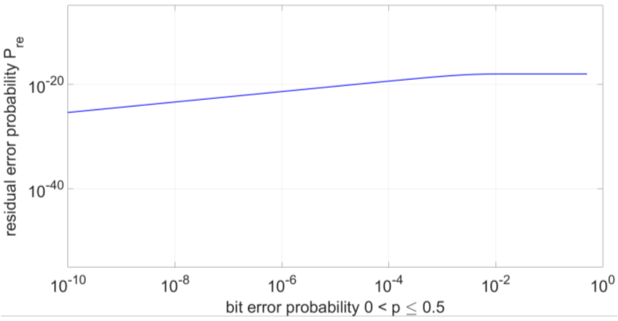


Figure 10: Residual Error Probability of MAC-60 (428 bit of data, assumption of BSC)

The security-integrity algorithms can only be analyzed for random errors based on the BSC.

Further assumptions about the detectability of errors corresponding to the deterministic criteria cannot be made.

The probability of any undetectable error is equal for each error pattern $\left(2^{-|mac|}\right)$ including those desribed by deterministic criteria. Therefore, it is not sufficient to be used as the only integrity protection in fail-safe communication.

However, it can be combined with a CRC algorithm.

The resulting combined solution limits the P_{re} of random errors up to the minimum P_{re} of both the safety algorithm and the security algorithm. The safety-integrity algorithm additionally assures the necessary compliance with deterministic criteria.

The P_{re} of both a CRC and a MAC as a function of the bit error probability are depicted in Figure 11. Since independency of the two checks cannot be proven in general, the minimum P_{re} is applied.

Obviously, the MAC contributes to a small P_{re}, and the CRC can maintain all criteria necessary for fail-safe communication.

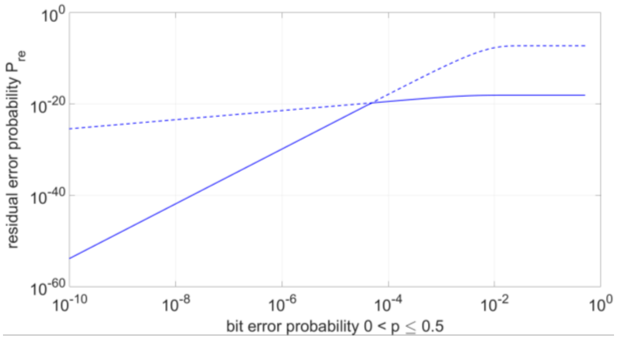


Figure 11: Residual Error Probability of CRC and MAC

The combination of the integrity algorithms can result in detection of errors from the application of security algorithms by the CRC.

Deeper analysis is in progress.

5.2 Sequence Integrity

The safety CRC can include values dependent on the previous messages (e.g. sequence numbers). As such it provides sequence integrity with the same probabilities as in Section 5.1.

The MAC can involve the previous mac or rely on a secret state updated continuously during protection of a sequence. It protects the sequence up to the current mac in this way. This principle of chaining authentication tags was first described in [15].

If the sequence integrity is solved with chained checksums, the conclusions from Section 5.1 also apply for sequence integrity.

5.3 Session Integrity

For the session integrity, the start and end of the underlying sequence have to be secured e.g. by marking the first message and last message. The time intervals between the messages have to comply with Δt_{live} (cf. Figure 5). Additionally, for each message, a corresponding acknowledgement is to be received in Δt_{ack}.

In order to draw reliable conclusions from the time intervals, the security-integrity of the corresponding time base has to be ensured.

5.4 Detection of Random Errors caused within Security Algorithms

Random errors resulting from execution of the security algorithms have to be detectable in safety algorithms, too. This is conform to the always aimed model of the black channel, that regards everything which is integrity protected by safety as random error sources, and therefore does not require further analysis of the underlying algorithms.

6 Communication Architecture

We propose the following combination of security algorithms and fail-safe algorithms in communication for satisfying the goals stated in Section 3 and Section 4. The sequence requirements are fulfilled by means of chained $macs$. Therefore, we only consider the message view and the session view in the following.

6.1 Message View

The messages of the sender are protected in the following order (cf. Figure 12):

1. The data of the critical application is first integrity protected by the safety algorithm attaching an fcs to the data.
2. The safety-integrity protected result is then encrypted for reaching security-confidentiality using a synchronized stream cipher.
3. Then the encrypted result is security-integrity protected by a MAC algorithm, which concatenates a mac.

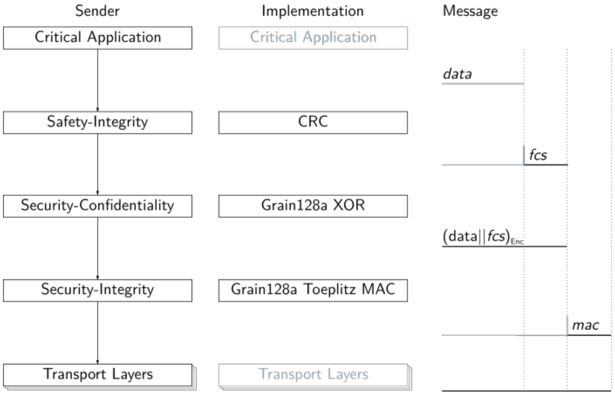


Figure 12: Implemenation and Message structure

The advantage of using the synchronized stream cipher Grain128a is that it propagates bit error patterns (cf. Section 4.3).

6.2 Session View

Sessions are established at a defined time between a sender and a receiver and broken down at a defined end point.

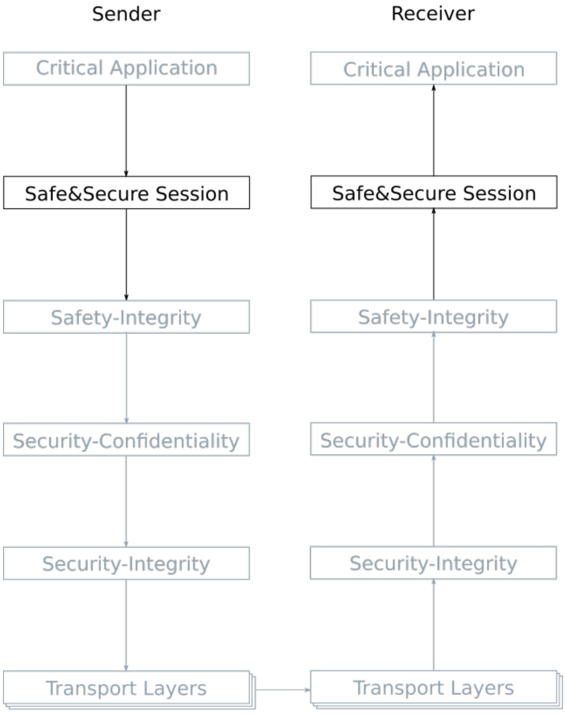


Figure 13: Session Layers

The order of integrity-protected messages and integrity-protected acknowledgements is ensured by chained fcs and chained mac. Addresses are included in the calculations of fcs and mac ensuring correct addressing, and thus providing authenticity. With specially marked messages indicating the start and end of a sequence, completeness of a sequence is protected. The participants have to authenticate to each other with asymmetric cryptography at the start of a session (using a key-exchange protocol not described here). The safety relevant configuration information that is used for the session has to be security-integrity protected. This is still an open topic.

The session is either fully available or broken down in a controlled manner by the critical application, whenever an error has been detected.

The algorithms had been chosen as follows:

- a secure session employs a well-known key-exchange before session start,
- CRC-24 is used for safety-integrity protection,
- Grain128a [16] as a stream generator,
- exclusive or in a synchronized stream-cipher mode reaches security confidentiality,
- a chained Toeplitz construction with 60 bit length gains security-integrity [17], and
- session management uses defined start and end messages (cf. Figure 13).

7 Conclusion and Future Work

The contribution presents an efficient combination of safety algorithms and security algorithms for their application in fail-safe communication. The distinction between safety function and operation function is taken advantage from. From different views on communication, we analyze the interferences between safety algorithms and security algorithms.

The analysis leads to a suitable architecture, where security algorithms do not affect the existing fail-safe communication error models. The parts of security algorithms, which presumably had to be certified under safety criteria are minimal.

In order to implement this architecture, care has to be taken to provide adequate quality (e.g. robustness [18]).

For key exchange and key distribution, asymmetric cryptographic algorithms and protocols still have to be evaluated and analyzed with respect to safety. Another open topic is the security-integrity of stored safety data.

References

[1] International Electrical Commision, IEC 61508 functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.

[2] International Electrical Commision, IEC 61784-3 Ed 3.0 Amendment 1: Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions, to appear in 2016.

[3] J. Åkerberg, "On Safe and Secure Communication in Process Automation," 2011.

[4] H.-H. Bock, J. Braband, B. Milius and H. Schäbe, "Towards an IT Security Protection Profile for Safety-Related Communication in Railway Automation," in Computer Safety, Reliability, and Security, vol. 7612, F. Ortmeier and P. Daniel, Eds., Springer Berlin Heidelberg, 2012, pp. 137-148.

[5] F. Wieczorek and F. Schiller, "Safety und Security für Feldbus-Anforderungen," atp edition - Automatisierungstechnische Praxis, no. 10, pp. 44-51, 2012.

[6] T. Dierks and E. Rescorla, RFC 5246, The Transport Layer Security (TLS) protocol version 1.2, 2008.

[7] International Organization for Standardization, 7498-1 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model, 1994.

[8] W. Peterson and E. J. Weldon, Error correcting codes, MIT Press, 1996.

[9] P. Sweeney, Error control coding: an introduction, Prentice-Hall, 1991.

[10] F. Schiller and T. Mattes, "Analysis of CRC-polynomials for safety-critical communication by deterministic and stochastic automata," in 6th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS 2006, Beijing, China, 2006.

[11] F. Schiller and T. Mattes, "An efficient method to evaluate CRC-polynomials for safety-critical industrial communication," Journal of Applied Computer Science, vol. 14, no. 1/2006, pp. 57-80, 2006.

[12] A. J. Menezes, S. A. Vanstone and P. C. V. Oorschot, Handbook of Applied Cryptography (discrete mathematics and its applications), 5th printing 2001 ed., Boca Raton, FL, USA: CRC Press, Inc., 1996, p. 816.

[13] A. Webster and S. Tavares, "On the design of S-Boxes," in Advances in Cryptology -- CRYPTO ’85 Proceedings, vol. 218, H. Williams, Ed., Springer, 1986, pp. 523-534.

[14] F. Schiller, T. Mattes, U. Weber and R. Mattes, "Undetectable manipulation of CRC checksums for communication and data storage," in Communications and Networking in China, vol. 26, P. Bond, Ed., Springer, 2009, pp. 1-9.

[15] L. Lamport, "Password Authentication with Insecure Communication," Commun. ACM, vol. 24, no. 11, pp. 770-772, 1981.

[16] M. Ågren, M. Hell, T. Johansson and W. Meier, "A new version of Grain-128 with authentication," in Symmetric Key Encryption Workshop 2011, 2011.

[17] H. Krawczyk, "LFSR-based Hashing and Authentication," in Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology, 1994.

[18] R. Langner, Robust Control System Networks, Momentum Press, 2012.

Corresponding address

Beckhoff Automation GmbH & Co. KG
Scientific Safety & Security
Ostendstraße 169, D-90482 Nuremberg
f.wieczorek@beckhoff.com

Development model for distributed safety function in mobile work machinery site

Ari Ronkainen[a], Risto Tiusanen[b], Timo Malm[b], Sami Pietikäinen[c]

[a] *Natural Resources Institute Finland*
[b] *VTT Technical Research Centre of Finland*
[c] *Wapice ltd*

Abstract

In mobile work machinery industry there is a drive for integration and co-operation between machines. This drive is due to higher demands in productivity and in changes of business models. The growing trend for the industry is to move from machine manufacturers to service and capacity providers.
As machines integrate to systems where machines need to co-operate among themselves and with human operators and operations management systems a question of managing safety arises. The solution of managing safety requires solutions in all management aspects of the system. This his paper focuses on machinery in such site. It is foreseeable that the machines may need to perform safety function in co-operation and the safe sates of the machinery or the system may be dependent on co-operation or states of the machinery in the system.
To develop machinery and machinery functions for integrated work-site system a development model is needed. Current standardization for safety related parts of control systems include development models, functional safety life-cycles, but they are intended for single machines, where every system related to safety function, are under the domain of the machine and its designer. In this paper a development model for mobile work machinery combinations is presented. The development model is based on functional safety lifecycles of today's standardization. The development model is applied and evaluated in a simple use-case for agricultural machinery.

Keywords:
Distributed safety; functional safety; development model

Introduction

In order to complete work tasks in mobile work machinery sites several machines need to co-operate. For example in harbours to unload a ship there needs to be a gantry to empty the ship and straddle carriers and cargo trucks to handle the containers and transport them to trucks. Similar cases can be found in several different sectors, like civil engineering, construction or agriculture.

To increase the productivity there is a drive to increase integration between systems. Machines start to integrate into systems. Also the transition of machine manufacturers more into service providers drives system integration.

When machinery systems begin to integrate and co-operate the questions of overall safety arise. There needs to be some way to ensure and manage the overall safety in the worksite. Especially if machines have means to communicate with each other and adapt their actions according to other machines and co-operate.

Current standards regarding safety related parts of control systems and functional safety standards consider only the scope of one machine. When the overall safety is managed by several machines the safety functions become distributed. The machines are covered by standards and legislation, but the overall, worksite level, functions are not.

These kinds of distributed safety arrangements have been managed in railroad and aviation domains for very long time.

The question set is: can existing standardization be used to create a frame work to manage these distributed safety functions and can advice be found from aviation or railroad systems.

Methods

To create a development model for distributed mobile work machinery site, reference is taken from other sectors of industry and society, where similar problems can be identified. For this study railroad systems and aviation systems were studied. In both railroad and airways systems there are machines, trains and airplanes, and background infrastructure, rails, traffic control systems, radar systems, communication system.

Several functional safety related standards also use development models as a reference or tool in design of safety related systems. These models are often called functional safety lifecycles. Reference was taken also from these standards. IEC 61508 and ISO 25119 were especially used.

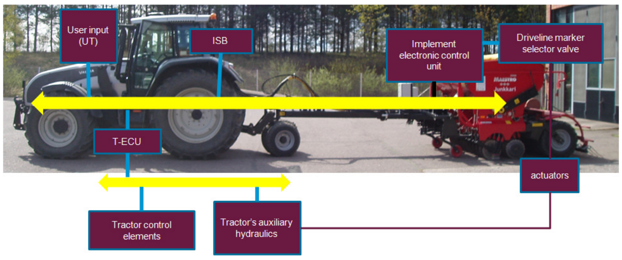

User input (UT)
ISB
Implement electronic control unit
Driveline marker selector valve
T-ECU
actuators
Tractor control elements
Tractor's auxiliary hydraulics

Figure 1: Tractor-implement combination and ISO 11783 network

To test the developed model, the model is applied in development of a distributed safety function in agricultural tractor-implement combination. The combination consists of a tractor and seed drill both connected with ISO 11783 communication network. In the network also some auxiliary devices exist.

ISO 11783 standard describes a serial data exchange network for tractors and machinery in agriculture and forestry. ISO 11783 network is also known by its trade name ISOBUS. The name ISOBUS and the implementation guide for ISO 11783 is governed by Agricultural Industry Electronics Foundation or AEF [1]. ISO 11783 allows machinery to share information or request functions from other machines [6]. This allows ISO 11783 network to be used in creation of distributed control functions.

In this case the function is a request for the working set to stop automated functions and transit to a safe state. The request is made by a device intended for this purpose. The device is called ISOBUS short-cut button (ISB)[2] and its functionalities are defined by Agricultural Electronics Industry Foundation [1]. The request is conveyed over ISO 11783 network to implement's electronic control unit (ECU). The Implement ECU makes a decision on which of two possible safe states to transit. The decision is based on a signal from an external system called task controller. The implement ECU then requests necessary control functions from the tractor over ISO 11783 network, needed to transit into safe state.

Results

The outcome of the development resulted in a draft development model. The process described in the model is illustrated in Figure 1. The process begins by defining the worksite, its limits, occupational health and safety regulations, safety goals, etc. and from these sources a worksite concept is to be defined. This concept should define what is done in the worksite, how, who are the actors involved and their responsibilities.

The purpose of the concept is to act as material for worksite safety analysis. In the analysis the risks related to operations at the work site are to be identified and from the identified risks requirements for worksite safety are to be formulated.

When the worksite has been defined and its risk identified, a worksite safety concept is to be formed. The concept should define how the safety requirements are met in the worksite. This should include the necessary procedures, functionalities, functions and the performance requirements. The concept should not focus solely on technological solutions but include all the layers of protection. A safety function should still be a secondary defence, if the risk could be eliminated completely.

Once the worksite safety concept is formed the requirements in that concept need to be allocated to the subsystems, whether they are machinery, infrastructure systems or anything in between. In this allocation process the interfaces between different systems that are needed to implement the worksite safety concept will become visible. The interfaces between different machines and systems will need to be defined and sufficient requirements set to ensure the integrity of the overall system over the interfaces.

When doing the allocation also the critical paths needed to perform distributed safety functions becomes visible. Now it is possible to analyse effects of failures in one system along the critical path to the overall function. If some level of adaptivity is desired on the operation of the worksite in case of a failure, like it is described in [3] & [7]. The management of degraded modes, or modes where some parts of the system are not functioning correctly or have failed, becomes important. At this stage for example a HAZOP analysis could be performed and design iteration started to define the necessary corrective actions and restrictions for each degraded mode.

The allocation of worksite safety requirements for each subsystem and the interface descriptions between the subsystems, form the output of this process. These requirements become design requirements for each subsystem, which are then to be developed according to their own development processes.

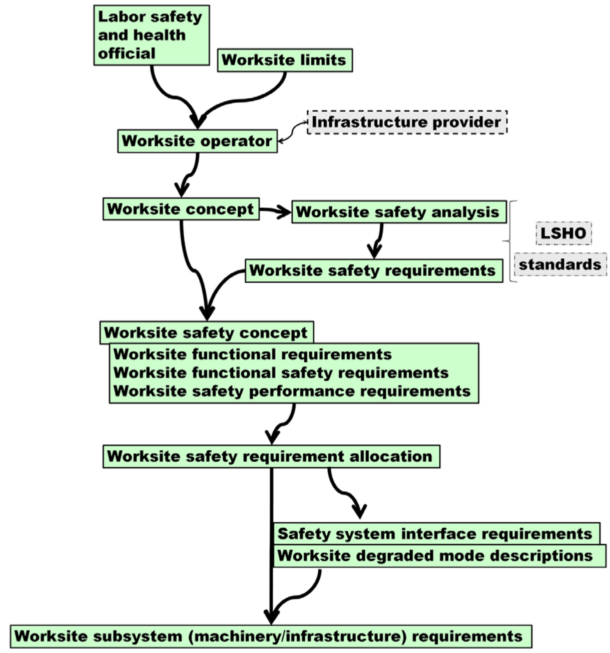

Labor safety and health official
Worksite limits
Infrastructure provider
Worksite operator
Worksite concept
Worksite safety analysis
LSHO
standards
Worksite safety requirements
Worksite safety concept
Worksite functional requirements
Worksite functional safety requirements
Worksite safety performance requirements
Worksite safety requirement allocation
Safety system interface requirements
Worksite degraded mode descriptions
Worksite subsystem (machinery/infrastructure) requirements

Figure 2: Draft development model for worksite level safety functions

The development model was tested in case described earlier in this paper. The worksite concept was formed from seed drill's risk analysis, seed drill's instructions for use, tractor's instructions for use and ISO11783 standards. It was assumed that these instructions already contained the requirements set by the labour health and safety officials and the limits of the worksite, arable farm in this case.

The worksite safety analysis was performed using worksite concept. Work cycle scenarios were crated and analyzed. From this analysis the functional requirement for means to halt the automation and transit to safe state was formed. Also requirement for two different safe states for different work states was set

The worksite safety concept was formed around the ISB requirement definition [2]. Additional functionality for detection of work states was defined. Also required agricultural performance level (AgPL) [4] was set for this functionality.

Safety requirements were allocated to the task controller [5], seed drill, and ISB device [2]. No additional requirements were set to the tractor as the development group had no possibility to make changes to the tractor. It was how ever assumed to fulfil to requirements of ISO

11783-6.The actual functionality was left to the responsibility of the seed drill.

When the requirements were allocated it was clear the functionality laid within the seed drill and that it was dependent on three separate systems: ISB device, Task Controller and the tractor. Now it was possible to define the interfaces and possible degraded modes.

The dependencies were only though ISO 11783 network and the signals between these systems were listed and HAZOP analysis was performed to identify significant signals and their possible failure modes. After the HAZOP analysis FMEA analysis was used to define meaning and defences needed to detect and react to those failure modes. It was also determined, based on these analyses that no degraded modes were allowed and that any failure in any part of the system resulted in to execution of the safety function.

The requirements that resulted from the safety requirement allocation, interface analysis and degraded mode analysis then formed the design requirements related to this function for each system involved.

Discussion

If one takes a look of the drafted development model in figure 1 can see that the process is still quite unrefined. One can also note that in a sense it very much resembles the functional safety lifecycles that are used in standards like IEC 61508 an d ISO 25119. It actually is just scaled-up and unrefined version of the said models.

During the development work, when airline and railway systems were studied three actors were identified that co-operate. The actors are regulative authority, infrastructure operator and service operator. Regulative authorities are actors like Federal Aviation Authority or Railroad authority. These authorities set the requirements for the system and oversee its continuous development. Infrastructure operators are actors like airports, or railroad department that own and operate the rails. Service operators are then the airlines and railroad companies that operate on the infrastructure. These three parties and their relationships are illustrated in figure 3. The co-operation of these actors sets a framework and ensures the overall safety of the system.

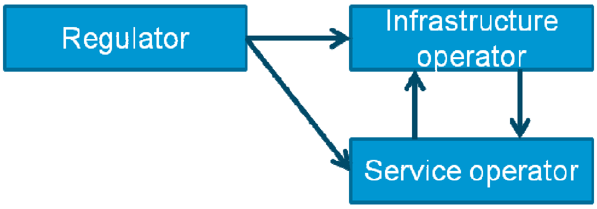


Figure 3: Actors in rail and airway systems

In mobile work machinery environments similar structures can be identified. Sometimes the identification can be more simple and sometimes not. For example in harbour environment the actors are easy to identify and in agricultural environment not. What is different is that in mobile work machinery environments these actors do not co-operate as in railroad and airline sector. Especially the role of regulative authority is much smaller and passive than in transport systems. By regulative authority in this case different national or sector specific labour health and safety officials are meant. This could be that so far there has not been a need for this kind of co-operation or that the risk levels involved are much smaller or that the authorities lack the resources, interest and knowledge to take more active role.

During the development of the use case, the main benefit of the used development model was that it gave the development process structure. This enabled systematic approach to the development.

During the development the systems safety approach [8] was considered a good practice as was the use of scenario based risk analysis. These methods helped in the allocation of safety requirements. During the safety requirement allocation, different requirement allocation leads to very different requirements both in the number of functionalities and in the level of requirements. This means that there is a need for iteration in the draft development model. This iteration is not currently presented in the draft model.

The main shortcoming in the model is the fact that it does not yet describe the roles of actors involved.

Conclusion

As a conclusion it can be said that the drafted development model was useful and beneficial for development of distributed safety functions.

It can also be concluded that the model illustrated in figure is not ready and needs more refinement. Actions in and outputs of each phase are not defined fluently. Also the required inputs from different actors are not properly defined yet. To define the process clearly and to refine it there would be a need to apply the model in several different use cases. In the industry there needs to be more discussion also with other stakeholders on their role and involvement in the development of distributed safety functions.

As with all development models used in the development of safety related parts of control systems there is the problem of aligning the reference development model with developers own development process. The alignment will take time but also it requires that the developers start to keep safety and functional safety as one aspect of the development not as something extra that needs to be carried out for the sake of standard or customer requirement.

One main benefit of these kinds of models is that they exist, bring structure and enable systematic approach and handling of this problem. For a designer this is one more layer of requirements on top of the normal design and safety process.

Acnowledgements

A part of this research is done in the project Agromassi an FAMOUS which are part of FIMECC-program EFFIMA.

References

[1] Agricultural Industry Electronics Foundation. http://www.aef-online.org

[2] Agricultural Industry Electronics Foundation. Guideline for ISOBUS Short Cut Button (ISB)

[3] Tiusanen et.al. Adaptive safety concepts for automated mobile work machine systems : simulator assisted research approach, 2012, Proceedings of the 7th International Conference on the Safety of Industrial Automated Systems

[4] International Standardization Organization. ISO 25119:2010 Tractors and machinery for agriculture and forestry -- Safety-related parts of control systems

[5] International Standardization Organization. ISO 11783-10 Tractors and machinery for agriculture and forestry -- Serial control and communications data network -- Part 10: Task controller and management information system data interchange

[6] International Standardization Organization. ISO 11783-10 Tractors and machinery for agriculture and forestry -- Serial control and communications data network -- Part 9: Tractor ECU

[7] Office of Rail Regulation, RAILWAY SAFETY PRINCIPLES and GUIDANCE

[8] Tisanen et.al. System Safety Concept for machinery Systems, VTT Research Notes 2437, 2008, ISBN 978-951-38-7215

Corresponding address

Vakolantie 55, FI-03400 Vihti, Finland
ari.ronkainen@luke.fi
+358 29 532 6488

SIAS 2015

8th INTERNATIONAL CONFERENCE
ON THE SAFETY OF INDUSTRIAL
AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

Session 3:
Risk assessment

Preventing vehicle-pedestrian collisions: the place of detection systems

Pascal LAMY, Jean-Pierre BUCHWEILLER

Institut National de Recherche et de Sécurité (INRS)- France

Abstract

Every year, employees are the victims of collisions with vehicles in accidents that can be serious and even fatal. In recent years, a range of pedestrian and obstacle detection systems have been developed for vehicles. These systems are often installed on a vehicle following an accident, but this is frequently on a case-by-case basis and it often yields limited success. The purpose of this communication is to place the use of detection systems within a global prevention strategy.

The first steps in the prevention of collision risks consist of setting up organisational measures and ensuring the visibility of drivers in areas liable to present risks of collision; priority should not initially be given to technical solutions. If organisational measures prove insufficient, detection systems, in combination with camera-screen systems, may then be beneficial. Despite their limitations, these systems may be of considerable help in reducing collision risks, by taking into account the type of vehicle used, the task, and the activity performed. The need for detection should therefore first be assessed by taking into account the specificity of the work situation and the definition of the hazardous areas, before then selecting a system capable of partially or completely satisfying that need. The implementation of the system should subsequently be monitored and initial feedback linked to its use should be obtained.

Keywords:

vehicle-pedestrian collision; detection; prevention approach

Introduction

The number of accidents involving people working close to vehicles in the workplace remains unacceptably high, despite the technical progress recently achieved in the development of new equipment and in the training given to drivers. The statistics recorded in the EPICEA[1] database over a ten year period give a number in the region of 200 serious accidents, of which more than half were fatal [1]. These accidents took place in a range of different sectors of activity and involved a number of different types of vehicle, for example in the construction industry (e.g., loaders, levellers, dumper trucks.); in waste collection and sorting (e.g., refuse collection vehicles, self-propelled forklift trucks, loaders); and while handling using a forklift truck (e.g., in the manufacturing industry, the agro-foodstuffs industry and in logistics).

For many years now, detection systems designed for use in the automobile sector have been adapted for use in utility vehicles and advanced technology has also been used in the development of new products [2,3,4]. These detection systems are typically installed on vehicles, often on a case-by-case basis, as a result of demands by prevention officers made in response to user requests following an accident. The effectiveness of these installations is very variable and depends on the awareness of the different actors and on their understanding of the equipment and situation. In order to ensure the success of this type of technical solution and to provide a pertinent response, it is necessary to reposition the detection system within a global prevention strategy.

The general prevention approach

Prevention measures and pedestrian detection

In the framework of preventing vehicle-pedestrian collisions, it is possible to act at several levels:

1. eliminate or reduce the risk at source,
2. take necessary protective measures regarding non eliminated risks,
3. inform the users of residual risks when protective measures are incomplete.

Preventive measures must combine:

- **organisational-type measures, such as the organisation of vehicle and pedestrian flows, controlling access to hazardous areas, the provision of specific waiting areas for drivers, etc.**
- **technical measures that aim to improve visibility.**

If these measures are insufficient, additional technical measures such as pedestrian detection systems can then be considered.

Man-machine interaction, which often occurs in a confined space, is always a source of danger and a lack of visibility from the driver's cab is a significant factor in many accidents.

[1] EPICEA is an anonymous French database containing more than 20,000 cases of occupational accidents affecting employees and covered by the social security system. These accidents are fatal, serious or significant from a prevention standpoint. The EPICEA database is not exhaustive as it does not reference all accidents.

A driver must be able to see pedestrians located close to the vehicle both directly and indirectly at all times (“Machines” directive 2006/42/EC).
The driver of the vehicle can then decide on the best driving strategy to adopt according to visual information gathered from the environment in order to prevent the risk of collision with pedestrians or other vehicles operating in the same workspace.

In order to achieve the optimum solution for prevention of collision, it is often necessary to combine use of the visual aid system with a detection system.

Visual aid systems (rear view mirrors and camera-monitor systems) can improve visibility in areas that present a risk of collision. However, when a driver is concentrating on the task in hand they are not always able to divide their attention between the different sources of information and do not always pay enough attention to their rear-view mirrors or to a control screen. Thus, to complete these visual aid systems, the installation of pedestrian and obstacle detection systems might be considered. The use of these devices is nevertheless limited as they cannot respond effectively in every situation. They are not safety components and therefore cannot be used as protective measures. However, they can be used advantageously to obtain information and to warn the driver, and possibly third persons, in the case of an imminent collision. In such situations, their use as a warning system falls within a global strategy for preventing vehicle-pedestrian collision risks.

No universal detection system has so far been developed. A system used in isolation cannot cover every situation of risk linked to the movement of a vehicle and any system may be capable of producing a non-detection or false detection. It is not desirable that systems act automatically on the brakes. Instead, they should be reserved for warning the driver or the person at risk so that in a potentially dangerous situation, the driver can stop their vehicle immediately.

The presence of this type of device on a vehicle in no way waives the need to conform to existing safety regulations in the workplace. Even though the driver is the main actor, the entire organisation of work is therefore involved. Among other things, the use of a detection device requires that the driver can see the area at risk, even if only indirectly. The driver must have been given training on how to use the system, its limitations, and precisely what instructions to follow when a warning signal is triggered.

Prevention by pedestrian detection: approach

The objective of this type of prevention strategy is to fully define the need prior to installation of any detection system. The person responsible for designing the strategy should be a prevention officer employed by the company. In the framework of a work group, the prevention officer should conduct an analysis for each vehicle and must not forget to assess all vehicles involved in cases where multiple vehicles are operating within the same work area or site.
The approach is iterative in that it is only relevant if a consensus has been reached and if all of the decisions and elements that led to these decisions have been documented.

A prevention strategy that looks to incorporate use of a detection system is divided into three main phases:

- Analysis of the work situation in order to: (i) describe the general situation and identify any dangerous work situations; (ii) assess visibility from the driver’s cab in dangerous areas; and (iii) estimate and evaluate the risks of collision in order to determine which situations should be dealt with first.

- Specifying the detection system, in order to decide whether or not a detection system is a viable solution given the risk assessment, and then creating a list of devices capable of satisfying this function.

- From this list, selecting those technical solutions that are capable of satisfying the specified function. This is achieved by defining any additional measures required, for example training, assistance, measures to ensure the effective operation of the device (e.g., periodic checks) and implementation of the solution (utilisation, driver’s opinion).

Comment: for further details of the global prevention strategy and a description of the detection techniques considered, see [5,6].

A prevention strategy with detection case-study : the example of a loader in a confined space

Insofar as a decision has been made to use technical systems after giving consideration to making improvements to work organisation and visibility, in this section, we describe the development of a prevention-by-detection strategy for the case of a loader moving on a confined site in which all types of waste are recycled (glass, paper, cardboard, wood, etc.). This example is provided as a demonstration of the prevention-by-detection strategy and should not be generalised for a vehicle of the same type operating in another environment or site. It is not exhaustive and certain choices were made on the basis of the particular field conditions and constraints of the company concerned. Above all, our example serves to support the premise and it must not be transposed in is current form to any similar situation in another firm or worksite.

Phase one: analysis of the situation

The aim of this phase of the strategy is to answer a number of basic questions:

What are the characteristics of the site? What type of vehicle is involved, what activity does it perform and under what conditions? What activities does the driver perform and where are they performed? What types of risk are present around the vehicle? How many pedestrians are present, why are they there, where are they located and are they present during the activity itself? Where are the areas in which the vehicles and pedestrians circulate and are these areas visible from the driver's cab? If so, is visibility partial or complete? Which risk situations should be prioritised?

In our example, the loader moves in a temporary storage area where the loading of trucks is carried out (this is a temporary storage area for material that arrives by truck and is then transferred to other sites). The loader moves on the site in order to remove piles of material and then load trucks with this material. The pedestrians present on the site include work colleagues, the drivers of trucks/vans belonging to the company and/or other companies, and visitors. Other vehicles are present. Obstacles are present both in front of the loader (linked to its activity) and behind it. The driver is unable to constantly survey the area when moving due to the activity being performed. Two types of movement can be distinguished: manoeuvring phases (loading, piling, scraping the ground, etc.), defined as 'starting/restarting', and rolling phases, defined as 'nominal speed' (movement from one work area to another).

In this analysis phase, all of the different movements are involved and the procedure must be performed exhaustively (for example, forward movement (re)starting, forward travel at nominal speed, reverse travel at nominal speed). In the following description, we do not describe every risk situation identified, but instead focus on the starting/restarting in reverse phase. Our identification of the dangerous situations shows risks at the rear of the vehicle for reverse travel when (re)starting (Fig. 1).

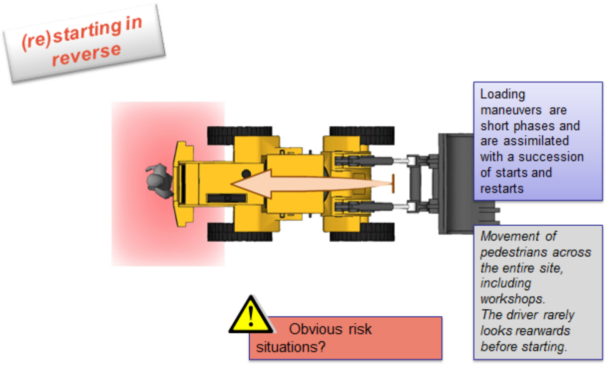

(re)starting in reverse
Loading maneuvers are short phases and are assimilated with a succession of starts and restarts
Movement of pedestrians across the entire site, including workshops. The driver rarely looks rearwards before starting.
Obvious risk situations?

Figure 1. Identification of dangerous situations at the rear of the vehicle on (re)starting in reverse.

Dangerous situations also exist at the sides during the same phase of movement (figure 2).

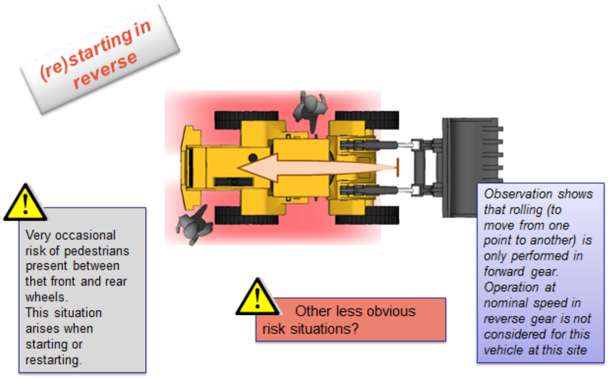

(re)starting in reverse
Very occasional risk of pedestrians present between thet front and rear wheels. This situation arises when starting or restarting.
Other less obvious risk situations?
Observation shows that rolling (to move from one point to another) is only performed in forward gear. Operation at nominal speed in reverse gear is not considered for this vehicle at this site

Figure 2. Identification of dangerous situations at the sides of the vehicle on (re)starting in reverse.

We do not consider the case of reverse travel at nominal speed here, not because there is no risk but because this type of movement should not be encouraged. Care must be taken to ensure that these types of long movement sequences are only performed with the vehicle moving forwards.

Having identified the dangerous situations, the visibility of these areas must now be assessed (Fig. 3). In reverse motion, a dead angle exists behind the counterweight (of about one meter). A device that allows the driver to check the area visually (rear view mirror, camera, etc.) should therefore be envisaged.

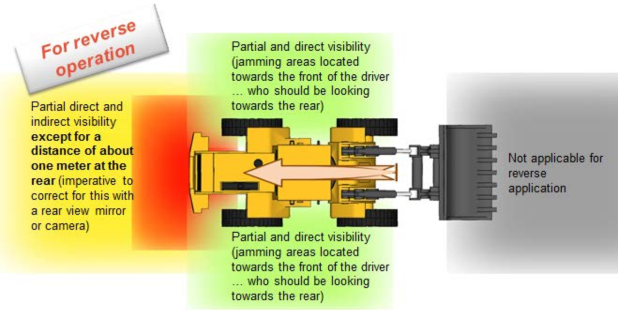

For reverse operation
Partial direct and indirect visibility **except for a distance of about one meter at the rear** (imperative to correct for this with a rear view mirror or camera)
Partial and direct visibility (jamming areas located towards the front of the driver ... who should be looking towards the rear)
Partial and direct visibility (jamming areas located towards the front of the driver ... who should be looking towards the rear)
Not applicable for reverse application

Figure 3. Assessment of visibility from the driver's cab.

Finally, it is necessary to determine which risk situations should be prioritised. This is achieved by taking into account the importance of risks related to collisions, any incidents or accidents that have been observed, and the choices made by the company. The selection of high-priority situations requires consideration by a work group. This is subjective but is an essential step that allows the actions to be ranked in terms of priority given the experiences of the company and its "prevention" policy. In particular, it takes into account the severity of the damage, and the frequency and duration of exposure to risk. Following our full assessment of the vehicle in this example, the situation to be treated first involves the risks located at the rear of the vehicle on starting in reverse gear. Second are the risk situations located at the front of the vehicle when starting in forwards motion and, third, the risk situations at the side of the vehicle when starting in reverse gear. The other risk situations are not described here.

When (re)starting in reverse gear we note the major risk that exists at the rear of the vehicle and, the lesser, though non-negligible risk that exists at the sides (Fig. 4).

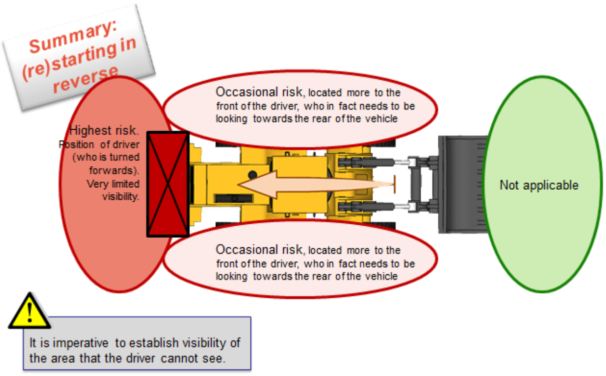
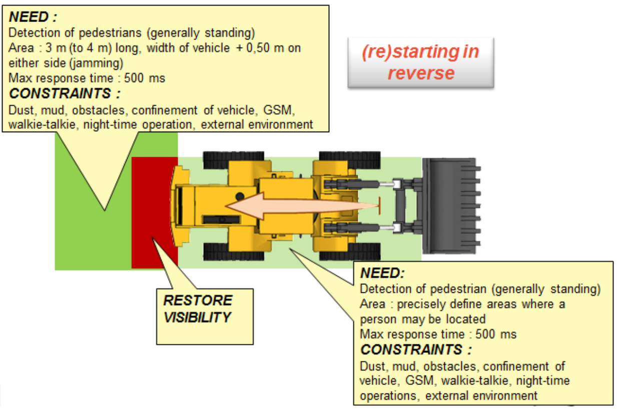

Summary: (re)starting in reverse
Highest risk. Position of driver (who is turned forwards). Very limited visibility.
Occasional risk, located more to the front of the driver, who in fact needs to be looking towards the rear of the vehicle
Occasional risk, located more to the front of the driver, who in fact needs to be looking towards the rear of the vehicle
Not applicable
It is imperative to establish visibility of the area that the driver cannot see.

Figure 4. Risks identified when (re)starting in reverse gear.

Phase two: expressing the need for detection and establishing an inventory of technical solutions

The aim here is to consider the situations in which a detection system might be used (wholly or partially), to consider whether commercially available systems can satisfy this demand, and then to decide on whether to continue this assessment for the risk situations listed. This step must be carried out with the participation of the company. The desired function of the detection system is first specified: what must be detected (a person, posture, etc.), where (define the detection area), under what conditions (specify the constraints, for example night work, presence of mud, dust, etc.), and within what time-limit (response time for stopping the vehicle)?

For reverse manoeuvring, we continue with our examination of the (re)starting phases. It is important to bear in mind that a blind angle exists at the rear, and that the specific need is that the driver can see this area. We assume that the vehicle moves at a speed below 5 kph during the starting/restarting phases, and that it is necessary to detect a person entering and/or located within the detection area. The postures to be detected is a standing or leaning posture, the width of the detection area is the width of the vehicle increased by 0.5 m on either side to take into account the risk of crushing of jamming at the extremity of the vehicle. Regarding the constraints, the presence of obstacles and the possible confinement of the vehicle in certain areas, which could trigger over-frequent detections, both need to be taken into account. In addition, it is also necessary to take account of the vehicle's movement in an external environment and the use of a cell phone or walkie-talkie on the site. These configurations are summarised in Figure 5 for the case of starting in reverse gear.



NEED :
Detection of pedestrians (generally standing)
Area : 3 m (to 4 m) long, width of vehicle + 0,50 m on either side (jamming)
Max response time : 500 ms
CONSTRAINTS :
Dust, mud, obstacles, confinement of vehicle, GSM, walkie-talkie, night-time operation, external environment

(re)starting in reverse

RESTORE VISIBILITY

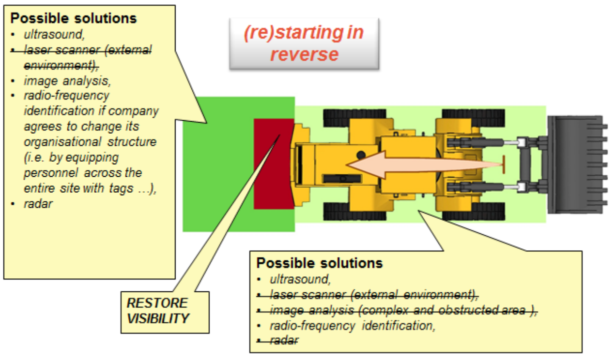
NEED:
Detection of pedestrian (generally standing)
Area : precisely define areas where a person may be located
Max response time : 500 ms
CONSTRAINTS :
Dust, mud, obstacles, confinement of vehicle, GSM, walkie-talkie, night-time operations, external environment

Figure 5. Expressing the need for detection while (re)starting in reverse gear and constraints linked to the activity.

Comment: the precise definition of a detection area requires knowledge of the vehicle's stopping distances (attention must also be given to the mental load of the driver and its impact on the stopping distance). A detection distance of 3 m was judged sufficient in this case, but more precise information must be obtained to ensure that the vehicle stops in time. Aiming for a long detection distance is futile since few systems currently on the market are capable of this. Furthermore, the further the detection distance required, the more likely it is to lead to a false detection.

Regarding the list of possible solutions, the aim here is to take into account the compatibility of the detection principles with the requirements specified for the purpose of the detection system and the organisation of the site. This list depends on the work group's understanding of detection principles and the time required to carry out the operation. However, certain solutions may be eliminated later, during the last phase of selection and implementation. The selection can be made from five possible types of technology: a laser scanner (a measure of time of flight), ultra high frequency radar, ultrasound (commonly known as a rear parking aid), radio frequency identification (RFID) or electro-magnetic waves badge and a camera with image analysis.

The possible technical solutions for our example of reverse manoeuvring are presented in Figure 6.



Possible solutions
- *ultrasound,*
- ~~*laser scanner (external environment),*~~
- *image analysis,*
- *radio-frequency identification if company agrees to change its organisational structure (i.e. by equipping personnel across the entire site with tags …),*
- *radar*

(re)starting in reverse

RESTORE VISIBILITY

Possible solutions
- *ultrasound,*
- ~~*laser scanner (external environment),*~~
- ~~*image analysis (complex and obstructed area),*~~
- *radio-frequency identification,*
- ~~*radar*~~

Figure 6. Possible detection solutions for the case of (re)starting in reverse gear.

Phase three: selection and implementation

The final phase of the prevention strategy consists of choosing one (or more) technical solutions and then implementing this solution in the workplace. Key questions include: what systems should be chosen; what instructions should be given to the driver to follow when an obstacle is detected and for checking the system; how can a driver be encouraged to accept the system; how should feedback based on user experience be dealt with? and, if it's relevant, any difficulties that the driver has with the system should give rise to a correction.
When choosing the system it is obviously necessary to examine those that are capable to respond to the specified detection function. Complementary measures - for example technical, organisational, assistance for implementation and use, or training – should also be defined. Abandoning recourse to a detection system remains possible if, for example, the system does not (or only partially) cover(s) the specific need or if the organisation of the site is incompatible with the solution considered.

For example, in our case study, the company did not want to modify its existing organisation by ensuring that all personnel carried a radio frequency badge, and this particular solution was therefore impossible. The options for the (re)starting in reverse gear phase are summarised in Figure 7.

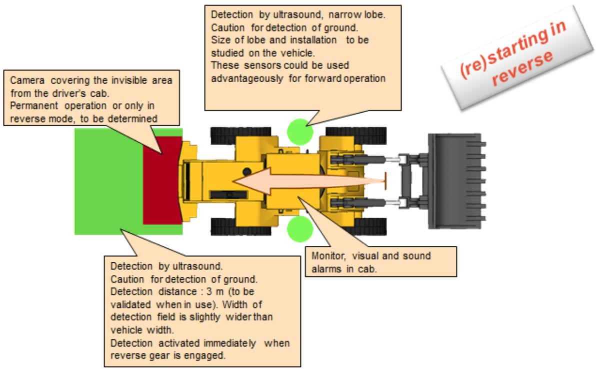

Detection by ultrasound, narrow lobe.
Caution for detection of ground.
Size of lobe and installation to be studied on the vehicle.
These sensors could be used advantageously for forward operation
(re)starting in reverse
Camera covering the invisible area from the driver's cab.
Permanent operation or only in reverse mode, to be determined
Detection by ultrasound.
Caution for detection of ground.
Detection distance : 3 m (to be validated when in use). Width of detection field is slightly wider than vehicle width.
Detection activated immediately when reverse gear is engaged.
Monitor, visual and sound alarms in cab.

Figure 7. Detection solution chosen for the (re)starting in reverse gear operation.

These particular options were obtained from group work within a specific company. They may be different in another companies or situations. Detection at the rear should only be operational at low speed to be compatible with the vehicle's stopping time. The installation and programming parameters must be determined precisely under real conditions. Detection will not cover perpendicular trajectories between the vehicle and pedestrians or persons lying on the ground.

Regarding implementation, care must be taken not to reduce visibility from the driver's cab. Installation of the system on the vehicle must take into account exposure to impacts, different types of projection, resistance to vibrations, accessibility for cleaning; training the driver to use the system, the limits of the system, setting out precise instructions to follow when an alarm is activated (stop), checking for efficient operation (for example, by the driver at the start of his shift or her shift), and communication of any difficulties observed in order to avoid rejection of the system.

Once the system has been implemented, an initial rapid assessment, followed by regular follow-up assessments, should be made (covering, for example, its utilisation, the opinion of the driver and the detection distance). On the basis of these assessments, the installation and programming may require modification or additional measures may be required to complete the system. Finally, acceptance of the system by the personnel is crucial to the success of the project. The personnel should therefore be involved in the design of the prevention strategy as early as possible.

REFERENCES

[1] MARSOT J., CHARPENTIER P., TISSOT C., *Collisions engins-piétons : Analyse des récits d'accidents de la base EPICEA*, Hygiène et Sécurité du Travail, ND 2318, 4ème trimestre 2009, 217, pp. 23-32.

[2] GARDEUX F., *Pedestrian collision avoidance: a multi-sensor approach for pedestrian detection transpose from automotive to mobile machine*, SIAS 2010, 6th International Conference of the Safety of Industrial Automated Systems, TAMPERE, 14-15 June 2010.

[3] KLEIN R., *Mobile plants-pedestrians collision avoidance - Personnel detection by means of radio waves*, SIAS 2010, 6th International Conference of the Safety of Industrial Automated Systems, TAMPERE, 14-15 June 2010.

[4] GAYRAUD F., ALLEZARD N., LUCAT L., MANSUY P., Pedestrian detection for industrial vehicles based on morphological recognition : first feedback after 18 months of operation, SIAS 2012, 7th International Conference of the Safety of Industrial Automated Systems, MONTREAL, 11-12 October 2012.

[5] LAMY P., CHARPENTIER P., LE BRECH A., BUCHWEILLER J.P., KLEIN R., BERTRAND P., MARSOT J., GARDEUX F., TIHAY D., Prévenir les collisions engins-piétons - Dispositifs d'avertissement, INRS, Paris, ED 6083, 60 p.

[6] LAMY P., BURY M., HELLA F., ZORE F., PAYET R., BUCHWEILLER J.P., JEGEN N., LUX A., WILD P., *Les bonnes pratiques pour prévenir les collisions engins-piétons*, HST 236, septembre 2014, pp. 22-38.

Corresponding address

1 rue du Morvan - CS 60027
F-54519 VANDOEUVRE cedex
pascal.lamy@inrs.fr

From risks to requirements – a round robin test

Timo Malm[1], Tor Stålhane[2], Charlotte de Bésche[3], Outi Venho-Ahonen[1] & Marita Hietikko[4]

[1]VTT Technical Research Centre of Finland Ltd, Tampere, Finland
{timo.malm, outi.venho-ahonen}@vtt.fi
[2]Norwegian University of Science and Technology, Trondheim, Norway
stalhane@idi.ntnu.no
[3]SP Technical Research Institute of Sweden, Borås, Sweden
{charlotte.debesche}@sp.se
[4]VTT Expert Services Ltd, Tampere, Finland
{marita.hietikko}@vtt.fi

Abstract

It is important to define the correct required safety level for safety-related control systems. A too high level causes exaggerated costs, since more components and validation resources are required to reach a higher level of safety. On the other hand, a too low level causes too low safety requirements and the risk for an accident will thus increase. The most important methods to assess risks and define corresponding requirements for control systems in the machinery sector are the ISO 13849-1 [5] and IEC 62061 [6] methods. We have run a round robin test to study how safety assessors estimate the parameters of risks and find the required SIL (Safety Integrity Level) and PL (Performance Level). The goal is to compare the properties of the methods. ISO 13849-1 has fewer parameters and the scale is simple (1 or 2), but the result has six levels, including a zero level. IEC 62061 has more dynamics in its parameters, but the result has only four levels, including a zero level.

We used nine cases related to mobile work machines and seven cases related to industrial robots. So far we have had 19 answers to the mobile work machine experiment and 17 answers to the robot experiment. For each mobile work machine case there was also a standard example, which resembled our case and it was therefore possible to compare the results to the result given by the standards. This paper will present the results of the experiment and discuss the reasons for the observed outcome and what should be done to obtain a more correct and uniform safety assessment.

Keywords:

risk assessment, safety, machinery, 13849-1, 62061

Introduction

It has been observed that 40 % of the faults contributing to programmable electronic systems related incidents emerge during the safety requirements specification phase of a system life cycle [1]. In addition, an average of 30 % of the software related defects are made in the requirements specification phase. The share is, however, much higher (60%) for excellent (almost fault free) software [4]. The major part of defects origin at the early life cycle phases of programmable electronic systems. Therefore, it is important to focus on the early life cycle phases of systems: safety requirements specification and risk assessment.

In the CompSoft project engineers and other specialists were asked in an online enquiry, which methods are applied in the machinery sector for risk assessment. A total of 72 answers were gathered from Finland, Sweden and Norway. According to the answers almost 70% applied ISO 13849-1, over 40% applied ISO 12100, over 30% applied IEC 61508 and less than 30% applied the IEC 62061 method in risk analysis – it was possible to choose more than one alternative. This means that the methods applied (ISO 13849-1 and IEC 62061) are quite relevant when considering the risk levels and corresponding control system requirements (Safety Integrity Level=SIL or Performance Level=PL).

When analysts perform risk assessment they get different results depending on their background. Risk assessment should result in specific PL or SIL demands in order to set requirements for the control systems. Too strict requirements lead to expensive systems and too low requirements cause systems to be unsafe.

In round robin tests the test persons analyse identical cases. In our case two methods are applied for each case. The applied methods result in SIL (IEC 62061) and PL (ISO 13849-1) requirement levels for the safety function of a control system. In most cases the safety function is supposed to be obvious, but it was possible to leave the question empty, if the question or safety function remains unclear.

The general objective of the project is to support risk assessment and safety requirements specification phases of safety related control system design by combining well-tried methods, techniques and principles. The aim is to apply the IEC 62061 (annex A) and ISO 13849-1 (annex A) standards, and to find ideas for how to improve or integrate them to support the design process better. This paper shows the results of the round robin test and some ideas for future development.

Parameters of risk

Risk assessment can be done for several purposes, such as defining hazards and their consequences, comparing risks and defining significant risks and related requirements. The purpose of the risk assessment here is to define risks and corresponding requirements. When the hazard is found and the relating significant risks are identified, we must also define requirements that can be used to minimize the risk.

The two standards used in the experiment are both based on the idea that the assessor shall assign values to parameters through a qualitative scheme – e.g. according to ISO 13849-1 "Possible to avoid" gives Av = 2. The EN 62061 standard [6] has four parameters – see Table 1and Table 2, while ISO 13849-1 standard [5] only has three parameters – see Figure 1.

Table 1. The SIL requirement parameters according to IEC 62061

Frequency and duration Fr		Probability of hzd. event, Pr		Avoidance Av	
<= 1 hour	5	Very high	5		
>1hour - <= day	5	Likely	4		
>1 day - <= 2 weeks	4	Possible	3	Impossible	5
>2 weeks - <= 1 year	3	Rarely	2	Possible	3
>1 year	2	Negligible	1	Likely	1

Table 2. The SIL requirement estimation according to IEC 62061.

Consequences	Severity Se	Class Cl = Fr + Pr + Av				
		3 – 4	5 – 7	8 - 10	11 - 13	14 - 15
Death, losing an eye or an arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3
Reversible, medical attention	2			OM	SIL 1	SIL 2
Reversible, first aid	1				OM	SIL 1

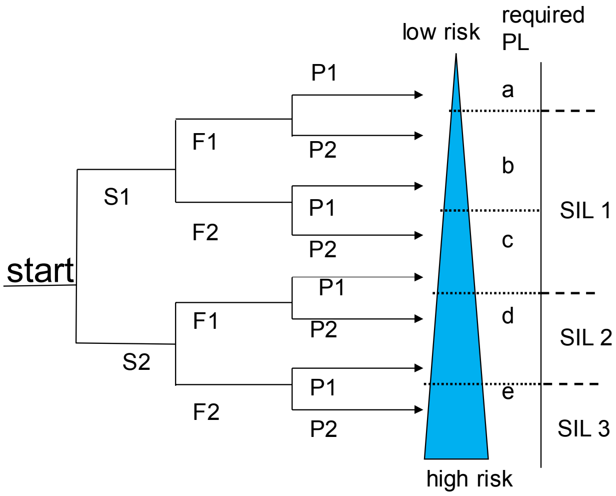


Figure 1. ISO 13849-1 decision tree for risk assessment.

ISO 13849-1 uses a decision tree to assign a risk to a system. The model uses three factors: S (severity) with the values S1 – slight injury and S2 – irreversible injury, F (occurrence frequency) with the values F1 – seldom and F2 – frequent or continuous and P (possibility to avoid the consequences) with the values P1 – possible to avoid under specific conditions and P2 scarcely possible. The decision tree is shown in Figure 1.

When we want to compare these two models for risk assessment, there are some problems that need to be addressed.

- The ISO 13849-1 has two alternatives for each of the parameters severity, frequency, exposure and avoidance, while EN 62061 has four alternatives for severity, five values for frequency and exposure and three alternatives for avoidance. In addition, EN 62061 has an extra parameter – the probability of the hazardous event.
- The ISO 13849-1 has five risk levels – a to e – of which four are mapped onto three SIL levels and "PL a" corresponds to SIL 0. As a consequence of this, both "PL b" and "PL c" are mapped onto SIL 1.
- The ISO 13849-1 uses a conditional probability Pr to assess P(danger | event). Considering that most people, including safety assessment experts, have problems assessing probabilities, a conditional probability might be beyond their capability. See for instance [7].

Round robin tests

The mobile work machine experiment and the robot experiment are realized by applying a round robin test. The purpose is to compare the two risk assessment methods, which are used to give us the requirements for the safety functions. Our aim is to evaluate how objective the methods are and discover if there is a difference between the methods. All the parameters gathered in the assessment are also evaluated in order to see how the parameters affect the results.

The methods used in the risk estimation are based on the SIL assignment process presented in EN 62061 and the risk graph for determining required PL_r for safety function presented in ISO 13849-1. In all cases the risk analysis text was prefilled and only the parameters should be filled in. All the test persons conducted the risk assessment for nine cases (either robot or mobile machine cases) and both used both the IEC 62061 and the ISO 13849-1 method. Background information of the persons or groups that analysed the cases was also collected.

When calculating average values in the round robin tests, the PLs are converted to SILs according to the following formula, using linear interpolation between the fixed numbers/letters (see Figure 4 and Figure 5):

$$\text{PL a}\rightarrow 0.5;\ \text{PLb}\rightarrow 1;\ \text{PL c}\rightarrow 1.3;\ \text{PL d}\rightarrow 2;\ \text{PL e}\rightarrow 3 \qquad (1)$$

Both SILs and PLs use a logarithmic scale and therefore comparison between them can be applied in corresponding parts of the scales for average calculations. All the other transformations are according to ISO 13849-1 probabilities, but “PL a” has no equivalence to SIL and is set to the middle value between SIL 0 (almost no risk) and SIL 1, which gives us a rough estimation and keeps the numbers easier to apply. SIL 0 is not described in the standards, but we assume that the distance from SIL 0 to SIL 1 is the same as from SIL 1 to SIL 2. This definition is more like risk and severity perspective than probability perspective since the probability of SIL 0 is not defined.

Mobile machine experiment

There are nine mobile machine cases related to tractor loaders, articulated wheeled loaders (loaders with a pivot joint, which allows the vehicle to “bend” or pivot on that joint), steel tracked dozer and movable elevating work platforms. The cases were selected from ISO/TS 15998-2 [9] and EN 280 [8] in order to enable us to compare our results to the standard’s results. The case descriptions are short since the texts were from the standards, which aim to have relatively wide scope. The applied examples are not in the normative part of the standards. All case descriptions gave hints to aid the analyst in choosing severity, frequency, exposure and possibility to avoid hazard, which are related to the parameters of risk. The analyst needed to estimate the required parameters for each case and the template (Excel) calculated the corresponding risk level (SIL and PL). The nine cases were chosen so that the cases cover both high and low risk examples. According to the corresponding machine standards (ISO/TS 15998-2 and EN 280), performance levels (PL) 0, a, b, c, d and e were included. The analysis was typically made in about 40 minutes, which indicates that the information for each case is quickly understood and analysed.

An example of the figure and case description is shown in figure 2.

Figure 2: Figure for case 1

Case: Tractor Loader- Backhoe Traveling <40 km/h Unexpected brake apply. Machine stops very abruptly, and may skid. Steering remains functional, but is limited. Bystander may be crushed between machine and hard surface. Bystander may be run over.

Robot experiment

The robot experiment resembled the work machine experiment in its setup, but with the difference that the nine hazards were all collected from the same robot cell. The cases are unfortunately not found in any standard, but they are possible real life cases. The robot test was sent to persons from institutes working with risk assessment and persons from the industry.

To have some kind of “right” answer to compare our results to, an expert assessment was made by two persons working with risk assessments. All personnel involved in making the cases were included from the experiment.

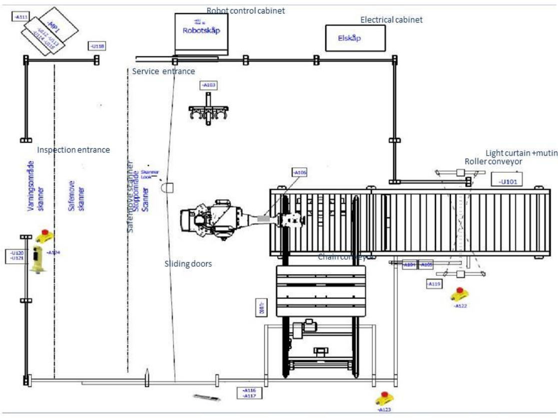


Figure 3: Robot case diagram

The robot cases have a more detailed description than the machinery cases as shown in the example below:

- **Hazard:** Moving elements
- **Hazardous event:** Robot or machine moves in unpredictable way or speed.
- **Harm:** impact/ punch/ crushing
- **Foreseeable sequence of events:** Unintentional impact on operating devices. Workers unintentionally impact operating device, e.g., changing speed or range of robot or starting chain conveyor.

- **Hazardous situation (when):** The system stands near a passage/entrance in a factory. Many people pass by. Both visitors and different workers.

Results of the experiments

The results of the mobile work machine experiment and robot experiment are first considered separately and then common features are discussed in the summary part of the section.

Mobile machine experiment results

Table 3 and Table 4 show how the test persons have answered the mobile work machine cases. On the left hand side of the tables we show the PL/SIL levels and at the bottom is the case number and above this, the answer suggested by a standard. The bold numbers (value can be seen also at the std. row) indicate the risk levels suggested by the standard. We see that there is some variation in all the nine cases although the average is usually the most common answer. This is true both for SILs and PLs. The SIL estimation concentrates on SIL 2 although according to the suggestions in the standards the results were more spread. There is slightly more variation regarding PLs than SILs.

Table 3. The number of answers to the mobile work machine cases according to the ISO 13849 method.

PL

e	0	0	1	0	2	1	2	6	3
d	9	6	4	12	9	10	2	5	2
c	8	12	11	4	7	7	2	5	7
b	1	0	1	2	1	0	4	1	1
a	0	1	2	1	0	1	7	1	5
0	1	0	0	0	0	0	1	1	0
std	-	c	b	c	e	d	c	d	c
Case	1	2	3	4	5	6	7	8	9

Table 4. The number of answers to the mobile work machine cases according to the IEC 62061 method.

SIL

3	1	1	1	3	2	3	1	9	3
2	15	14	10	11	15	12	2	4	4
1	1	0	2	3	2	2	3	3	3
0	2	4	6	2	0	2	12	3	8
std	-	c	b	c	e	d	c	d	c
Case	1	2	3	4	5	6	7	8	9

Figure 4 shows PL values converted to SIL values according to formula (1). In most cases the analysts arrived at roughly the same results as the standards, but in cases 1 and 5 the results were different. In case 1, the standard estimates that the risk is low (SIL 0), whereas the mean value of analysts is about 1.5. In this case the driver may hit his head to the windshield at low speed or drive over a bystander because of braking. The standard assumes that heavy braking is possible in a case of failure and no means, e.g., ABS, are required to decrease braking. In case 5, the standard risk/requirement is SIL 3, whereas the average is less that SIL 2. In this case steering is lost while the machine may be in traffic. The traffic possibility is, however, not specifically mentioned in the text. When a machine may be driven in traffic the risk is estimated to be high. In both of these cases additional knowledge about the risk levels and more time for the analysis could have resulted in answers which are closer to the standards.

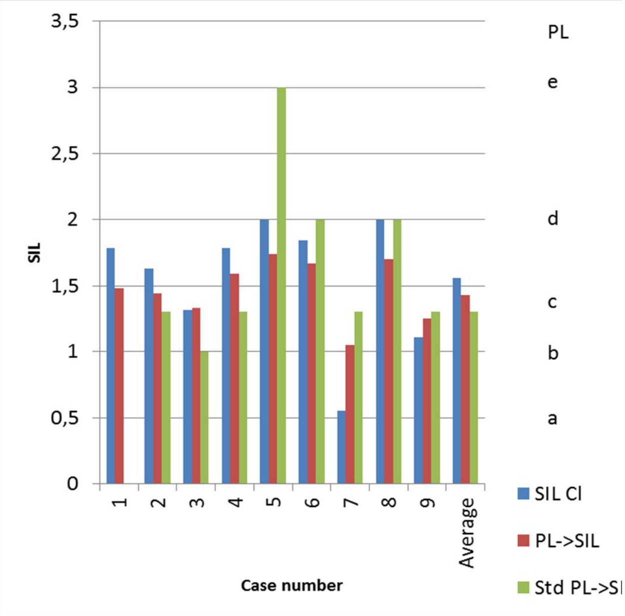


Figure 4. The average value and standard suggestion for each mobile machine case.

Robot experiment results

Table 5 and Table 6 show the answers of the robot experiment. In the tables the "correct answer" according to the expert group, are in bold and can be seen also at the std. row. For case 1 and 8 there is no right answer since no safety functions are needed. The graphs look similar, as should be expected.

Table 5. The number of answers of the nine robot cases according to the ISO 13849 method.

PL									
e	1	1	1	0	2	5	0	0	3
d	3	12	7	9	3	5	10	4	8
c	2	4	9	6	3	3	7	1	5
b	0	0	0	0	6	3	0	1	0
a	1	0	0	0	3	1	0	0	1
0	0	0	0	0	0	0	0	0	0
std		c	a	c	e	d	c		d
Case	1	2	3	4	5	6	7	8	9

Table 6. The number of answers of the nine robot cases according to the IEC 62061 method.

SIL									
3	1	2	1	1	1	8	2	0	2
2	2	14	12	12	5	3	13	2	11
1	1	1	2	0	5	3	2	4	2
0	3	0	2	2	6	3	0	0	2
std		2	1	2	2	2	2		2
Case	1	2	3	4	5	6	7	8	9

Figure 5 shows the average answers to each case.

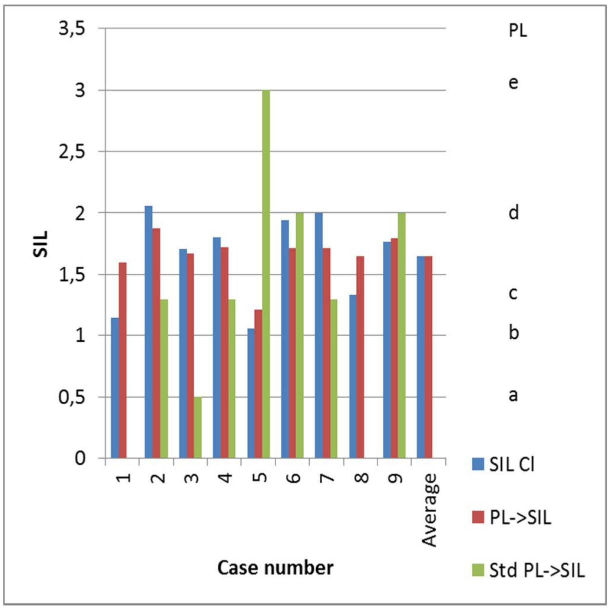


Figure 5. Average values for each nine robot cases and the expert judgement.

In general, it is more common to assess the risk to a value higher than, or equal to the recommended value than that it is assessed to a lower value.

Case 5 was generally assessed to a much lower level than the expert judgement. In this case a product was dropped by the robot and an access button was the safety means. The difference between the assessors' and the expert judgement was probably due to too little information about the system and the case.

Case 3 was generally assessed to be at a higher risk level than the expert assessment (c instead of a). The case was about unintentional start-up and interlocking doors were the safety means. According to the case description there are instructions for service technician to always use a padlock on the door before going into the cell to make sure the door cannot be closed and interlocked. The mitigation by instructions for padlock shall be calculated into the assessment according to IEC 62061, but people seem to have missed this information.

Summary of the experiments

Table 7 shows a cross-tabulation of the SIL and PL answers from both the mobile work machine and the robot cases. Each cell shows how many times the analysts choose specific PL (ISO 13849 method) and for the same case corresponding SIL (IEC 62061 method). The cells with text in bold indicate the equivalence between SILs and PLs, i.e. if all numbers were in these cells all test persons would have arrived at the same risk levels with both methods. However, we see that the bottom left corner has more values (97) than the top right corner (50). This indicates that the test persons have assessed the risks to be higher when applying the IEC 62061 standard than when using the ISO 13849 standard. The difference is clear when the risk is at the intermittent level – close to PL c. For example: in 62 out of 93 cases the test persons estimated the risk level to be SIL 2 when in the same cases the PL assessment was PL c. The calculated average value for the robot experiment of the methods was about the same (see Figure 5, the average column), but at the mobile machine experiment the IEC 62061 standard gave slightly higher values (see Figure 4). The total average SIL when applying the IEC 62061standard is 1.6, and applying the ISO 13849 standard is 1.3 (transformation according to formula (1)).

Table 7. Cross-tabulation of all mobile machine and robot cases.

SIL \ PL	0	a	b	c	d	e
0	3	21	10	16	5	2
1	0	3	8	18	9	1
2	0	0	2	68	84	7
3	0	0	1	1	22	18

Table 7 shows also that SIL 0 is chosen much more often than PL 0 – 57 vs. 3 times. PL a corresponds to SIL 0, but yet there is disproportion between PL 0/PL a and SIL 0. When studying the answers more closely we see that when applying the IEC 62061 method, the severity factor is often set to “1” or “2” which often results in SIL 0. In addition, SIL 3 is chosen more often (40) than PL e (27).

We registered the expertise of all analysts and in most cases the persons did have several areas of expertise. For the mobile work machine experiment we used the expertise groups risk assessment, automation, machinery, research and work machines. For the robot experiment the expertise groups were electronic components, robots, software, system integrator and distributor/agent. In both cases the amount of test persons in each group was relatively small and there was also overlap between the groups.

The differences between the expertise groups were relatively small. In mobile work machine experiment the lowest risk levels were given by the work machine experts i.e. the persons who know best the work machines. The average value for work machine experts was SIL 1.37 and the total average was SIL 1.64 according to IEC 62061 method calculations. In the robot experiment the robot specialist evaluated the risks to be at a slightly higher level than the other participants. The value was SIL 1.78 and the average was SIL 1.67. Based on the data available, we cannot say that the experts who know the specific technology give lower or higher risk level answers than other technology experts.

Discussion

The round robin test included nine cases related to mobile work machines and nine cases related to a robot cell. In all cases two methods were applied to assess the risk level. The test persons (analysts) did not use a lot of time for each case and usually they did not have additional material like standards to support their decisions. Therefore, the decisions are mainly based on experience and by using each participant's background knowledge. The information given for each the mobile work machine case was short and focused on the parameters of the risk. For the robot case there was more material and all cases were related to the same robot cell. More information might give more accurate results, but on the other hand the parameter descriptions were given more precisely at the mobile work machine test

It is often claimed that the analysis tool should be calibrated to the relevant branch of technology in order to reach valid results [3]. This refers to the tacit information and culture related to each branch of technology. In our case the analysts were not able to do any comparison with the practise of the relevant branch of technology. This may result in a wider range of answers, but does not matter when we are comparing the standards. When comparing the results of the standard methods the analysts estimated the risk parameters, assuming that the risk is at the same level and yet, by choosing different parameters, the level of the assessed risk may be different.

The two experiments (machinery and robot cell) had quite different case descriptions as shown in the experiment descriptions above. If we use one of the standard readability formulas – in this case Kincaid [11] – we find that the readability index correlates strongly with the number of correctly identified risk levels when using the ISO 13849. The table below shows readability and number of correctly identified risk levels for the machinery.

Table 8. Number of matches between standard answer and analyst answer in mobile machine experiment.

Case	ISO 13849	Kincaid
1	0	12,4
2	12	73,8
3	1	35,6
4	4	51,5
5	2	48,9
6	10	63,9
7	2	50,3
8	5	46,6
9	7	61,9

The correlations are as follows:

Table 9. Correlation of readability and "correct" answers.

Experiment	Correlation	p
Machinery	0.90	0.00
Robot cell	0.69	0.04

It seems safe to assume that the readability of the case description strongly influences the analyst's ability to arrive at the correct risk level when using the ISO 13849 standard. No such relationship was identified for the IEC standard.

When we apply the IEC 62061 method, SIL 1 is a quite rare result compared to the ISO 13849 method. In addition, according to the standards (mobile work machine experiment), the risk should have been assessed to SIL 1 in five out of nine cases, but in none of the cases the SIL 1 got the majority of the results and only in one case was it the average. Figure 6 presents the distribution of all answers which shows the difference between the two methods. This indicates that the IEC 62061 standard tends to give SIL 0 and SIL 2 values more often than SIL 1 values.

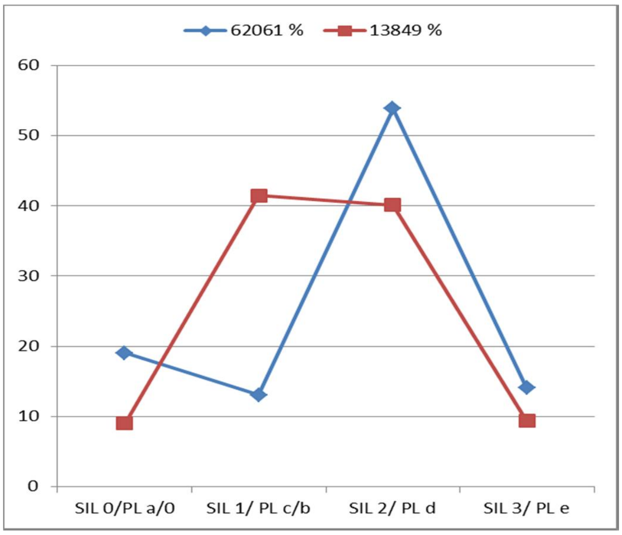


Figure 6. Distribution of answers (%) in mobile machine and robot cases. There were totally 299 answers in the experiments.

In the matrix of the IEC 62061 standard (see Table 2) SIL 1 is available only in three cells of the matrix and it is not available when severity is high (Severity=4). This leads to low number of SIL 1 results in the risk analysis. The ISO 13849 risk graph (see Figure 1) or the matrix (see Table 10) show that half the matrix cells leads to either PL b or PL c, which both are associated to SIL 1. One could claim that in machinery systems there should be more SIL 1 safety functions than SIL 2 safety functions, but the IEC 62061 method does not support this assumption.

Table 10. The ISO 13849 risk graph presented as a matrix form.

\Avoid	P1		P2	
Sev\Freq	F1	F2	F1	F2
S1	a	b	b	c
S2	c	d	d	e

The number of answers in the mobile machine experiment according to parameters (ISO 13849-1) is presented in Table 11. Severity 0 cases are not included in the table since in those cases the other parameters were not estimated. The table resembles Table 10, but the amounts of answers are included.

Table 11. The amounts of answers in the mobile machine experiment according to severity, frequency and avoidance factors (ISO 13849).

\Avoid	P1		P2	
Sev\Freq	F1	F2	F1	F2
S1	a= 18	b= 6	b=5	c=4
S2	c=59	d=24	d=35	e=15

The amount of answers according to severity and class (Cl) are described at Table 12 (IEC 62061 matrix). The table can be associated with Table 2 and the SIL values are in the corresponding cells. SIL 2 is in **bold**, SIL 1 is in *italic*s. In addition, the SIL requirements are also shown in the cells. Table 12 shows that a large amount of the answers (27) are just below SIL 1 at the "other measures" area (according to IEC 62061; see also Table 2). The class factor (Cl=Fr+Pr+Av) shows that most of the answers are in the middle (8-10). This may be related to the cases, but it is also possible that the analysts tend to avoid extreme values. This is a quite common response, known as the end-aversion bias or the central tendency [12].

Table 12 and Table 11 also show that a large amount of analysts estimated the severity to the highest level. This may be related to the cases or that the analysts tend to find the highest severity possible. When applying the IEC 62061 method this leads to at least SIL 2. In order to have more SIL 1 than SIL 2 values when the severity is 4, the Cl values 3 – 7 should result in SIL 1. If also the "OM" cells (Table 2) corresponds to SIL 1 the result would be closer to the ISO 13849 method result. One point is that in nearly all of the hazardous cases a good analyst can find a scenario in which a person is killed, but the probability can be very low. More precise estimation will be presented at the final report of the project.

Table 12. The amounts of answers in mobile machine experiment according to severity and class ranging (IEC 62061).

	Cl=Fr+Pr+Av				
Severity	3-4	5-7	8-10	11-13	14-15
4	SIL 2: 3	SIL 2: 31	SIL2: 50	SIL3: 23	SIL 3: 1
3	0	20	*SIL 1:* *18*	SIL 2: 3	SIL 3: 0
2	0	3	5	*SIL 1:* *0*	SIL 2: 0
1	0	4	2	2	*SIL 1:* *1*

In the results, the severity parameter is often given the highest value. The question is if the severity level really is high or if the analysts estimate the severity level to be too high. There were different risk levels in the cases, but the severity parameter of the standards were considered only in five mobile machine cases, i.e. the cases picked from the ISO 15998-2 standard [9]. This means that comparison of parameters against the standards is not done for the complete set of the cases.

In most of the cases the answers of the test persons are close to the standards and the average was a little higher than the standard's suggestion. This indicates that the analysis methods tend to result in higher risk levels than the standard suggests. However, it is possible that more available information for the analysts could result in values closer to the standards.

Since the two standards use different number of parameters and different texts for guiding the parameter value selection, we might expect large differences in the parameter value assessments. This is, however, not the case. As the diagrams below (see Figure 7, Figure 8 and Figure 9) show, the parameters in the two standards that are comparable follow the same paths. The diagrams are from the mobile work machine experiment.

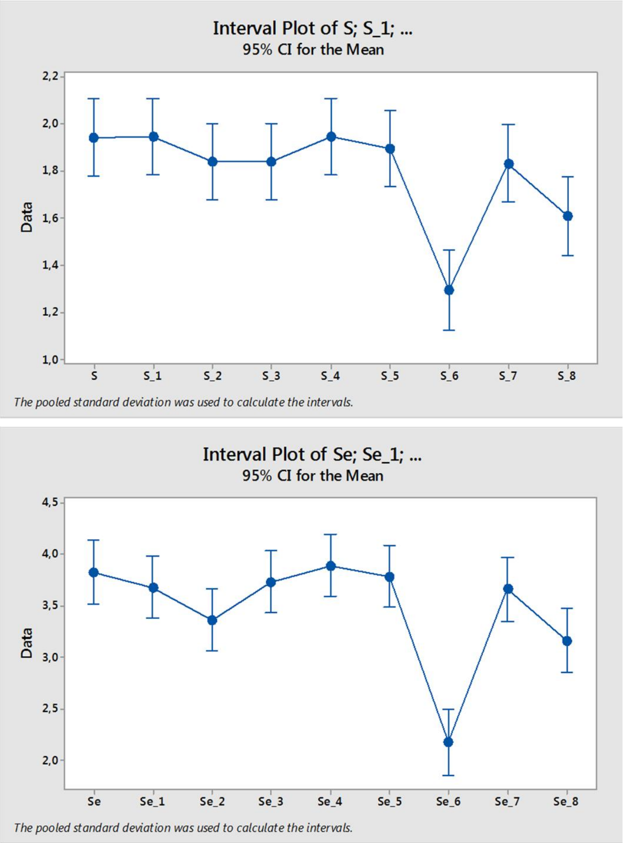


Figure 7. Paths for mean value of severity (S, Se). Above ISO 13849 method and below IEC 62061 method.

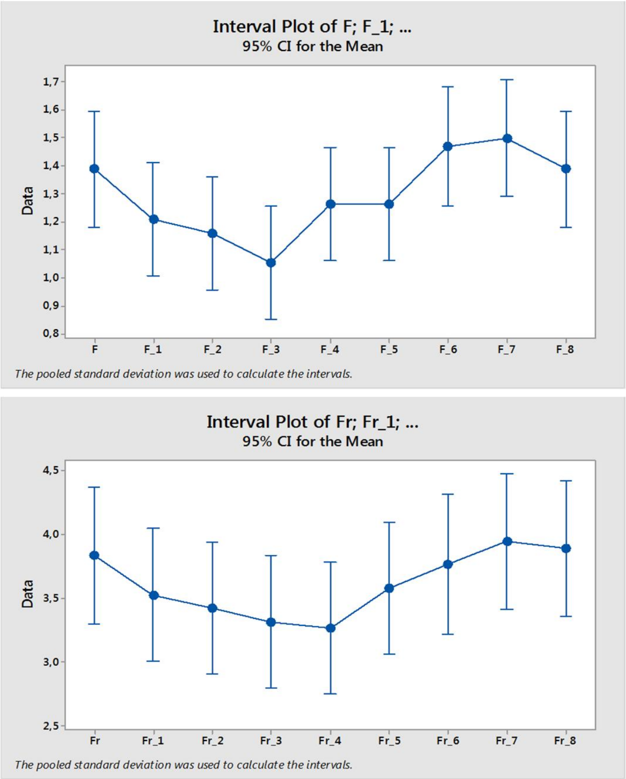


Figure 8. Paths for mean value of frequency (F, Fr). Above ISO 13849 method and below IEC 62061 method.

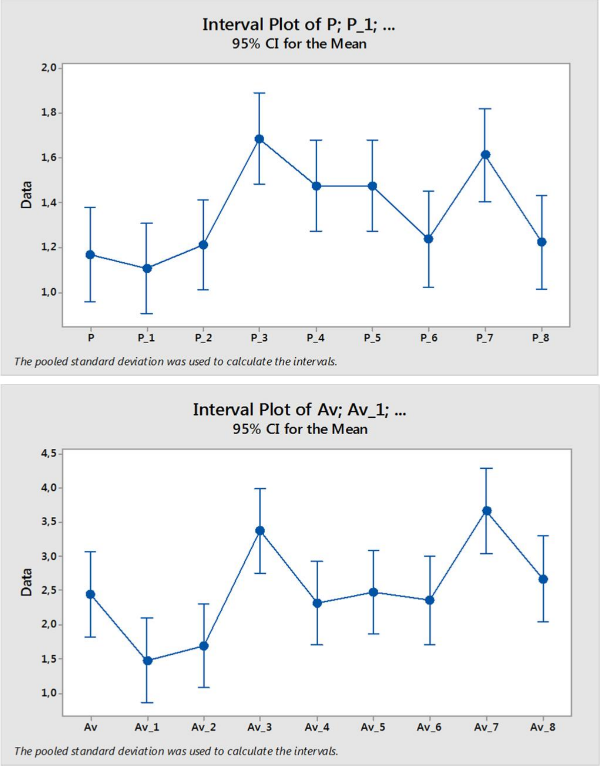


Figure 9. Paths for mean value of probability to avoid hazard (P, Av). Above ISO 13849 method and below IEC 62061 method.

If this is true, the mean values for each parameter should show a high degree of correlation. We computed the Spearman correlation for each comparable parameter pair and got the results shown in Table 13.

The two standards have the following risks assessments formulas:

- ISO 13849-1:
  R = S * P(harmful event) * P(not avoid)
- IEC 62061:
  R = S * P(harmful event) * P(harm | harmful event) * P(not avoid)

The parameter not found in ISO 13849 is the conditional probability P(harm | harmful event) since this standard assumes that a harmful event always will lead to harm. As mentioned earlier, the assessment of conditional probabilities is probably beyond the capability of most assessors.

Since hazard avoidance already is included in the P(not avoid) factor, the P(harm | harmful event) factor is related to near misses, i.e., P(near miss) = 1 – P(harm | harmful event). However, in many branches of industry the registration of near miss events is not complete and consistent and it is unreasonable to assume that assessors have access to this type of information.

Table 13: Standard parameter correlations

	Moving machinery	
Parameters	Spearman correlation	Level of significance
S – Se	0.83	0.005
F – Fr	0.82	0.007
P – Av	0.71	0.032
	Robot	
Parameters	Spearman correlation	Level of significance
S – Se	0.90	0.001
F – Fr	0.92	0.001
P – Av	0.43	0. 249

Conclusion

It can be seen that the distribution of parameters in both IEC 62061 method and ISO 13449 method give relatively similar results for each case. This is as expected since the analysts have been analysing the same cases. Yet there is a difference between final PL and SIL results. The IEC 62061 method does not give SIL 1 as often as the ISO 13849 method gives the corresponding result PL b or PL c. Instead, the IEC 62061 method results more often SIL 0 and SIL 2. The cases in the mobile machine experiment were chosen from standards and they indicate that there should have been more SIL 1 results than the IEC 62061 method results show. This means that when applying the IEC 62061 method, the analyst should consider all SIL 0 and SIL 2 results and decide if SIL 1 could be closer to the final result.

In mobile work machine experiment one case was chosen to have the lowest risk (SIL 0) and one the highest risk (SIL 3) according to corresponding standards. These extreme values were often not found by the analysts. If there is little information available the analysts tend to avoid extreme results. In these two cases more information from standards could have resulted more standard like answers.

When using ISO 13849 the readability of the case description is important, while when using IEC 62061, the assessor needs access to near miss information. The work of Hendrickx et al. [10] shows that assessors prefer case description over relative frequency information. If near miss information is not available, the assessors should use ISO 13849 and stay away from IEC 62061.

Acknowledgement

The project was made together with VTT (Finland), NTNU (Norway) and SP (Sweden). The major part of funding in Finland came from the Finnish Work Environment Fund. The rest of the funding for each partner was own funding of all participants. It is also remarkable how many companies from Finland, Norway and Sweden gave their support by answering the questions and making analysis for the test cases.

References

[1] Chambers C, Croll PR, Bowell M. A study of incidents involving programmable electronic safety-related systems. Interacting with computers, vol. 11. Elsevier Science B.V; no. 6, June 1999. p. 597–609.

[2] Hietikko M, Malm T, Alanen J. Risk estimation studies in the context of a machine control function. Reliability Engineering and System Safety. Vol. 96 (2011) No: 7, 767-774. doi-link: 10.1016/j.ress.2011.02.009

[3] IEC 61508-5. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 5: Examples of methods for determination of safety integrity levels. 97 p

[4] Jones C. Software quality in 2012: A survey of the state of the art. Namcook Analytics LLC. 2008 (achieved 9.6.2015). 25 p. http://sqgne.org/presentations/2012-13/Jones-Sep-2012.pdf

[5] SFS-EN ISO 13849-1. 2008. Safety of machinery — Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS 180 p.

[6] SFS-EN 62061. 2005. Safety of machinery — Functional safety of safety-related electrical, electric and programmable electronic control systems. 198 p.

[7] Kahneman, Daniel; Tversky, Amos: On the reality of cognitive illusions. Psychological Review, Vol 103(3), Jul 1996, 582-591

[8] EN 280. 2013. Mobile elevating work platforms. Design calculations. Stability criteria. Construction. Safety. Examinations and tests. 98 p.

[9] ISO/TS 15998-2. 2012. Earth-moving machinery -- Machine control systems (MCS) using electronic components -- Part 2: Use and application of ISO 15998. 58 p.

[10] Hendrickx, L., Vlek, C., and Oppewal, H.:”Relative importance of Scenario Information and frequency Information in the Judgement of Risk”. Acta Psychologica, 72 (1984), p 41 – 63

[11] Dragan, M. and Woo, A.: “The Methodology Used to Assess the Readability of the NNAAP Examination.” NNAAP and MACE Technical Brief, February 2010

[12] Choi, B.C.K. and Pak, A.N.P.: A catalog of Biases in Questionnaires, Public Health Research - Practice and Policy. Vol. 2, no. 1, January 2005.

Corresponding address

Timo Malm

VTT Technical Research Centre of Finland Ltd, Box 1300,
FI-33720 Tampere, Finland

Analysis of two risk estimation tools applied to safety of machinery

Yuvin Chinniah[a]

François Gauthier[b]

Damien Burlet-Vienney[c]

Barthélemy Aucourt[a]

[a]Polytechnique Montreal; [b]Universite du Quebec a Trois-Rivieres; [c]Institut de recherche Robert-Sauvé en santé et en sécurité du travail

Abstract

Risk estimation is a critical step in the priorization of risk reduction methods associated with machinery. Erroneous risk estimation may lead to insufficient risk reduction measures. Previous research has shown that there are many risk estimation tools which can be classified into families such as matrices and risk graphs. Different parameters are used in those tools, e.g. severity of harm (S), frequency/duration of exposure (Exf/Exd), probability of hazardous event (Pe), possibility of avoiding harm (A) and probability of harm (Ph). The different inputs of the risk estimation tools (e.g. the definitions for those parameters, the number of levels for those parameters) and the number of outputs of the tools (risk level or index) vary. Construction rules for risk estimation tools have been proposed in a previous study. In this article, a risk matrix from the American National Standards Institute ANSI B11.TR3 and a risk graph taken from International Standard Organization technical report ISO 14121.TR2 are tested by 25 subjects, experts in safety of machinery from Quebec, Canada. A questionnaire was developed. To avoid any bias, the actual tools were not presented to the experts. They chose the different levels for each parameter when applying the 2 risk estimation tools to 4 predefined hazardous situations involving machinery, and representing low, medium-low, medium-high and high risk. The subjects were also asked to propose a perceived risk level for each scenario. The results and the comments made by subjects were analysed. It was found that the risk level for each scenario depends on the tool being used and on the user. The risk graph underestimated risks and the risk matrix overestimated risks when compared to the perceived risk levels.

Keywords:

Risk estimation; matrix; graph; parameters; hazardous situations

Introduction

Risk related to machinery is defined in international standard ISO 12100 (2010) *Safety of machinery - General principles for design - Risk assessment and risk reduction* as a combination of the severity of harm and the probability of occurrence of that harm [1]. Engineers, occupational health and safety personnel, workers, supervisors and managers often carry out machinery risk assessment. The advantages of machinery risk assessment are numerous: hazards are identified effectively and better risk reduction measures can be implemented, injuries and deaths are prevented, fines and criminal prosecution are avoided, regulatory compliance is ensured and productivity is increased. Machines possess mechanical and electrical hazards, as well as those generated by heat, noise, vibration, radiation and dangerous chemical and biological substances.

ISO 12100 (2010) describes risk assessment as two stages namely risk analysis and risk evaluation. Risk analysis consists of (i) determining the limits of the machinery, (ii) hazard identification and (iii) estimating the risk. The risk estimation step, which is carried out for each identified hazard and hazardous situation, is important since its results will dictate risk evaluation and therefore the choice and prioritization of risk reduction methods. Experts interested in the risk estimation stage observed that: "*The methods used in the different European countries for assessing a machine's risks, when these methods exist, may lead to different, and even contradictory results. In some cases, they may potentially require, for a given machine, different levels of safety…*" [2]. Some variability in the results can be considered "natural", and therefore tolerable, but too great a dispersion can lead to under or over risk estimates and consequently to inappropriate risk reduction measures, inadequate prioritization of interventions and loss of credibility in the results [3]. Abrahamsson [4] also mentions that potential users perceive risk estimation tools as not being very credible or as unusable.

There is a lack of research dealing with the understanding of the risk estimation process in the field of machinery safety and with the identification of the variables that can influence the proper estimation of risk. A survey of risk assessment tools for industrial machinery was done and 108 tools were identified and classified [5]. Etherton et al. (2008) evaluated one particular risk estimation tool in reducing machinery risk [6]. In a previous study, tools were analysed theoretically using equivalent scales for their parameters, and construction rules for the design of risk estimation tools were proposed [7][8].

In this paper, two tools taken from this previous study are tested by 25 subjects on 4 scenarios and the results are presented.

Methods

Description of the selected hazardous scenarios

Four hazardous scenarios involving machinery representing mechanical hazards were presented to 25 subjects during the experimentation. Table 1 describes these 4 scenarios and shows the theoritical reference risk level obtained from the previous study [7]. This reference risk level is expressed in percentage of maximum risk, with 0% beeing no risk and 100% beeing maximum possible risk.

The scenarios were based on the components of the accidental process and risk according to ISO 12100 (2010) [1]. Each scenario included a picture of the work station and of the machine as well as a description of the activity, of the hazard, of the hazardous situation, of the hazardous event and of the possible harm. Information about exposure, probability of occurrence of the hazardous event and possibility of avoidance was also presented.

Table 1: Scenarios used to test the 2 tools

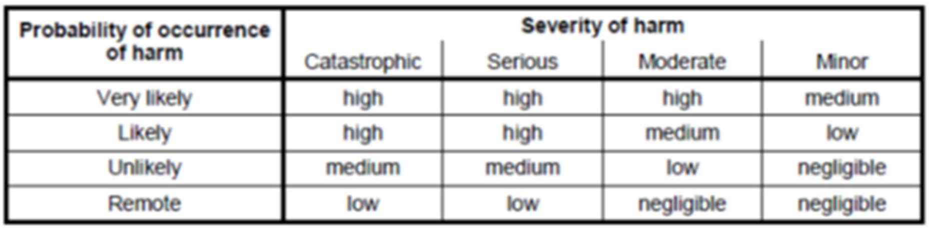
Scenario	Title	Summary	Reference risk level (from [7])
A	Punch press with travelling table	Demonstration of a punch press in automatic mode punching holes in a metal sheet on a travelling table during a trade show	Low (47.7%)
G	Self-guided vehicle	Self-guided vehicle moving in a workshop following a predetermined path	Medium-low (61.9%)
M	Paper machine	Reel in manual mode and workers removing torn/damaged parts of paper	Medium-high (74.8%)
S	Robot	Worker changing tool on a robot fed lathe for machining metal parts	High (85.0%)

Description of the selected risk estimation tools

Two well-known tools were tested, namely the risk matrix from ANSI B11.TR3 [9] (also found in ISO 14121.TR2) and a risk graph taken from ISO 14121.TR2 [10] as shown in Figures 1 and 2 respectively.

Table 2 shows the parameters used in those tools, their number of levels, and the results from the previous study [7]. The theoretical risk levels for each scenario obtained from the previous study is also expressed in percentage of maximum risk (100% beeing maximum possible risk).

The actual tools were not presented to the subjects. This was done to prevent subjects from biasing the results i.e. make the tool give the result they want by choosing the corresponding parameters. Instead, only the input parameters for each tool were presented to the subjects.



Probability of occurrence of harm	Severity of harm			
	Catastrophic	Serious	Moderate	Minor
Very likely	high	high	high	medium
Likely	high	high	medium	low
Unlikely	medium	medium	low	negligible
Remote	low	low	negligible	negligible

Figure 1: Risk matrix from ANSI B11.TR3 [9]

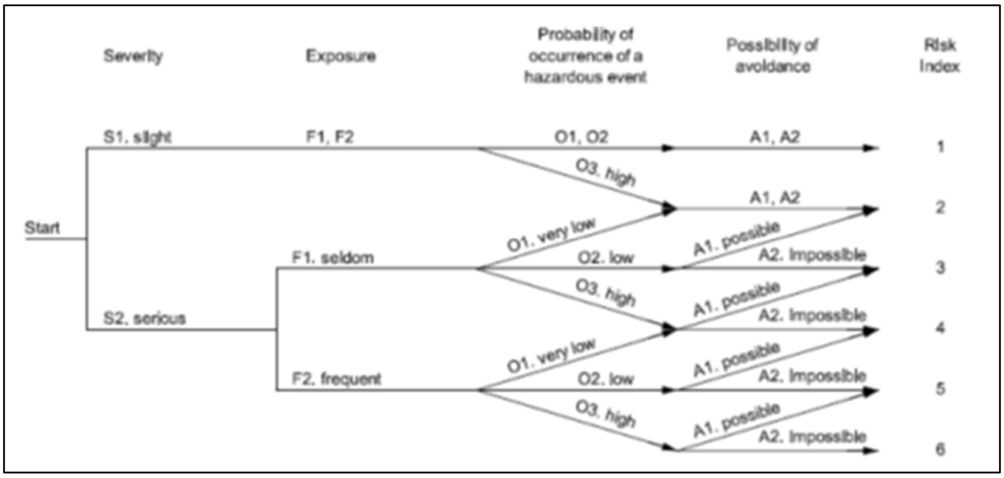


Figure 2: Risk graph from ISO 14121.TR2 [10]

Table 2: Parameters and risk levels obtained from the theoretical study for the two tools tested

Tools	Number of levels							Risk estimation tendency	Overall Average risk (%)	Risk levels obtained from theoretical study (%) when tools were applied to the 4 scenarios (A, G, M, S)			
	S	Ph	Exf	Exd	P	A	R			A	G	M	S
ANSI B11.TR3	4	4					4	High estimating tool	85.0	75.0	100.0	100.0	100.0
ISO 14121.TR2	2		2		3	2	6	Low estimating tool	50.8	33.3	66.7	33.3	33.3

Legend: S: severity of harm; Ph: probability of harm; Exf: Frequency of exposure; Exd: duration of exposure; P: Probability of occurrence of hazardous event; A: possibility of avoiding harm; R: risk level

Selection of subjects and experimentation

In order to ensure consistent and reliable data, the subjects participating in the study had to possess a good level of knowledge and experience on (i) the risk assessment process, and (ii) the use of the risk estimation tools. Thus, to be eligible, potential candidates should meet the following criteria: the subject is known to have some experience in safety of machinery, has participated to at least one machinery risk analysis over the past 5 years and had received formal training on the subject; or has participated to at least 5 machinery risk analysis if no specific training had been followed. This information on candidates have been verified during the recruitment process using a questionnaire dedicated to the identification of the subject.

A sample of 25 participants who were advisors in occupational health and safety organisations, maintenance or occupational health and safety personnel in manufacturing plants, and engineers specialized in safety of machinery, was obtained. The confidentiality of subjects has been guaranteed by the signing of a consent form approved by the ethics committee of Universite du Quebec a Trois-Rivieres.

In order to validate their perceptions of risk, subjects were asked to intuitively estimate the risk of each scenario using a visual analog scale. A visual analog scale is a 10 cm line on wich the subject is asked to put a mark reflecting its perception of the level of a variable. In this case, the risk line was defined with the endmarks “Minimum risk” and “Maximum risk”. The “perceived risks” obtained were consistent with the reference risk levels of the scenarios as determnied in the previous study (see Table 1).

For each scenario, the subjects were first asked to select the proper level for each parameter of the tools. The researcher then used the input parameters to estimate the risk and inform the subject of the results. The satisfaction of the subjects with the result of each tool to each scenario was recorded using an ordinal satisfaction scale (*Strongly disagree; Disagree, Neither agree or disagree; Agree; Strongly agree* …with the obtained risk level). Their comments and impressions regarding the application of each tool to each scenario were also noted down.

Criteria used to analyse the results

Three criteria were used to analyze the data for each tested tool:

- The ability to discriminate the different scenarios according to their specific risk level (**classification of scenarios**);
- The satisfaction of the subjects with the result of each tool to each scenario (**ordinal satisfaction scale** and **comments**);
- The convergence of results (inter-subject repeatability defined by the **modal percentage**, the proportion of the 25 subjects selecting the same risk level for a given scenario).

These criteria address three different facets of the results. Indeed, a tool with a good convergence but unable to discriminate the different scenarios according to their specific risk level will be useless. Similarly, a tool can have a good convergence and a good ability to discriminate the scenarios, but if the users often disagree with its results (their perceived risk beeing lower or higher), they will not use it.

Results and discussion

Risk matrix from ANSI B11.TR3

Classification of scenarios using the risk matrix ANSI B11.TR3

The results obtained when the 25 subjects applied the risk matrix to the 4 scenarios are given in Table 3. With regard to the ability of the tool to discriminate the risk levels of the 4 scenarios, the classification is undetermined for 5 subjects and 10 subjects have reversed the order of one or more of the scenarios as compared to the reference risk levels. 12 subjects classified the scenarios correctly (according to the reference risk levels order, i.e. AGMS) using this tool. This represents less than half of the subjects only.

41 of the 100 subject/scenario pairs (25 subjects with 4 scenarios) are strictly distinguished. In 59% of cases, the level of risk could not be distinguished between 2 (22 occurences) or 3 (5 occurrences) scenarios.

Table 3: Classification of scenarios for the risk matrix ANSI B11.TR3

Classification of scenarios	Number of occurrences
Right classification of scenarios (AGMS)	12
Cases where more than 2 scenarios were estimated at the same level of risk	5
Cases where subjects reversed the order of one or more of the scenarios	10

Convergence and subjects satisfaction for the risk matrix ANSI B11.TR3

Table 4 summarizes results obtained for convergence and subjects satisfaction for this risk matrix. The subjects diasgree with the results in 15 cases out of of the 100 subject/scenario pairs. Among the 13 negative comments collected (spread over the 4 scenarios), 9 reported a calculated risk level highier than the subject's perception. Four (4) subjects mentionned that the calculated risk level was lower than their perception for scenario A. The global convergence of the tool is just at the threshold (set at 60%, i.e. 15 of the 25 subjects chose selected the same risk level). In particular, only 48% of the subjects get the same level of risk for scenarios A and G.

Thus, for this risk matrix, it can be said that subjects:

- Were globally satisfied with the results;
- Experienced difficulties regarding classification of the scenarios (4 inversions of scenations A and G, and 4 inversions of scenations M and S);
- Had poor convergence for scenarios A and G.

A detailed analysis of the results suggests that the low modal percentages obtained with this risk matrix for scenarios A and G (48%), as well as the difficulty to classify them in the correct order may find its origin in the weak convergence of subjects for the probability of occurrence of harm parameter (Ph). Indeed, the modal percentage for this risk estimation parameter on these scenarios is 52%.

This discrepancy might be due to construction problems with the parameter, as suggested by Gauthier et al. [8]. Its levels are poorly defined (there is no definition associated with the figurative terms used) and there is a gap between the *Unlikely* and *Likely* levels. The impact of these flaws is translated into the risk levels obtained. The matrix, with two parameters and 16 possible combinations for 4 levels of risk, is sensitive to the choice of the level of a parameter. This demonstrates the negative impact that may have a parameter with flaws in a sensitive matrix.

Table 4: Satisfaction and convergence for the risk matrix ANSI B11.TR3

Scenario	Satisfaction				Convergence
	Number of subjects disagreeing (*Disagree or Strongly disagree*) with the level of risk obtained	Number of negative comments			Modal percentage
		Risk level higher than subject's perception	Risk level Lower than subject's perception	Total	
A	6	2	4	6	48%
G	2	2	0	2	48%
M	5	3	0	3	76%
S	2	2	0	2	68%
Total	15	9	4	13	60%

Risk graph from ISO 14121.TR2

Classification of scenarios using the risk graph ISO 14121.TR2

The results obtained when the 25 subjects applied this risk graph to the 4 scenarios are given in Table 5. Only 10 subjects found a classification comparable to the reference risk levels (i.e. AGMS). In 12 cases, the subjects reversed the order of one or more scenarios.

It is worth noting that with this tool, scenario A was always classified as a low risk or medium-low risk scenario, and that scenario S was always classified as an medium-high or a high risk scenario.

However, intermediate risk level scenarios (medium-low and medium-high) were more difficult to classified with this risk graph. Indeed, scenario G was found in the four possible positions and scenario M occured at three different positions (never at the lowest risk level).

Table 5: Classification of scenarios for the risk graph ISO 14121.TR2

Classification of scenarios	Number of occurrences
Right classification of scenarios (AGMS)	10
Cases where more than 2 scenarios were estimated at the same level of risk	3
Cases where subjects reversed the order of one or more of the scenarios	12

With regard to the ability of the tool to discriminate the risk levels of the 4 scenarios, 39 of the 100 subject/scenario pairs are distinguished. In 61% of cases, the level of risk could not be distinguished between 2 (26 times) or 3 (3 times) scenarios.

Convergence and subjects satisfaction for the risk graph ISO 14121.TR2

Table 6 summarizes results obtained for convergence and subjects satisfaction for this risk graph. This tool generated a lot of dissatisfaction, in the light of the number of subjects disagreeing with the resulting risk levels (40). It also generated a total of 37 negative comments. In particular, the tool had a problem with scenario M (medium-high risk level). All the negative comments related to this scenario go in the same direction: the calculated risk is too low compared to the subjects' perceived risk level.

However, this trend of low estimate appears to be independent of the scenario, since 33 of the 37 subjects' comments are stating that the risk level obtanined using this tool is lower than their perception. Convergence is good for scenarios A (low risk level) and scenario M (medium-high risk level). On the other hand, the convergence is below 60% for scenario G (medium-low risk level) and scenario S (high risk level).

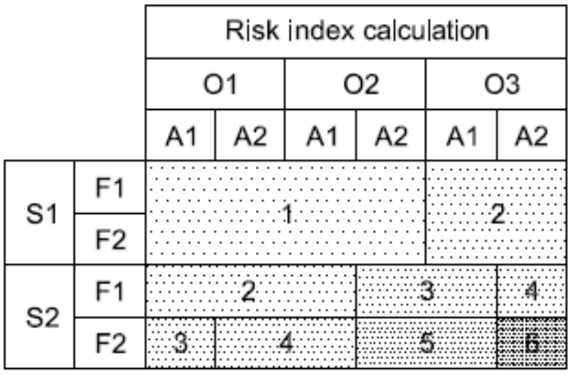
Thus, for this tool, it can be said that subjects:

- Were globally dissatisfied with the results (low estimating tool);
- Experienced difficulties regarding classification of the scenarios;
- Had poor convergence for scenarios G and S.

Table 6: Satisfaction and convergence for the risk graph ISO 14121.TR2

Scenario	Satisfaction				Convergence
	Number of subjects disagreeing (*Disagree or Strongly disagree*) with the level of risk obtained	Number of negative comments			Modal percentage
		Risk level higher than subject's perception	Risk level Lower than subject's perception	Total	
A	8	1	7	8	80%
G	12	3	3	6	44%
M	13	0	15	15	76%
S	7	0	8	8	52%
Total	40	4	33	37	63%

A detailed analysis of the results suggest that this problem is rooted in the architecture of the tool with a non-uniform distribution of the levels of risk, as illustrated in Figure 3, an equivalent risk matrix for this risk graph. The figure shows that 15 of the 24 possible settings combinations (62.5%) lead to a risk index of 1 or 2 (out of 6). In particular, when selecting a low severity (S1), regardless of other settings, the level of risk will be 1 (lowest risk), except when pobability of occurrence of hazardous event is set at O3 level.



		Risk index calculation					
		O1		O2		O3	
		A1	A2	A1	A2	A1	A2
S1	F1	1				2	
	F2						
S2	F1	2			3		4
	F2	3	4		5		6

Figure 3: Equivalent risk matrix for the risk graph from ISO 14121.TR2 [10]

This risk graph performed poorly regarding the classification of the scenarios (i.e. only 10 out of 25 subjects classified the scenarios correctly), notably regarding scenarios G and M. For scenarios G (44%) and S (52%), convergence was poor. Other possible reasons for this poor performance could be that (i) the severity of harm has only two levels, with poor definitions and (ii) since the frequency of exposure parameter (F in this tool) is poorly defined, half the subjects chose F1 and the other half F2 for scenarios A, G and S. Those defects are found in the first two parameters of the risk graph and their weights in calculating risk index are important. Moreover, an incremental change in S (e.g. <u>S1</u>, F2, O2 and A2 compared with <u>S2</u>, F2, O2 and A2) can change risk level from 1 to 5. Also, when referring to Figure 3, one sees that adjacent cells have more than a unit incremental change (risk indexes 2 and 4, risk indexes 3 and 5) implying that a unit change in F causes 2 units changes in risk level. The combined defects in the S and F parameters and in their influence on the estimated risk explain the results for scenario G.

Conclusion

In this article, a risk matrix from ANSI B11.TR3 and a risk graph taken from ISO14121.TR2 were tested by 25 experts in safety of machinery from Quebec. They chose the different levels for each parameter when applying the 2 risk estimation tools to 4 predefined hazardous situations involving machinery, and representing low, medium-low, medium-high and high risk. Comments made by experts subjects were also analysed. It was found that the risk level for each scenario depends on the tool being used and on the user. However, in general, the risk graph underestimates risk mostly because the risk levels are not uniformly distributed. The exposure/frequency parameters have poor convergence as the definitions are poor. The probability of harm (Ph) in the risk matrix has poor convergence. Such problems in the parameters and in the architectures lead to poor performance of the tools.

References

[1] ISO 12100 (2010) Safety of machinery - General principles for design - Risk assessment and risk reduction, International Standard Organization.

[2] Charpentier, P. (2003) Projet européen RAMSEM-Développement et validation d'une méthode d'appréciation du risque machine basée sur les principes de la normes EN 1050. Projet A.5/1,058 de l'INRS.

[3] Parry, G.W. (1999) Uncertainty in PRA and its implications for use in Risk-informed decision making, Proceedings of the 4th International conference on probabilistic safety assessment and management, PSAM 4, Edited by Mosleh, A. & Bari, R.A., New York.

[4] Abrahamsson, M. (2000) Treatment of uncertainty in risk based regulations and standards for risk analysis, Report 3116, Lund University, Sweden, 82 pages.

[5] Paques, J.-J. and Gauthier, F. (2007) Analysis and Classification of the Tools for Assessing the Risks Associated with Industrial Machines, Journal of Occupational Safety and Ergonomics, 13(2), pp. 173-187.

[6] Etherton, J., Main, B., Cloutier, D. and Christensen, W. (2008) Reducing Risk on Machinery: A Field Evaluation Pilot Study of Risk Assessment, Risk Analysis, 28(3), pp 711–721.

[7] Chinniah Y., Gauthier F., Lambert F., Moulet F. (2011) Experimental analysis of tools used for estimating risk associated with industrial machines, Studies and Research Projects/Report R-684, Montreal, IRSST, 77 pages.

[8] Gauthier F., Lambert S. and Chinniah Y. (2012) Experimental analysis of 31 risk estimation tools applied to safety of machinery, International Journal of Occupational Safety and Ergonomics, 18(2), pp. 245-265.

[9] ANSI B11.TR3 (2000). ANSI Technical Report - Risk assessment and risk reduction - A guide to estimate, evaluate and reduce risk associated with machine tools, American national Standard.

[10] ISO 14121-2 (2007) Risk Assessment - Part 2: Practical guidance and examples of methods, International Standard Organization.

Corresponding address

Yuvin Chinniah
Department of Mathematical and Industrial Engineering
Ecole Polytechnique de Montreal
2900, boul. Edouard-Montpetit
Campus de l'Universite de Montreal
2500, chemin de Polytechnique
Montreal (Québec)
CANADA
H3T 1J4
yuvin.chinniah@polymtl.ca

An extract of the future standard on Ergonomics methods Part 2-A methodology for work analysis to support design-

DR. HDR. Elie Fadier,
Technical Expertise and Consulting department
INRS- France
Elie.fadier@inrs.fr

The most important and interesting way to inform you of this standard is to give you an EXTRACT of the standard project that will be published by March 2016.

This extract will give you an idea on the essential elements to be learned from this European standard. This standard is currently under discussion to be proposed as such or adapted to ISO standard.

Contents

Page

SIAS 2015

8th INTERNATIONAL CONFERENCE
ON THE SAFETY OF INDUSTRIAL
AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

Session 4:
Safety-related control systems

Derek Jones, Rockwell Automation, Borgue/United Kingdom

Functional Decomposition from IEC 62061 – How to determine individual safety functions. From requirement to implementation

It is commonly acknowledged that one of the most frequent causes of failure associated with safety related control system functions is incorrect specification. Failure caused by technical faults is not entirely unknown but because of the quantified and structural requirements of functional safety standards it is a comparatively rare event. We should never become complacent by it seems that measures for random hardware failure and the most obvious aspects of control and avoidance of systematic failure are proving reasonably effective.

So what can be done about errors in specification? In truth this is part of the classic systematic failure. If the specification is incorrect or (more usually) incomplete then the design process is built on foundations of sand.

The classic outcome of an incorrect specification is not a direct dangerous failure. It is more subtle than that but just as worrying. It is a safety function that does not take account of all the requirements including productivity, maintenance and ergonomics as well as the obvious direct functional safety aspects. A typical result is that essential activities such as maintenance, setting or inspection cannot be performed efficiently. This creates an incentive to defeat the safety function.

So what tools do we have to prevent this and ensure that a safety requirements specification is complete and appropriate in every aspect?

The functional decomposition process from IEC 62061 provides a simple yet traceable and structured methodology that can be used as a common interface between the cross functional teams on the journey from the functional requirements specification through to the engineered system design.

The process defines the limits of the safety function thus solving some common problems encountered during the quantitative calculations. It can save money and time by ensuring agreement between all stakeholders at the functional concept stage before expensive engineering work commences. That minimises the likelihood of late or retrospective changes to the specification after engineering work has already commenced. It increases the probability that the implemented safety function will, in fact, be safe, suitable and efficient.

Research and considerations of electromagnetic noise immunity of programmable electronic system and common cause failure of safety-related programmable electronic system

Tsuyoshi TOEDA [a], Noboru SUGIMOTO [b]

[a] Auomation Componet Planning Depertment, Industrial & Instrumentation Equipment Division, Industrial Infrastructure Business Group, Fuji Electric Co., Ltd.

[b] Program in Safenology, Graduate Programs in Frontier Sciences and Innovation, Graduate School of Science and Technology, Meiji University

Abstract

Electrical/Electronic/Programmable Electronic System (abbreviated as "E/E/PES" hereafter) represented by Programmable Logic Controller (abbreviated as "PLC" hereafter) conducts most of industrial automatic controls. PLC conforms to international safety standards, which are certified by the third party, and has been used for more safety controls. However, there has been no example of quantitatively conducted research and report on failures of safety-related E/E/PES resulting from electromagnetic noise. We have researched and considered a correlation between electromagnetic noise immunity of safety-related E/E/PES and failures resulting from electromagnetic noise on the basis of our development, test, and quality assurance results for four generations. The results are reported below.

1) We revealed that most of the dangerous side failure factors of safety-related E/E/PES were Common Cause Failure (abbreviated as "CCF" hereafter) and most of CCF resulted from electromagnetic noise.

2) We analyzed the PLC return ratio in the field and then verified the correlation between electromagnetic noise immunity and PLC return ratio to derive a unique formula.

3) We devised a new formula indicating that safety of safety-related E/E/PES improves when electromagnetic noise immunity is enhanced. Furthermore, we verified the formula to reveal the correlation between electromagnetic noise immunity of safety-related E/E/PES and safety level of functional safety standards.

Keywords:

Functional safety; Safety of machinery; Common cause failure; Impulse noise immunity; Plogrammable logic controller;

Introduction

The above abstract summarizes 1) Methods, 2) Results, and 3) Discussion of the present study, which have been obtained on the basis of the development, test, and quality assurance results for four generations of PLCs manufactured by Fuji Electric Co., Ltd. (abbreviated as Fuji hereafter) shown below.

· Former generation: In 1982, Fuji released the first PLC with a mold case and microcomputer. Many failures occurred due to electromagnetic noise. Repair of the returned products required much labor.

· First generation: In 1985, Fuji released the first PLC with integrated circuits dedicated to instruction execution and communication control. Although measures against electromagnetic noise had been taken, the insufficient electromagnetic noise immunity of the initial product required internal modification many times.

· Second generation: In 1990, Fuji released the most high-speed PLC in the electrical machinery industry of the day with an internal clock that had been drastically speeded up. As a result of development aiming to enhance the electromagnetic noise immunity, the PLC return rate due to electromagnetic noise was reduced by half compared with the former generation. We intermittently continued taking measures against electromagnetic noise according to the result.

· Third generation: In 1998, Fuji released a PLC that was developed aiming at the largest noise immunity in the world after reviewing the basics of electromagnetism. Established electromagnetic noise measure techniques drastically reduced the PLC return rate due to electromagnetic noise.

Methods

Current problem with CCF

The possibility of hardware failure that shows the reliability of a safety-related E/E/PES is an important indicator to guarantee the productivity and safety of the production system. In particular, the probability of dangerous failure of redundant and multiple protective hardware derived from the Performance Level (abbreviated as PL hereafter) provided in Safety of machinery (ISO 13849-1, 2006) and Safety Integrity Level (abbreviated as SIL hereafter) provided in Functional Safety (IEC 61508, 2010) can be determined by, for example, the formula in IEC 61508:2010 for calculating Probability of dangerous Failure per Hour / Probability of Failure on Demand (abbreviated as PFH/PFD hereafter). However, with respect to CCF that occupies the largest part of PFH/PFD values, even safety-related engineers have only been discussing qualitative measures such as electrical and physical separation, and diversity of the principle and algorithm.

CCF and electromagnetic noise

The present study has clarified the fact that most of the dangerous failure possibility of safety-related

E/E/PESs is CCF that causes a simultaneous system failure to multiple channels such as a redundant system, and electromagnetic noise occupies a large part of the factors. Moreover, we have suggested the importance of the basic technique of electromagnetic noise measures and front loading (sufficiently enhancing the quality at the design stage), deriving a formula showing that high electromagnetic noise immunity is directly connected to reduction of the PLC return rate due to noise on the basis of the field data. With respect to PFH formula, we have devised a new formula reflecting the effects of electromagnetic noise immunity, verifying and considering electromagnetic noise immunity required for safety-related E/E/PESs based on the formula.

PFH$_D$

The failure probability per unit time of safety-related hardware λ [FIT (Failure In Time: failures×10^{-9}/h)] (MIL-HDBK-217F, 1991) is based on the failure probability of individual components in the same way as ordinary devices. IEC 61508-6:2010 shows the probability of dangerous failure per hour of redundant safety-related E/E/PESs such as a safety control PLC as follows.

IEC 61508-6:2010　B.3.3.2.2　1oo2

$$PFH_G=2((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU}t_{CE}+\beta\lambda_{DU}\quad [FIT] \quad (1)$$

IEC 61508-6:2010　B.3.3.2.5　2oo3

$$PFH_G=6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU}t_{CE}+\beta\lambda_{DU}\quad [FIT] \quad (2)$$

(Note 1) 1oo2: Duplex system (determined as unsafe when one failure occurs)

(Note 2) 2oo3: Triple system (determined as unsafe when two failures occur)

(Note 3) PFH$_G$: Average probability of dangerous failure

(Note 4) λ_{DD}: Probability of dangerous detected failure

(Note 5) λ_{DU}: Probability of dangerous undetected failure

(Note 6) β: Probability of common cause failure (selected from 2,10, or 20%)

(Note 7) β_D: Probability of detected common cause failure (selected from 1.5, or 10%)

(Note 8) t_{CE} : Mean time to repair [h]

Regardless of safe or dangerous, the above detected failure can stop the safety-related E/E/PES control safely when it occurs. In other words, treating the detected failures in the same way as safe failures in safety-related systems, we can define the probability of dangerous detected failure / hour (λ_{DD}) as zero paying attention only to the "probability of dangerous undetected failure (λ_{DU})". Formulas (1) and (2) can be simplified as follows.

$$PFH_D=2(1-\beta)^2\lambda_{DU}^2t_{CE}+\beta\lambda_{DU}\quad [FIT] \quad (3)$$

$$PFH_D=6(1-\beta)^2\lambda_{DU}^2t_{CE}+\beta\lambda_{DU}\quad [FIT] \quad (4)$$

(Note 9) PFH$_D$: Average probability of dangerous undetected failure

The following shows the result of substituting the hardware failure probability of two sets of Fuji's PLC systems (1oo2) having 256 I/O points shown in Table 1 into Formula (3) on the assumption that the time required for module replacement or mean time to repair (t_{CE}) is one hour. The reason why we have assumed t_{CE} to be one hour is because an average PLC user (machine user) has a PLC for replacement as a countermeasure against failures and replaces the PLC in approximately 30 minutes before a service person arrives.

$$PFH_D=2(1-0.02)^2(1{,}000\times10^{-9})^2\times1+0.02\times1{,}000\times10^{-9}$$

$$=0.0019208\times10^{-9}+20\times10^{-9}\quad [FIT] \quad (3.1)$$

(Note 10) β=2%：ISO 13849-1:2006 Annex F.1

(Note 11) $\lambda_{DU}=2{,}000\times(1-0.5)=1{,}000$　[FIT]

(Note 12) $\lambda_{DU}=\lambda\times(1-SFF)$：IEC 61508-4:2010 3.6.15

(Note 13) In the case SFF=50%：IEC 61508-2:2010 Table 3, Hardware fault tolerance=1, SIL1

(Note 14) $\lambda\fallingdotseq1{,}000\times10^{-9}\times2$ … Table 1

$=2{,}000\times10^{-9}$… 2 sets

(Note 15) SFF: Safe Failure Fraction

(Note 16) $SFF=(\lambda-\lambda_{DU})/\lambda$: IEC 61508-4:2010 3.6.15

(Note 17) $\lambda=\lambda_S+\lambda_{DD}+\lambda_{DU}$: IEC 61508-4:2010 3.6.15

As shown above, when the failure probability of an actual PLC is applied, the first term of the right-hand side of Formula (3) for safety-related E/E/PES is reduced to approximately 1/10,000 compared with the second term of the right-hand side, and that of Formula (4) to approximately 1/2,300. It is not λ_{DU} of individual redundant devices but λ_{DU} due to a common cause such as electromagnetic noise, design, and device configuration that dominates PFH$_D$ of safety-related E/E/PESs.

Main factor of Common Cause Failure (CCF)

As shown in attached Table A, in ISO 13849-1:2006, measures against CFF are scored according to the contents for the convenience of standards users. In particular, items concerning Electro Magnetic Compatibility (abbreviated as EMC hereafter) account for 40 points. Other items are related to quality standards required as a product and technical requirements that engineers must meet. It is possible to score 65 points or more that the standards require as long as measures against EMC are taken. However, to take EMC measures requires acquisition of basic electromagnetism theory and know-how acquired by experience. Even some PLCs for which third-party safety certification is obtained are on the market without sufficient EMC measures. The following describes, using an example, that EMC measures are basic technique of electric engineers, and the technique of EMC measures and the front loading (sufficiently enhancing the quality at the design stage) produce significant results.

Results

EMC measures in PLC

The real cause of external noise that leads PLC to malfunction is internal noise current and voltage. The internal noise current is generated by electromagnetic induction phenomenon resulting from, for example, electrostatic discharge, arc discharge due to interruption of electric circuits and unnecessary radio waves, and the internal noise voltage is generated as the result of it. Even if a PLC is insulated from the outside by a photocoupler, coils, and shield plates, noise current inevitably invades the internal circuits through stray capacitance and returns to the noise source. Moreover, noise current, which flows into the circuit network inside the printed circuit board through various routs, mostly flows into the power supply and the GND pattern with low impedance. In other words, less noise current is superimposed on the signal line patterns with high impedance compared with the power supply and the GND pattern. If the impedance of the power supply and GND pattern is lowered, the internal noise voltage is also lowered. Noise current slightly flowing into the signal lines can be bypassed with a capacitor, however, the fundamental problem lies in the design technique of the printed circuit board that requires bypass.

There is a domestic immunity test called square wave impulse noise test (JEMA [The Japan Electrical Manufacturers' Association] standards JEM-TR177, 2007), which is not specified in EMC international standards (IEC 61000-6-2, 2008). In the PLC industry, the rough standard of square noise immunity as a general specification should be as follows: 1,500 V of square wave noise voltage and 1 ns of square wave noise voltage rise time (Fuji Electric Co., Ltd. Catalogue 22B2-J-004, 2013).

Result of EMC measures in PLC

Table 2 shows square wave noise (Impulse noise) immunity in Fuji's PLCs of the last four generations that have been shipped by now and the return rate obtained by dividing the number of returned items supposedly due to malfunction resulting from electromagnetic noise divided by the number of items shipped. It is evident that the number of malfunction due to electromagnetic noise at customers' sites is reduced as the impulse noise immunity is improved. The following four PLC generations are shown in Table 2: the former generation released in 1982, the first generation in 1985, the second generation in 1990, and the third generation in 1998. We have conducted the impulse noise test using a uniform method including power supply – ground, power supply – input, and input–output.

Fig.1 is a correlation chart based on the data of Table 2. It can be confirmed that there is a high correlation coefficient of -0.8 between the pulse noise immunity and return rate due to malfunction by electromagnetic noise. The result of calculating the exponential approximation formula is unique Formula (5) that indicates the return rate due to electromagnetic noise on the market (Y) to pulse noise immunity (X). The reason why we regarded Y as the return rate is because the failures of the returned items occurred on the customers' sites and we considered them not as transient malfunction but as Fuji's PLC failures.

$$Y=468{,}675e^{-0.0051X} \quad [\text{ppm}] \quad (R2=0.9256) \qquad (5)$$

(Note 18) e: base of natural logarithms

(Note 19) ppm: parts per million

Method and criteria of impulse noise test

Table 3 shows the features of Fuji's PLCs of each generation. We have conducted the impulse noise test using a uniform method including power supply – ground, power supply – input, and input–output in the configuration shown in Fig. 2. The acceptability criteria of the impulse noise test is that there occurs no CPU runaway, power supply interruption, wrong input/output, communication error when noise is applied for more than 10 minutes. These test method and criteria are reflected in JEM-TR177 titled Guideline of impulse noise immunity test to electrical equipment in industrial environment, as a technical document of Japan Electrical Manufacturers' Association (General Incorporated Association). Fig. 3 illustrates the features and performance of the impulse noise generator specified in JEM-TR177.

Discussion

Device of new PFH_D formula for safety-related E/E/PES

It has already been described that Formulas (1) and (2), which are representative formulas in IEC 61508:2010 for calculating the probability of dangerous failure in safety-related E/E/PESs, can be simplified to Formulas (3) and (4).

$PFH_D=2(1-\beta)^2\lambda_{DU}{}^2t_{CE}+\beta\lambda_{DU}$ Formula (3) See above.

$PFH_D=6(1-\beta)^2\lambda_{DU}{}^2t_{CE}+\beta\lambda_{DU}$ Formula (4) See above.

Here, Formula (5), which has been obtained by the study of Fuji's returned PLCs supposedly due to malfunction by electromagnetic noise, suggests that it is necessary to newly add effects of failures due to electromagnetic noise to the entire failure rate of safety-related E/E/PESs λ. The reasons why are described below.

· The entire failure rate of safety-related E/E/PESs λ is the total value of the failure rates of individual electronic components comprising a safety-related E/E/PES λp.

· The failure factor caused by electromagnetic noise is not applied to derivation of individual component failure rate λp specified in MIL-HDBK-217F, a standard of electronic component failure rate calculation. A formula for calculating λp of IC (Integrated Circuit) is shown in Formula (6) as an example.

$$\lambda p=(C1 \cdot \pi T+C2 \cdot \pi E) \cdot \pi Q \cdot \pi L \quad [\text{FIT}] \qquad (6)$$

(Note 20) C1: Semiconductor die complexity failure rate (by market result)

(Note 21) πT: Temperature factor (by element material and junction temperature)

(Note 22) C2: Package failure rate (by market result)

(Note 23) πE: Environment factor (by use environment such as use on land, at sea, in the air or in space)

(Note 24) πQ: Quality factor (by procurement method and temperature screening)

(Note 25) πL: Learning factor (by number of production years)

In addition to the above fact about the entire failure rate of safety-related E/E/PESs λ, it is possible to demonstrate the following with respect to safety-related E/E/PES failure mode due to electromagnetic noise and handling of the failure rate.

・It is impossible to determine whether the failure mode is in the safe side or in the dangerous side since the result of safety-related a E/E/PES failure due to electromagnetic noise cannot be predicted.

・Electromagnetic noise is equally applied to the redundant system and diagnosis function to cause a failure, which is not guaranteed to be detected. Therefore, the probability of safety-related E/E/PES hardware failure due to electromagnetic noise needs to be added to probability of dangerous undetected failure λ_{DU}.

From the above consideration, we have devised brand-new Formulas (7) and (8) for calculating the probability of dangerous undetected failure of safety-related E/E/PES by adding a term of Formula (5) that derives “failure rate in proportion to electromagnetic noise immunity” to λ_{DU} in Formulas (3) and (4)

$$PFH_D=2(1-\beta)^2(\lambda_{DU}+\lambda\times Y)^2\ t_{CE}+\beta(\lambda_{DU}+\lambda\times Y)\quad [FIT]\qquad (7)$$

$$PFH_D=6(1-\beta)^2(\lambda_{DU}+\lambda\times Y)^2\ t_{CE}+\beta(\lambda_{DU}+\lambda\times Y)\quad [FIT]\qquad (8)$$

Here, $Y=468{,}675e^{-0.0051X}$ [ppm], X = Square noise immunity [V] Formula (5) See above.

(Note 26) λ×Y [FIT] is equivalent to safety-related E/E/PES failure rate due to electromagnetic noise that should be added to λ_{DU}.

Verification and discussion of formula obtained by adding effects of electromagnetic noise to PFH_D of safety-related E/E/PES

Table 4 lists PFH_D values and the corresponding SIL levels. The PFH_D values are obtained by combining λ_{DU} ≒1,000 [FIT], λ≒2,000 [FIT], and t_{CE}=1 [h] in a PLC system consisting of I/O 256 points with β factor value of 2% specified in ISO 13849-1:2006 Annex F F1 Note, and adding the electromagnetic noise immunity. The result of this verification reveals for the first time that PLCs having electromagnetic noise immunity of less than 1,500V are not suitable for being used as safety-related systems. Furthermore, it also indicates that the impulse noise immunity standard of 1,500V obtained by empirical knowledge in the domestic PLC industry is correct.

The Institution of Engineering and Technology, which is abbreviated as the IET, has published a variety of documents (IET fact file, 2008, IET guidance, 2013) concerning effects of electromagnetic noise on safety-related E/E/PESs and the measures. They suggest quantitative measures such as design technique, electrical and physical separation, and diversity of the principle and algorithm. Their approach differs from that of the present study based on field data. We have confirmed the corelation between the impulse noise immunity and failure rate due to electromagnetic noise and developed an idea of introducing the term of electromagnetic noise into the PFH_D formula, obtaining the result quantitatively showing that safety-related E/E/PES resistant to electromagnetic noise also has high safety.

Conclusion

Study of common cause failure and return rate due to electromagnetic noise

With regard to derivation of the probability of dangerous failure in redundant and multiple protective hardware provided in Functional Safety IEC 61508, 2010, we have confirmed that the proportion of individual failure to common cause failure is 1 to 10,000 in one redundant system using Fuji’s PLC as a model, suggesting that measures against common cause failure enhances safety. Moreover, it has been indicated that there is a high correlation between the impulse noise immunity and return rate based on the return rate of Fuji’s PLCs in the field due to malfunction by electromagnetic noise.

Introduction and discussion of term of electromagnetic noise immunity into PFH_D

We have derived an exponential approximation formula of impulse noise immunity and on-site failure probability from Fuji’s seven models. Moreover, we have devised a new formula for calculating the probability of dangerous failure by combining the obtained failure probability and λ_{DU}. Verification of the formula suggests that the impulse noise immunity of 1,500V obtained by empirical knowledge in the domestic PLC industry is quantitatively correct. Furthermore, it can be interpreted that PLCs having impulse noise immunity of less than 1,500V are not suitable for being used as safety-related systems.

Tables

Table 1: Calculation of the λ total for standard PLC per single 256 points I/O system

Classification	Module Type	Specification	λ* [case/h]	Units [pcs]	∑λ [case/h]
Power supply module	NP1S-22	100/200VAC input	108.6×10^{-9}	1	108.6×10^{-9}
Base board	NP1BS-08	8 slots	72.2×10^{-9}	1	72.2×10^{-9}
CPU module	NP1PM-48E	48Ksteps with Ethernet	357.9×10^{-9}	1	357.9×10^{-9}
Input module	NP1X3206-W	24VDC input 32 points	37.5×10^{-9}	4	149.9×10^{-9}
Output module	NP1Y32T09P1	Tr sink output 32 points	77.8×10^{-9}	4	311.0×10^{-9}
			λ Total at 40 deg. C		999.6×10^{-9}

*Source of the components λ in each modules: MIL-HDBK-217F

Table 2: Return rate due to noise immunity level

PLC Generation	Impulse noise immunity level [V]	Return rate due to noise immunity level [ppm]
Former	800	3,710
$1_{st.}$	1,100	3,270
	1,200	820
$2_{nd.}$	1,400	411
	1,500	268
	1,700	210
$3_{rd.}$	2,200	3

Table 3: Features of each PLC generation

PLC Generation	Product name	Release year	Execution time of basic instruction [µs]	Width [mm]	Height [mm]	Depth [mm]	Impulse noise immunity level [V]	Features (at the time)
Before $1_{st.}$	mini	1982	24.000	260	182	121	800	First compact size PLC which use a microcomputer.
$1_{st.}$	F	1985	1.000	482	255	100	1,100	Large size PLC which use Application specific integrated circuits (ASICs).
	F2	1989	0.800	482	255	100	1,200	Models change-over the F series.
$2_{nd.}$	FLEX	1990	0.160	435	135	120	1,400	New generation PLC which use high speed internal clock.
	F3	1993	0.125	482	255	100	1,500	Models change-over the F2 series.
	F3C	1995	0.125	413	130	122	1,700	Compact size PLC of F3 capability.
$3_{rd.}$	SX	1998	0.020	413	105	108	2,200	World fastest PLC which has best impulse noise immunity.

Table 4: Effects of the noise immunity level to PFH_D value and SIL level

Noise immunity [V]	PFH_D	SIL level	Noise immunity [V]	PFH_D	SIL level
100	6.918×10^{-1}	None	1600	5.518×10^{-6}	1
200	2.262×10^{-1}	None	1700	3.288×10^{-6}	1
300	8.319×10^{-2}	None	1800	1.971×10^{-6}	1
400	3.097×10^{-2}	None	1900	1.187×10^{-6}	1
500	1.175×10^{-2}	None	2000	7.193×10^{-7}	2
600	4.589×10^{-3}	None	2100	4.394×10^{-7}	2
700	1.866×10^{-3}	None	2200	2.716×10^{-7}	2
800	7.995×10^{-4}	None	2300	1.710×10^{-7}	2
900	3.644×10^{-4}	None	2400	1.107×10^{-7}	2
1000	1.771×10^{-4}	None	2500	7.444×10^{-8}	3
1100	9.129×10^{-5}	None	2600	5.269×10^{-8}	3
1200	4.940×10^{-5}	None	2700	3.963×10^{-8}	3
1300	2.772×10^{-5}	None	2800	3.179×10^{-8}	3
1400	1.595×10^{-5}	None	2900	2.708×10^{-8}	3
1500	9.329×10^{-6}	1	3000	2.425×10^{-8}	3

Figures

Figure 1: Correlation chart of return rate due to noise immunity level

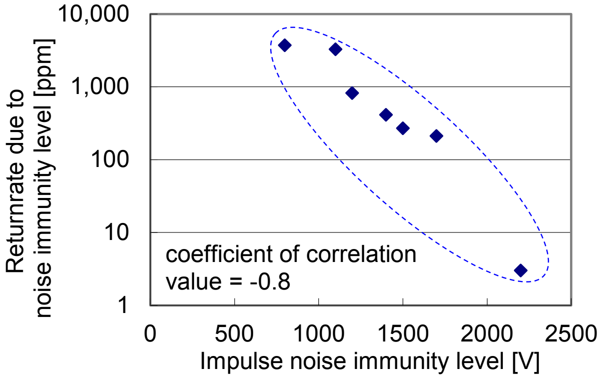


Figure 2: An example of impulse noise test

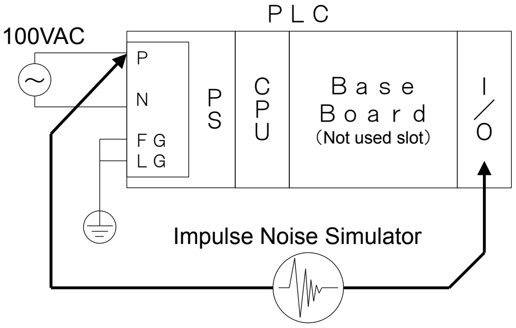
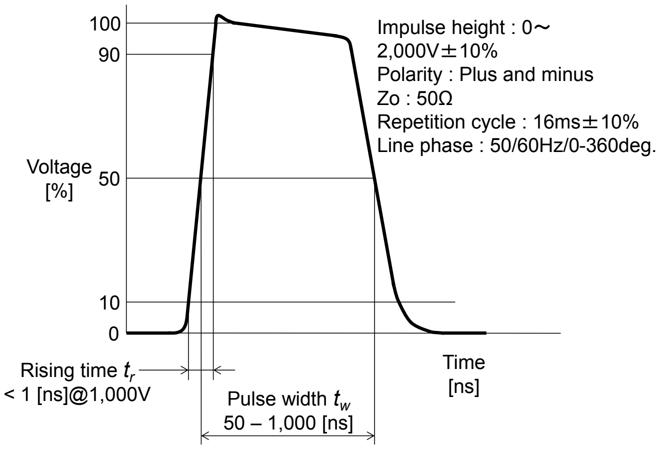


Figure 3: Specification of impulse noise output for impulse noise simulator



References

[1] International Organization for Standardization. Safety of machinery - Safety-related parts of control systems-. ISO 13849-1:2006

[2] International Electric Commission. Functional safety of - Safety related electric/electronics/programmable electronic safety-related systems –. IEC 61508:2010

[3] Department of defense USA. Military Handbook Reliability predication of electronic equipment . MIL-HDBK-217F:1991

[4] International Electric Commission. Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments. IEC 61000-6-2:2005

[5] The Japan Electrical Manufactures' Association (in Japanese). Guideline of impulse noise immunity test to electrical equipment in industrial environment. JEM-TR177:2007

[6] Fuji Electric Co., Ltd. (in Japanese). Catalog of the MICREX-SX series. 22B2-J-0004:2014

[7] The Institution of Engineering and Technology. Electromagnetic Compatibility for Functional Safety:2008.

[8] The Institution of Engineering and Technology. Overview of techniques and measures related to EMC for Functional Safety:2013.

Corresponding address

Tsuyoshi TOEDA
1, Fuji-machi, Hino-city, Tokyo 191-8502 JAPAN
toeda-tsuyoshi@fujielectric.com;
toeda0522@yahoo.co.jp

Appendix table A EMC related requirements of ISO 13849-1:2006 Table F.1

No.	Measure against CCF	Score (✓: related to EMC)
1	Separation/ Segregation	
	Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creep age distances on printed-circuit boards.	15✓
2	Diversity	
	Different technologies/design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, Measuring of distance and pressure, digital and analog. Components of different manufactures.	20
3	Design/application/experience	
3.1	Protection against over-voltage, over-pressure, over-current, etc.	15
3.2	Components used are well-tried.	5
4	Assessment/analysis	
	Are the results of a failure mode and effect analysis taken into account to avoid common-cause failures in design?	5
5	Competence/training	
	Have designers/ maintainers been trained to understand the causes and consequences of common cause failures?	5
6	Environmental	
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.	25✓
6.2	Other influences Have the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards) bee considered?	10
	Total	[max. achievable 100]

Total score	Measures for avoiding CCF[a]
65 or better	Meets the requirements
Less than 65	Process failed ⇒ choose additional measures

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

Improvement of ISO 13849-1 as a result of practical feedback: amendment 1 (2016)

Michael Hauke[a], Ralf Apfeld[a], Thomas Bömer[a], Michael Huelke[a], Klaus Becker[b]

[a] Institute for Occupational Safety and Health, (IFA), Sankt Augustin
[b] German Social Accident Insurance Institution for the energy, textile, electrical and media products sectors, (BGETEM), Wiesbaden

Abstract

The ISO standard 13849-1 "Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design" has been published in a completely revised version in 2006. The concept of control system categories (tested/untested single channel, redundant channel) had been expanded by the quantification of the probability of a dangerous failure of the safety function and safety related software – leading to the performance level (PL).

Several years of practical use of this revised standard demonstrated wide acceptance of the new concept. However with growing experience in the application several improvements appeared to be necessary. The Amendment 1 of ISO 13849-1 has now passed the FDIS stage and offers new solutions for: integration of components without safety rating by the manufacturer (e.g. standard PLCs); consideration of the "probability of occurrence of a hazardous event"; higher typical $MTTF_D$ estimates for hydraulic components with a small number of annual operations; evaluation of the quantifiable aspects of the PL without using $MTTF_D$ values but based on the use of well-tried components; and many more. The presentation will illustrate these new solutions and review the achievements of the Amendment in the light of the new standardization project ISO/IEC 17305 to merge ISO 13849-1 with the parallel IEC standard 62061.

Keywords:

Amendment, ISO 13849, IEC 62061, ISO/IEC 17305, Functional safety, Machinery, Design, Control system, Safety related, SRP/CS

Introduction

Almost ten years after it was first published in revised form as EN ISO 13849-1, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, the first amendment of this standard has now appeared. Since the amendment was intended primarily to improve clarity and ease of application, it contains only a few significant changes. A number of detail improvements and additions have however been made that are apparent in the standard's practical application. This paper describes the essential changes. Where the text of the amendment needs interpretation, it provides recommendations.

General changes

Table 1, "Recommended application of IEC 62061 and ISO 13849-1", has been replaced by a reference to the technical report ISO/TR 23849 [1], which has since appeared. The latter addresses in detail the differences between the two standards and their common aspects.

The foreword now clarifies that the standard applies to safety-related parts of control systems (SRP/CS) with high demand or continuous mode of operation (frequency of demands on a SRP/CS is greater than one per year).

The abbreviation "PFH_D" has been introduced for the "average probability of dangerous failure per hour". The dimension of this variable is 1/time and its typical unit is 1/h.

The notation for the "mean time to dangerous failure" now has a capital D, i.e. "$MTTF_D$" (formerly "$MTTF_d$"). The same applies for B_{10D}, T_{10D} etc.

Design considerations

Besides updating of the references to ISO 12100:2010 [2] (instead of to the preceding standard, ISO 12100-1:2003), the amendment explains that the sub-systems of an SRP/CS can also be designed against other standards governing functional safety (e.g. IEC 62061, IEC 61508, IEC 61496). They can then – where applicable following "translation" of an SIL to a PL in accordance with Table 4 of the standard – be integrated as sub-systems. In this case, the rules for "combination of SRP/CS" (Section 6.3 of the standard) are to be applied. This is also explained in ISO/TR 23849.

The limitation of the $MTTF_D$ for each channel to 100 years has been increased to 2,500 years for Category 4 sub-systems. The corresponding pairs of $MTTF_D$ and PFH_D values have been added to Annex K of the standard (see [3] and [4]). The limitation to 100 years was originally introduced in order to enable high Performance Levels to be attained on a basis other than a high statistical reliability of the individual components. However, since redundancy and fault detection are already at a very high level in Category 4, the $MTTF_D$ constraint can be loosened in this case. The superior PFH values that can be attained as a result then also enable a greater number of PL e sub-systems to be combined without the entire SRP/CS "slipping down" to PL d. Further information can be found in [4].

Two changes have been made concerning the assumptions for the designated architectures, which form the basis for the simplified method for estimation of a PL:

- For Category 2, so far the demand rate had to be ≤ 1/100 of the test rate.
  Now the testing may occur immediately upon demand of the safety function, if the overall time to detect the fault and to bring the machine to a non-hazardous condition (usually the machine is stopped) is shorter than the time to reach the hazard. Here ISO 13855 [5] for the calculation of safety distances is referenced.
  Chapter 4 of [6] gives further explanation.
- For Category 2, so far the $MTTF_{D, TE}$ of the test equipment was compared to the $MTTF_{D, L}$ of the logic.
  Now the $MTTF_D$ of the test channel has to be greater than half the $MTTF_D$ of the functional channel.
  Previously this new rule was only given in a note under the condition that the blocks of each channel cannot be separated.

Annex K contains a new note on the aspect of the test rate in relation to the demand rate, the reasoning for which is also found in [6]:

"If for category 2 the demand rate is less than or equal to 1/25 of the testrate (see 4.5.4), then the PFH_D values stated in the table K.1 for category 2 multiplied by a factor of 1.1 can be used as a worst case estimate."

A further comment explains that the PFH_D values in Annex K were calculated with the discrete values for DC_{avg}, 60%, 90% and 99%.

New PL estimation procedure without $MTTF_D$ for the non-electrical output part of the SRP/CS

In response to calls voiced by industry, an additional and further simplified method for determining the PFH_D and the quantifiable aspects of the PL of a subsystem has been added in the form of a new Section 4.5.5. The method is based primarily upon the implemented Category inclusive of DC_{avg} and CCF. This method does not require calculation of the $MTTF_D$; however, well tried or proven-in-use components must be used throughout in the functional channels – in Category 1 as well as in Categories 2, 3 and 4.

This method is applicable only:

- for the output part (subsystem) of the SRP/CS (power transmission elements) and
- when for mechanical, hydraulic or pneumatic components (or components employing mixed technology) no application-specific reliability data ($MTTF_D$, failure rate, B_{10D} or similar) are available.

Table 1 shows the estimated PFH_D value and the resulting attainable PL according to the implemented Category and under the additional conditions placed upon the method.

Proven-in-use demonstration is based upon an analysis of experience in the field for a specific configuration of a component. The analysis must show that the probability of dangerous systematic faults is sufficiently low for each safety function using the component to reach its required Performance Level (PL_r). Such a demonstration has not been common in machine construction before now.

The method is subject to the following additional conditions:

- In Category 1: use of well-tried components and well-tried safety principles (as previously, and established in the Category 1 definition).
- In Category 2: the $MTTF_D$ of the test channel is at least 10 years.
- In Categories 2, 3 and 4: use of well-tried or proven-in-use components and well-tried safety principles. In Category 2 according to the standard this applies also for the test channel.
- In Categories 2 and 3: adequate measures against CCF, and for each component DC at least "low".
- In Category 4: adequate measures against CCF, and for each component DC "high".

The following additional information is provided:

- Category 1: the T_{10D} values for the safety-related components that are not monitored during the process can be determined from data from the machine manufacturer that are proven in use.
- Categories 2, 3 and 4: since recourse cannot be made to formula E.1 of the standard for calculation of the DC_{avg} owing to the unavailability of $MTTF_D$ values, the DC_{avg} is formed in this case simply as the arithmetic mean of the single DC values of all components in the functional channels.

Table 1: PL and PFH_D as worst case estimation based on Category, DC_{avg}, and use of well-tried-components (on the basis of the table in Section 4.5.5 of the standard).

	PFH_D (1/h)		**Cat. B**	**Cat. 1**	**Cat. 2**	**Cat. 3**	**Cat. 4**
PL b	**$5.0*10^{-6}$**	⇦	●	o	o	o	o
PL c	**$1.7*10^{-6}$**	⇦	-	●	●	o	o
PL d	**$2.9*10^{-7}$**	⇦	-	-	-	●	o
PL e	**$4.7*10^{-8}$**	⇦	-	-	-	-	●
o	Applied Category is recommended						
●	Applied Category is optional						
-	Category is not allowed						

Handling of requirements concerning safety-related embedded software (SRESW) where standard components are used

The use of bought-in industrial standard components not developed specifically for use in safety functions and containing embedded software was not previously addressed in its own right in the standard. Numerous examples of SRP/CS exist in practice however that make use of standard components such as PLCs, frequency converters or intelligent sensors and that achieve safety for example by diverse redundancy with fault detection at system level. An example employing a standard PLC and a standard frequency converter is shown in Annex I of the standard. Since observance of the SRESW requirements is not generally confirmed by the manufacturer for such standard components and cannot be performed subsequently by the integrator, satisfaction of the SRESW requirements could often strictly speaking not be demonstrated in the past.

Amendment 1 now dispenses with the need for satisfaction of the SRESW requirements be demonstrated, provided the following conditions are met:

- The SRP/CS is limited to PL a or PL b and uses Categories B, 2 or 3.
- The SRP/CS is limited to PL c or PL d and may use multiple components for two channels in Categories 2 or 3. The components of these two channels use diverse technologies.

Besides the SRESW requirements, the standard sets out further more hardware related requirements, concerning for example the avoidance and control of systematic faults and suitability for the anticipated environmental conditions such as climate, vibration and EMC. These additional requirements continue to apply irrespective of SRESW. They also include the requirement for basic safety principles to be applied from Category B upwards and well-tried safety principles from Category 1 upwards. In addition, for all Categories, the basic requirement of Category B must be met that the SRP/CS must be designed, constructed, selected, assembled and combined at least in compliance with the relevant standards, for example with EN 61131-2 for PLCs or EN 61800-1/-2 for frequency converters.

Development with quality assurance in accordance with ISO 900x is not made an explicit requirement by the standard; however, it constitutes an intelligent requirement that is reflected in the seven basic measures for PL a and b in Section 4.6.2 of the standard that apply to SRESW developed in-house.

The purpose of the requirement for diverse technologies in the two channels is that the probability of a dangerous failure of the SRP/CS is strongly reduced by a fault in the SRESW.

In the following examples “diverse technology” may usually considered to be fulfilled:

- One channel (functional channel or test channel) contains components with embedded software. The second channel contains exclusively components without software, thus mechanical, electronic, electromechanical, pneumatic or hydraulic components.
- Both channels use diverse embedded software, e.g. different operating systems, on the same or different hardware.
- Both channels use different hardware (e.g. microprocessors with different processor cores), since it can be assumed, that the development of the corresponding embedded software took place on different programming environments.

In the following examples “diverse technology” may usually considered not to be fulfilled:

- Both channels use similar components of different manufacturers without further information about the diversity of the embedded software. Here it can normally not be excluded that both manufacturers use the same parts of embedded software, possibly even on the same hardware (brandlabeling).
- Both channels use similar components of one manufacturer but of different type without further information about the embedded software.

Safety functions

A provision has been added at this point stating that depending upon the application, it may be advantageous to define a separate safety function without power available. An example are vertical axes which must be prevented from lowering under gravity even in the event of loss of power. Where power is available, the axis is held for example by an electric drive, whereas in the event of power loss a mechanical brake is applied.

Categories

It was previously permissible in Category 2 "only" to provide a warning of the hazard when the initiation of a safe state following detection of a fault is not possible.

It is now specified explicitly – depending on the PL_r – in which case a warning alone is permissible:

- For PL_r a up to and including PL_r c, whenever practicable the ouptut (OTE) shall initiate a safe state that is maintained until the fault is cleared. When this is not practicable (e.g. welding of the contact in the final switching device), it may be sufficient for the output of the test equipment (OTE) to provide a warning.
- For PL_r = d, the output (OTE) shall initiate a safe state that is maintained until the fault is cleared.

Combination of SRP/CS

Manufacturers of almost all bought-in SRP/CS now also state the PFH_D value in addition to the PL (or SIL). On SRP/CS developed in-house, these values are in any case available.

The following procedure can therefore be followed for combination (in series) of SRP/CS that together execute a safety function:

- Limitation by non-quantifiable aspects: the total PL is at most as great as the lowest PL of all combined SRP/CS.
- Limitation by quantifiable aspects: the total PL is also at most as great as the PL corresponding to the summated PFH_D in accordance with Table 3 of the standard. The summated PFH_D is formed as the sum of all PFH_D values of all combined SRP/CS.

The combination method according to Table 11 of the standard is now intended only as an exception for cases in which only PL values and no PFH_D values are available for the combined SRP/CS.

Determining of the PL_r

Several changes have been made to Annex A. Firstly, substantially more emphasis is now placed upon the informative character of the method described here for determining the PL_r. This method is not binding and constitutes only an estimate of the risk reduction. Owing to the normative compromise reached in the group of experts in consideration of reasons that may also lie outside the parameters of the risk graph, it is acceptable for Type C standards to contain provisions concerning the PL_r that deviate from the PL_r that would be produced from the risk graph.

The comment for distinguishing between F1 and F2 is now formulated as follows:

- In case of no other justification, F2 should be chosen if the frequency is higher than once per 15 minutes.
- F1 may be chosen if the accumulated exposure time does not exceed 1/20 of the overall operating time and the frequency is not highter than once per 15 minutes.

The probability of occurence of a hazardous event has now been added in addition to severity of injury (S), frequency and/or exposure time to hazard (F) and possibility of avoiding the hazard or limiting the harm (P). If this quantity can be justified as low, the PL_r may be reduced by one level (but not below PL_r a, see Figure 1 below).

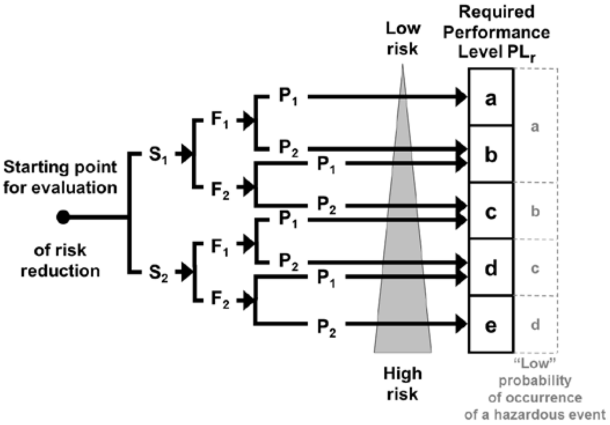

Required Performance Level PL_r
Low risk
High risk
Starting point for evaluation
of risk reduction
S_1
S_2
F_1
F_2
P_1
P_2
a
b
c
d
e
"Low" probability of occurrence of a hazardous event

Figure 1: Interpretation of the risk graph according to the Amendment 1 of EN ISO 13849-1

This quantity is known from ISO 12100 and ISO/TR 14121-2 as well as in EN 62061. It is dependent upon human behaviour or technical failure and is generally very difficult to assess. Reliability data and history of accidents on comparable machines (with the same risk, same process, same oerator action and same technology causing the hazard) may justify the assessment. Where the history of accidents is concerned, it must be considered that it is generally based upon technical protective measures that have already been installed, and not upon the situation prior to specification of the intended safety function (starting point of the risk graph). A low number of accidents could therefore confirm the existing PL_r assessment upon which the history of accidents is based. It does however not justify assessing the PL_r to be specified as being lower than is currently the case.

In a new Section A.3, the standard now addresses the subject of overlapping hazards and clarifies that each hazard can be assessed separately during the risk assessment. The safety functions for separate hazards may be separated, as a result of which only the power control elements for one hazard arise as the output of the associated SRP/CS (and are input into the PFH_D). In a manufacturing cell involving multiple robots, the safety-related stop functions, for example in response to opening of a safety door, can therefore be defined individually as separate safety functions for each robot. The same consideration applies for example when a rotary table features multiple clamping devices. However, when multiple hazards in a part of a machine are directly connected to each other, it is advisable for them to be considered together in a combined safety function. An example is a welding robot in continual use on which an operator is exposed at one and the same time to the hazards of crushing by movement and burning by the welding process, both hazards being presented by the tool centre point. More detailed explanations on the analysis of overlapping hazards can be found in [7].

Good Engineering Practice Method and $MTTF_D$

Changes shown by industrial practice to be necessary have been made at several points in Table C.1, "Good engineering practices method":

- For hydraulic components (essentially, valves), higher typical $MTTF_D$ values can now be applied as a function of the mean number of annual operations n_{op}. The previous $MTTF_D$ value of 150 years can be doubled to 300 years when n_{op} < 1,000,000 cycles per year. Even less frequent actuation (fewer than 500,000 or 250,000 cycles per year) leads to further doubling (to 600 and 1,200 years respectively). The estimation has thus been brought more closely into line with that for pneumatic components.
- The typical B_{10D} value for contactors under nominal load has been reduced from 2,000,000 to 1,300,000 cycles per year. The reason is that a value deviating from 50% (the usual estimated value in the standard) was explicitly stated in the product standard for contactors as the proportion of dangerous failures.
- The two lines for emergency-stop devices have been merged. Emergency-stop devices and enabling devices can be assessed as Category 1 or Category 3/4 sub-systems, depending upon the number of electrical output contacts and fault detection in the downstream SRP/CS. Each contact element (including the mechanical actuation) can be regarded as a channel with a relevant B_{10D} value of 100,000 cycles. For enabling switches, this encompasses both break functions, i.e. fully depressing and releasing. ISO 13849-2, Table D.8, according to which fault exclusion is permitted under certain conditions, can also be applied independently of the above.

The "$MTTF_D$ for components, worst case" column has been deleted from Tables C.2 to C.7 for semiconductors and passive components. The figures stated there with a safety factor of 10 compared to the typical case were no longer of practical relevance, since more suitable failure data are available in any case directly from the manufacturer for the majority of components of this type, and the "typical" case is otherwise adequate for the purpose of estimation.

Typical values are now also applied for the electrical components in place of the worst case for the "parts count method" in Table D.1.

Diagnostic Coverage

Two measures have been deleted from Table E.1 owing to their lack of practical relevance:

- Redundant shut-off path with no monitoring of the actuator (DC = 0%).

- Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment (the DC is to be estimated individually for each shut-off path; analysis in combination is not appropriate).

The DC measure of "fault detection by the process" is now described in more detail:

- For estimation of the DC in the range stated from 0 to 99%, all relevant dangerous failures can first be identified, and of these the failures can subsequently be determined that are detected in the process. From the detected proportion, one of the values can then be estimated from none (0%), low (60%), medium (90%) or high (99%).
  This provision applies by analogy to other measures for which a DC range is stated, for example "indirect monitoring".
- This measure may of course be used for a component only when dangerous failures of the component concerned are actually apparent in the (production) process. When components in the safety path are only actuated on demand of the safety function, fault detection by the process cannot be assumed for these components.

CCF

Clarity has been improved or information added at certain points in Table F.1.

Illustrating Examples

Certain information has been updated in Annex I (examples) in order for the content to be brought more closely into line with the rest of the standard, particularly Annexes C to F. For example, the $MTTF_D$ values of both switches and of the contactor are now determined from B_{10D} values via n_{op}.

Discussion

The Amendment 1 of the wide accepted ISO 13849-1 has successfully answered many needs which arose during its practical application throughout the last years: integration of components without safety rating by the manufacturer (e.g. standard PLCs); consideration of the “probability of occurrence of a hazardous event”; higher typical $MTTF_D$ estimates for hydraulic components with a small number of annual operations; evaluation of the quantifiable aspects of the PL without using $MTTF_D$ values but based on the use of well-tried components; and many more. With these new solutions the standard is ready for another longer period of practical application.

At the same time the Amendment started, a new work item proposal to merge IEC 62061 and ISO 13849 to a combined standard ISO/IEC 17305 was initiated. This project has so far produced a first committee draft which merely integrates the content of both standards and adds some additional methods. At the moment it is not foreseeable when this projekt may be finished and what the added value compared to ISO 13849 will be. Many reasons for this new work item proposal, as e.g.simplified rules adaptable from low to high complex systems or improvements of the risk estimation method, have already been solved by the Amendment 1 of ISO 13849-1. Other improvements may earlier be converted by publishing a technical report in addition to the well established functional safety standards. Some reasons, as the use of a common reliability approach for components in the type B standards and the component standards, may be implemented independent from the “merging”.

The next step in the long-term evolution of ISO 13849-1 would be to start a maintenance cycle. This would give the opportunity to improve major issues which were identified in the amendment process but were outside its scope. Examples are the revision of the software requirements or integration of other improvements, even from the “merging” project.

Conclusion

The Amendment 1 of ISO 13849-1 has made great contributions for improved applicability by integrating many proposals arising from practical needs throughout the last years. The changes fit neatly into the concept of the standard, so that in general for existing SRP/CS no re-assessment is necessary.

The IFA will support the improvements of the Amendment 1 by updating their well established tools to assist the practical application of the standard, see www.dguv.de/ifa/13849. The Performance Level Calculator disc [3] has already been updated and a first publication to explain the changes introduced by the Amendment (similar to this paper) will soon been released. The revision of the well known BGIA Report 2/2008e [8] including many circuit examples has already started as well as an update of the software tool SISTEMA [9] to support the new content of the standard.

References

[1] ISO/TR 23849: 2010, Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery

[2] EN ISO 12100:2010, Safety of machinery – General principles for design – Risk assessment and risk reduction

[3] Performance Level Calculator Disc, 5th edition 2015, IFA, Sankt Augustin http://www.dguv.de/webcode/e20892

[4] *Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schaefer, M.*: Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) No 6, pp. 34-37 http://www.dguv.de/medien/ifa/de/pub/grl/pdf/2009_249.pdf

[5] EN ISO 13855:2010, Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body

[6] *Hauke, M.; Apfeld, R.*: The SISTEMA Cookbook - Part 4: When the designated architectures don't match. DGUV, Berlin 2012 http://www.dguv.de/webcode/e109249

[7] *Apfeld, R.; Schaefer, M.*: Safety functions to EN ISO 13849-1 where multiple overlapping hazards are present, IFA, Sankt Augustin 2011 http://www.dguv.de/medien/ifa/en/pra/en13849/safety_functions.pdf

[8] *Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.; et al.*: Functional safety of machine

controls - Application of EN ISO 13849; BGIA Report 2/2008e; DGUV, Berlin 2009 http://www.dguv.de/webcode/e91335

[9] Software-Assistent SISTEMA: Safety Integrity Software Tool for the Evaluation of Machine Applications; A Tool for the Easy Application of the Control Standard EN ISO 13849-1 http://www.dguv.de/webcode/e34183

Corresponding address

Institute for Occupational Safety and Health (IFA), Alte Heerstrasse 111, 53757 Sankt Augustin, Germany, www.dguv.de/ifa

German Social Accident Insurance Institution for the energy, textile, electrical and media products sectors (BGETEM), Rheinstr. 6-8, 65185 Wiesbaden, Germany, www.bgetem.de

Servomotors and power drive systems - Key elements for the failsafe design of a servomotor press

James BAUDOIN, Jean-Paul BELLO, Jean-Christophe BLAISE

Institut national de recherche et de sécurité (INRS)

Abstract

Servomotor presses are innovative machines and their sales are increasing. Development of servomotors and the recent arrival on the market of power drive systems, featuring so-called "pre-defined" safety functions, have contributed to their emergence. There is still no specific European or international safety standard for these machines, although such a reference frame is currently being drafted by the ISO's "Metal forming machine tools" standardisation group. Against this background, INRS has conducted a study to assess the impact of new servomotor press design principles. This paper describes the three main stages fulfilled in this study and its different results. These stages involved making an inventory of techniques specific to servomotor presses, conducting a detailed study of these techniques and reviewing the validity of conventional protective devices for use on servomotor presses. More specifically, the present study indicates that a safety-related power drive system (PDS/SR) reacts to a failure by initiating a failsafe position and this may be different from the intended function. This can result in safety function degradation in the case of a servomotor press. To conclude, the paper describes the conditions, under which the protective devices included in design standards for "conventional" machines, can remain valid. For example, stopping time control is decisive in calculating the minimum safety distance required by protective devices.

Introduction to the Problem

Metalworking presses remain particularly dangerous machines, which demand implementation of appropriate safety measures for preventing serious occupational accidents.

INRS has focused on a generation of innovative servomotor presses; these are destined to become more widespread because the functions they offer are attractive to their users. For example, their slide movement and force characteristics are variable in real time, offering the possibility of performing complex work cycles. To date, no safety standard takes into account the specific characteristics of this type of press. It is important that these machines, which implement new technologies, achieve a level of safety equivalent to conventional presses.

Special techniques for actuating and stopping potentially dangerous moving parts are applied to these new presses. Slide movements are directly dependent on an electrical servomotor and cannot therefore be separated from this motor's rotation (see Figure 1).

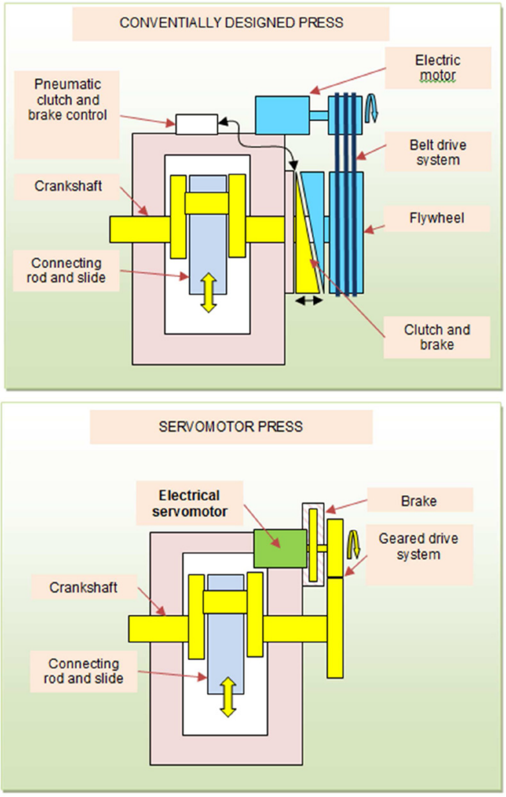


Figure 1: Diagrammatic view of eccentric drive conventional and servomotor mechanical presses

Development of servomotors and the recent arrival on the market of electronic power systems integrating "predefined" safety functions (IEC 61800-5-2 [1]) have contributed to the emergence of this type of press. Energy input-based stop functions, which have so far never been used as safety functions on these machines, can now be implemented. Development of design principles applicable to failsafe control systems suitable for servomotor presses using such electronic systems has proved to be necessary.

The INRS study was conducted in three stages, specifically making an inventory of techniques specific to servomotor presses, conducting a detailed study of these techniques and reviewing the validity of conventional protective devices for use on servomotor presses.

Inventory of Techniques specific to Servomotor Presses

Slide movements on servomotor presses are directly interlocked with drive servomotor movements. Servomotor rotation is only controlled, when a slide movement is required. Servomotors are used for:

- Controlling cycle stops and varying slide displacement characteristics at all points of the stroke (e.g. movement direction, speed, torque, etc.)
- Fulfilling safety functions (e.g. slide stop and hold to stop) based on energy input (regulation as long as energy supply is available).

Their control is ensured by an electrical control system incorporating an electronic power regulator. The latter is usually a safety-related power drive system (PDS/SR = Power Drive System/Safety-Related as defined by IEC 61800-5-2), which ensures control of safety functions such as safe stops.

It should be noted that a slide mechanical stopping device, such as a brake, is provided for controlling stops that cannot be controlled by one or more servomotors (e.g. when servomotors are de-energised).

Mechanical transmission between servomotors and slide

The purpose of the transmission mechanism is to convert the servomotor rotational movement into the slide translational movement (stroke). The following servomotor press and/or press-brakeslide drive techniques are used:

- An eccentric drive system: a connecting rod or toggle joint identical to those used in conventional mechanical presses
- A nut-and-bolt jointed mechanical system, in which one of the two parts is connected to the servomotor and the other to the slide
- Hydraulic cylinders usually controlled by servo pumps
- Systems combining pulleys and belts; these are more specifically found in press-brakes.

These mechanical systems can be coupled with the servomotors either directly or through gear or belt mechanical reduction drives.

The inventory of drive techniques for the servomotor presses available on the market in 2013 allowed us to classify concisely the main solutions used for presses and press-brakes. These are shown in graphical form in Figure 2.

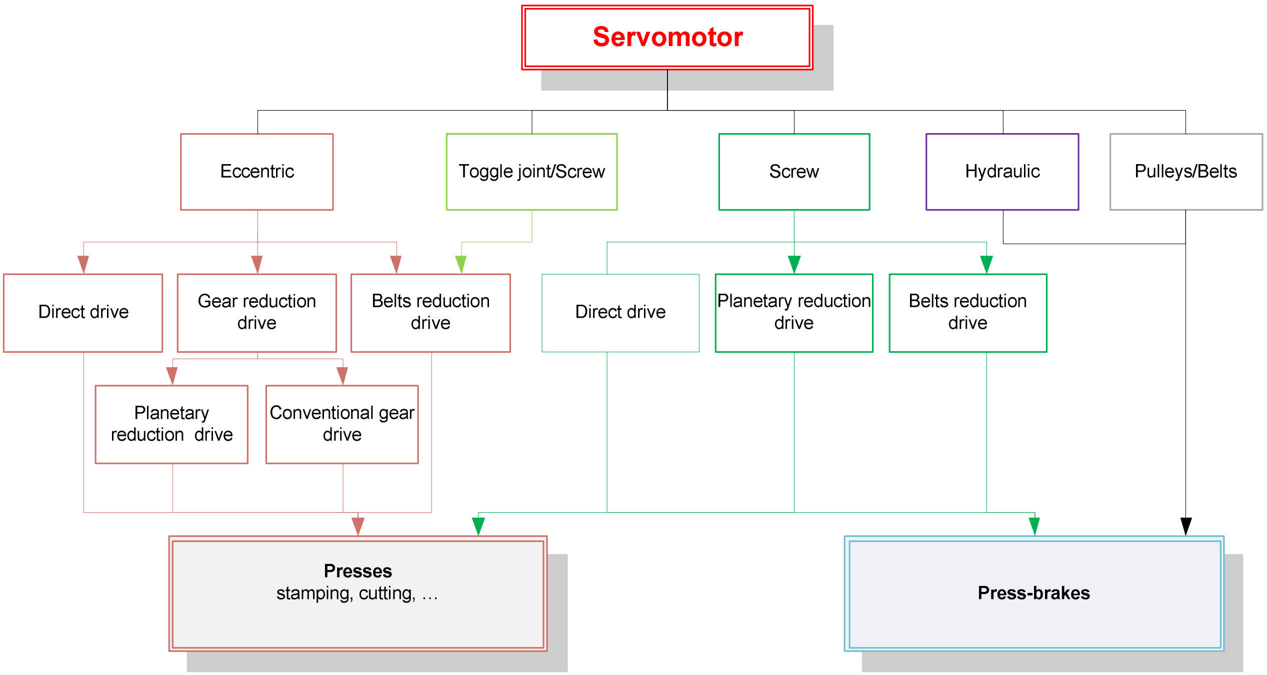


Figure 2: Classification of drive techniques for servomotor presses

Simplified representation of a servomotor press control path

The example illustrated in Figure 3 shows the different electrical and mechanical components in a control path for a servomotor mechanical press.

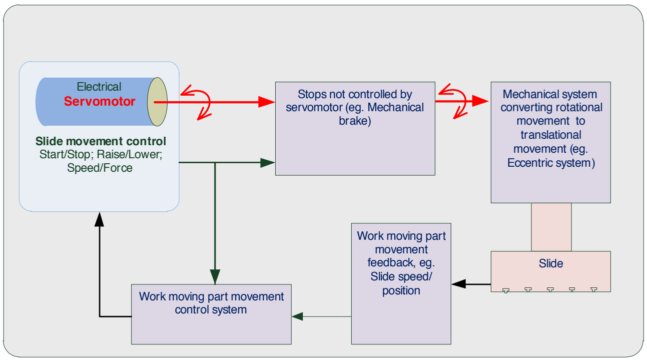

Electrical
Servomotor
Slide movement control
Start/Stop; Raise/Lower; Speed/Force
Stops not controlled by servomotor (eg. Mechanical brake)
Mechanical system converting rotational movement to translational movement (eg. Eccentric system)
Slide
Work moving part movement feedback, eg. Slide speed/ position
Work moving part movement control system

Figure 3: Representation of a servomotor press control chain

Inventory of Techniques specific to Servomotor Presses

The remainder of this document deals exclusively with the case of eccentric drive mechanical presses and does not consider the mechanical part of the transmission movement between the servomotor and the slide. To study the influence on safety of new technologies implemented on servomotor presses, we must first specify the safety functions contributing to operator protection by defining objectives. The following stage involves ensuring that components contributing to these safety functions effectively meet these objectives under normal operation and in the event of failure.

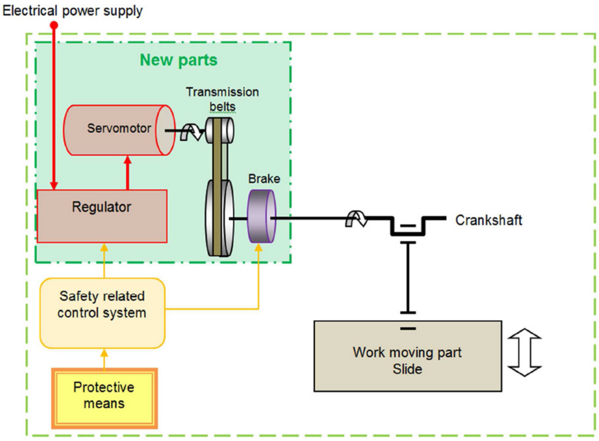


Figure 4: Example of kinematic chain for an eccentric drive servomotor press

Analysis of the kinematic chain of eccentric drive servomotor presses has enabled us to identify the parts (links) involved in the slide downward movement and to analyse their functional role. Figure 4 illustrates the different parts comprising this kinematic chain by highlighting in the green square the parts that differentiate this type of press from a conventional (clutch/brake) mechanical press.

Measures should be taken right from design stage to ensure that no single link in this chain, whether it be mechanical, electrical or other, can be hazardously affected in relation to fulfilling safety functions. Failure mode and effects analysis (FMEA) must therefore be carried out. Our study allowed us to determine and analyse the following points for each of the links in the kinematic chain and for each of the safety functions considered:

- Type of failure, if necessary part of component affected by a potentially hazardous failure and the conditions, under which this failure appears (type of stop, phase of press cycle, etc.)
- Effect on safety function behaviour
- Type of hazard that may result from this failure
- Measures to be implemented in reaction to failures and to prevent occurrence of hazardous situations.

The following sections detail a number of key points in these FMEAs.

Specifying safe stop functions

The manufacturer of a servomotor press must perform a risk assessment and reduce all risks right from design stage in compliance with the requirements of the so-called Machinery directive and when applying the recommendations of ISO Standard 12100 [14].

Human interventions in the tool zone (slide movement area) are usually required on all presses, including those integrating servomotors. For example, such interventions may be for operations involving setting or maintenance or during certain production phases, such as manual loading and unloading of parts. Safety measures must therefore be foreseen to ensure that no downward movement of the slide can occur as long as an operator is in this zone.

ISO Standard 12100 recommends the manufacturer to apply intrinsic prevention measures as a priority in order to eliminate hazards. However, this is usually impossible for hazards relating to a press slide. In most cases, guards or protective devices are required to protect the operator from the slide and this has indeed been assumed in the remainder of this study.

Slide safe stop functions suited to each potentially hazardous situation must therefore be foreseen and implemented. Our study reveals that these stop functions can play several roles, depending on the prevention devices provided and the conditions, in which they will be implemented. They can be applied to holding a static load and/or stopping a movement in progress and hence they require us to consider and accurately specify different characteristics.

As an example, a "photoelectric barrier-based stop" safety function fulfils two purposes:

- Preventing slide movement accomplishment as long as the photoelectric barrier is activated - a slide "safe" hold to stop function

- Stopping slide movements "covered" by the photoelectric barrier during its activation - a stop function initiated during the movement, for which the maximum slide movement response time must be precisely controlled.

To implement this stop function, it should be considered that:

- The servomotor and its control system (regulator) are involved in controlling stop functions: this is not the case for conventionally designed machines, on which a clutch/brake system is used. This system can be used actively by acting on certain parameters (torque, speed) to control deceleration phases and to ensure that the slide stop is maintained
- The slide embodies a resultant load under the effect of gravity; it cannot be maintained in position by a servomotor or servomotors no longer supplied with energy
- A mechanical brake is therefore needed to ensure the stop phases not guaranteed by the servomotor(s).

As detailed below, specific "types" of stop have been defined to take into account all these considerations.

Safe hold to stop without energy

Exclusion of electrical power supply to servomotor(s) concerned and simultaneous exclusion of energy supply (electrical or other) to device maintaining slide stop (mechanical restraint device).

Safe hold to stop with energy

Slide stop maintained while conserving electrical power supply to servomotor concerned.

Type 0 safe stop

Immediate exclusion of electrical power supply to servomotor(s) concerned and immediate exclusion of energy supply (electrical or other) to mechanical brake.

Type 1 safe stop

- Servomotor deceleration maintaining electrical power supply until movement stopped
- When stop is reached, exclusion of servomotor electrical power supply and immediate exclusion of energy supply (electrical or other) to mechanical brake.

Type 2 safe stop

- Servomotor deceleration until movement stopped
- When reached, stop is maintained

All actions performed, while maintaining electrical power supply to servomotor.

Protection stop

Slide stopped and stop maintained in reaction to activation of a protective device (mobile guards with locking devices, protective systems such as photoelectric barriers, 2-hand control devices, etc.) during a hazardous movement and acting in the form of a Type 0 safe stop or a Type 1 safe stop.

Analysis of Safety-Related Power Drive System (PDS/SR) behaviour

The PDS/SR is composed of the servomotor and its control system (electronic regulator and sensors) as illustrated in Figure 5.

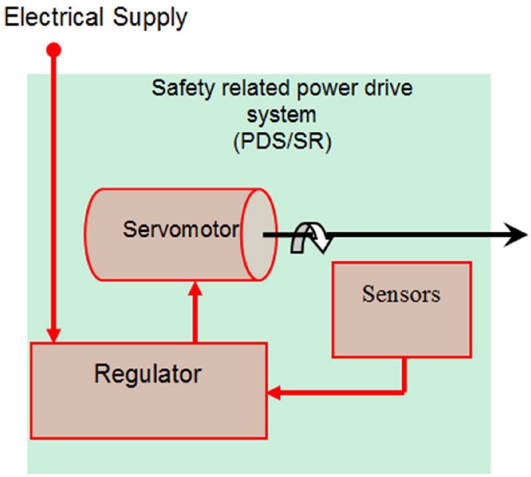


Figure 5: Diagrammatic representation of PDS/SR

Stop function implementation

If we take the example of implementing a "Type 1 safe stop", the electronic regulator is involved in controlling slide deceleration, while the servomotor electrical power is maintained until the movement has stopped. When a stop is reached, the regulator switches off the power supply to the servomotor until it is commanded again. An electronic regulator contributing to a stop function must be designed such that it is capable of ensuring safety functions based on a safety "performance level" according to ISO Standard 13849-1 [3] or an SIL according to IEC Standard 62061 [4], which are compatible with the level of risk to be covered. In the present case, use of a component complying with IEC Standard 61800-5-2 is recommended. This standard specified the safety functions to be implemented by PDS/SR, including stops such as "SS1" (Safe Stop 1). Some of these functions may be suitable for contributing to a "Type 1 safe stop".

As previously mentioned, this guarantee is insufficient and it is also necessary to analyse PDS/SR behaviour, when subject to failure of one of its parts (servomotor, electronic regulator, sensors). Analysing the behaviour of this type of component, when a failure occurs, shows that the servomotor stopping conditions can be degraded. For example, non-adherence to the deceleration slope or acceleration or unintended shutting off of the servomotor power supply.

The PDS/SR can detect this failure. However, alone it can only provide one fall-back function: guaranteeing that no torque will be exerted by the servomotor. This function is termed STO (Safe Torque Off) in IEC Standard 61800-5-2.

The manufacturer must therefore:

- Select, from the proposed electronic regulator options, the unit that allows failure detection and reaction compatible with the machine risk analysis
- Provide compulsory automatic application of a brake to overcome failed PDS/SR incapacity, despite it being designed to ensure a safety function, and ensure slide stoppage
- Take into account the moving part's stopping time, when a failure occurs and when this failure has an impact on the specified safety function (e.g. protection stop) This stopping time may differ from that obtained when PDS/SR failure has not occurred, depending on the failure detection time, the STO function activation time and the stopping performance characteristics of the brake.

Figure 6 illustrates an example of Type 1 safe stop function behaviour, when using an SS1.b stop as defined by IEC Standard 61800-5-2. The same function is shown in Figure 7, when there is a failure resulting in longer slide stopping time.

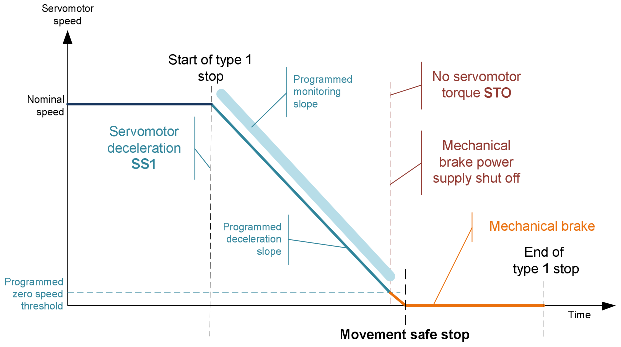


Figure 6: Chronogram of a Type 1 safe stop function using an SS1, b stop)

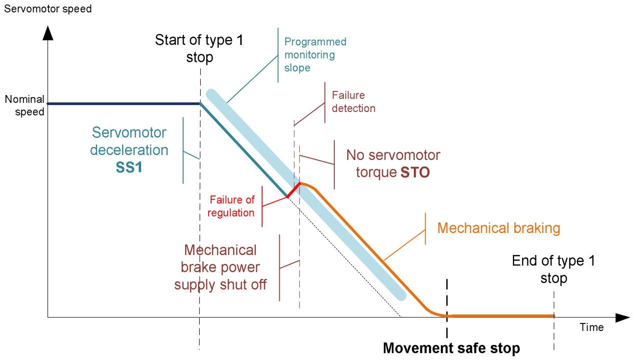


Figure 7: Chronogram of a Type 1 safe stop function using an SS1, b) stop and reaction under PDS/SR failure

Figure 8 illustrates an example of Type 2 safe stop function behaviour, when using an SS2.b stop as defined by IEC Standard 61800-5-2.

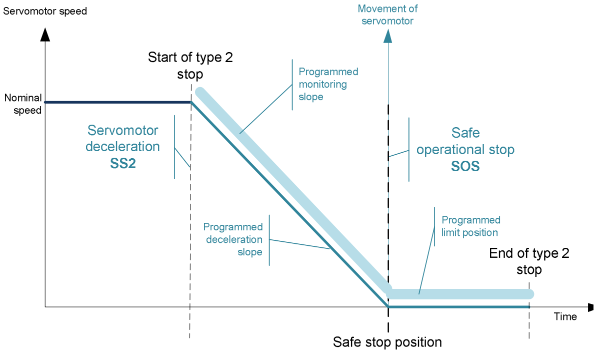


Figure 8: Chronogram of a Type 2 safe stop function using an SS2, b) stop function

Figure 9 illustrates the implementation of this type of stop via the PDS/SR with a failure occurring during the stop holding phase. This failure generates an unintended slide movement, when the protective device can be inhibited.

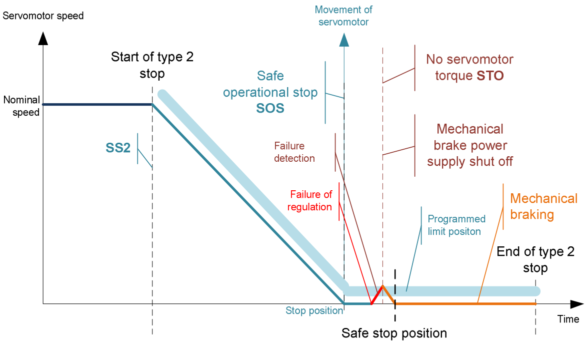


Figure 9: Chronogram of a Type 2 safe stop function with implementation of an SS2, b) function and reaction to a PDS/SR failure during stop holding phase

The operator may already be in a hazardous zone in this situation. The slide may have moved prior to the reaction to the failure stopping the movement; this is impossible with Type 0 and Type 1 safe stops. This stopping principle may only be acceptable, if the unintended movement remains within limits fixed by risk assessment.

This example is representative of similar problems that may arise for most of the safety functions ensured by PDS/SRs on the market. In the event of failure, they can only ensure one fall-back function themselves, namely an STO. The manufacturer must therefore adopt a strategy similar to that described for the case of a stop to ensure that the failure causes no hazard.

Slide movement control using a servomotor

On eccentric drive presses, the motor rotational direction is not always representative of the slide displacement direction and, even less so, when the "pendulum cycle" is used; this allows movement reversals independent of the connecting rod kinematics.

However, protective device inhibition is commonplace during the slide raising phase, if this is not hazardous. Technical measures must therefore be taken for controlling servomotor and slide movement directions to guarantee that inhibition can only be active during the cycle phases, in which it is expected.

Among prevention means foreseeable on a press, a continuous action control combined with a low slide displacement speed can be used. The PDS/SR contributes to implementation of this safety function in relation to stop control and safe speed limitation aspects. Speed limitation must be guaranteed at least throughout the slide lowering phase based on the fact that, on an eccentric drive press, the relationship between the servomotor rotational speed and the slide speed is sinusoidal, not linear (maximum speed at 90° and zero at 180°).

To ensure "safe" directional and speed control of the slide movement, the following specific measures must be implemented:

- Implement a safety function to control slide displacement direction and speed
- Ensure movement data acquisition for the slide itself rather than from the servomotor
- Control characteristics of sensors used (encoder), especially their potentially hazardous failure modes
- Analyse and control behaviour of different measures in the event of a failure to prevent all hazardous situations.

Braking and/or stop restraint device

Presence of a braking and/or restraint device is essential whatever the type of safe stop envisaged. This system can be used to:

- Keep the slide stationary
- Brake and stop the slide during Type 0 safe stops
- Brake and stop the slide in the event of PDS/SR failure or energy absence for Type 1 or Type 2 safe stops.
-

The braking system can be located at various places in the transmission chain (between the servomotor and the slide), but all the transmission parts between the brake and the slide must be failsafe.

The braking system must be correctly dimensioned to ensure the parts of the function, to which it must contribute. For maintaining a stop only, the system must be dimensioned to retain the maximum weight of the moving part (slide, tools, etc.) without inertia. When it is to ensure braking under normal operation or in the event of a failure, it must be calibrated not only for the moving part's maximum characteristics (speed, weight, etc.), but also in accordance with the expected or required stopping performance characteristics in relation to positioning of protective devices. The main difference with respect to the brake of a conventional press (e.g. mechanical press incorporating a clutch-brake system) is that its level of usage may be very low (case of Type 1 or Type 2 safe stops).

The brake design rules remain the same as those established in particular in Standard EN692 for existing mechanical presses. Similarly, measures must be implemented to control automatically brake wear.

Validity of Conventional Protective Devices on Servomotor Presses

At design stage, the manufacturer often has to select a means of protection (guard, protective device) to cover hazards identified during risk assessment. Implementation of servomotors on presses does not change the assessment of hazards for operators. Means of protection listed in normative reference documents relating to the design of "conventional" machines remain valid under certain conditions.

Total control of moving part stopping time prevails, when guards without a locking device and protective devices are used. This is in fact necessary in order to position correctly the protective devices in relation to the hazardous zone. Implementation of certain stop functions by a PDS/SR may cause longer response time in the event of a failure, so this time must be known and precisely controlled.

Stopping time depends on several factors including stop type configuration, the options retained for this stop type within the PDS/SR and the performance characteristics expected of the braking system. In every case, the stopping time must integrate the worst case conditions for the machine (speed, moving part weight) and well as at PDS/SR level.

The moving part stopping time has no effect on safety in the case of guards with a locking system. Moreover, only a hold to stop function is required, if this means of protection is implemented without protection inhibition during the slide raising phase.

Choosing this means of protection may therefore allow one to take advantage of servomotor functionalities by overcoming technical constraints involving stop time control.

Discussion and Conclusions

Unlike "conventional" presses the power drive system on servomotor presses no longer simply supplies the mechanical or electrical energy required to actuate only the slide movements. It contributes fully to fulfilling the safety functions implemented to protect from identified risks.

The PDS/SR becomes the nucleus of the control system allowing implementation of new operating modes and ensuring, in part, many of the safety functions required to protect operators (different types of stop, speed and position control and limitation, rotational direction control, etc.).

By virtue of its design (electronic component) and method of controlling multiple safety functions (by supplying energy), the PDS/SR can be affected by failures leading to degradation of the safety functions to be fulfilled.

Safety function degradation can be reflected in terms of either longer response times or the impossibility of fulfilling alone the expected function in the event of an internal failure or in the absence of energy in the PDS/SR.

Different systems on the market all provide a safety fall-back function comprising no servomotor torque. While this fall-back position is enough for some machines, it cannot fully ensure the expected functions, in particular those for ensuring a stop and hold to stop, for metal presses, in which potentially hazardous moving parts work vertically and are subjected to gravity.

When access to the hazardous zone is possible during slide movement (when guards without a mechanical locking system or protective devices are used), a brake capable of stopping the slide for a Type 0 stop, in the event of a PDS/SR failure or a loss of electrical power must be provided. This brake must be dimensioned for the machine maximum capacity. The stopping time required for positioning the protective devices must be determined under worst case conditions for the machine (speed, driving weight). The most penalising failure must be considered in terms of the response time of the overall control system including the PDS/SR.

Implementation of a restraint device may be enough, when access to the hazardous zone is impossible during slide movement (case of guards with a mechanical locking system without inhibition).

The protective devices recommended for conventional presses are equally recommended for these new presses. Special attention should be given to determining the stopping time required for calculating the safety distance for positioning certain guards and protection systems.

When inhibition during a slide raising phase is not essential, we recommend studying the option of using an interlocking guard with a locking device, even if the risk analysis offers the possibility of using other protective devices. Controlling slide stopping time is not necessary with an interlocked guard so there will be less technical constraints involved in designing and manufacturing the press (no braking system, only a restraint device and limited number of safety functions controlled by the PDS/SR, etc.).

An important point concerning Type 2 safe stops has been revealed and their consequences have been clearly identified. It remains to be defined, during standardisation work, whether this principle can be accepted for these presses and to what extent an unintended movement caused by a failure does not create a hazard.

During the course of 2015, the detailed results of the INRS study will be published in a scientific and technical memorandum aimed at designers, users and prevention specialists.

They will also be used for standardisation work undertaken by the ISO/TC 39/SC 10/WG1 group dealing with servomotor presses.

References

[1] IEC 61800-5-2:2007 - Adjustable speed electrical power drive systems -Part 5-2: Safety requirements – Functional, 2007, 70 p.

[2] NF EN ISO 12100 - Safety of machinery - General principles for design - Risk assessment and risk reduction, 2010, 93 p.

[3] NF EN ISO 13849-1 - Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design, 2008, 88 p.

[4] NF EN 62061 - Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems, 2005,104 p.

Corresponding address

James Baudoin, james.baudoin@inrs.fr

INRS Centre de Lorraine

Rue du Morvan - CS 60027 - 54519 Vandœuvre Cedex - France

Tel. +33 3 83 50 20 00

Note: The following manuscript was submitted but not presented orally

Optimal safety devices in safety-related control systems for low to middle risk applications

Ikuo Maeda [a], Kazuya Okada [a], Yoshio Sekino [a], Masao Dohi [a], Toshihiro Fujita [a], Takao Fukui [a], Shigeru Tsujimura [a], Masatake Yamano [a], Tatsuyoshi Kuriyama [a], Takeshi Kondo [a], Takeo Yasui [a]

[a] *IDEC CORPORATION*

Abstract

The risk assessment has been widely accepted and risk reduction measures have been implemented in a lot of work places with high risks. However safety measures for work places with low to middle level risks have not been appropriately implemented so far.

The potential risks on machinery safety depend on the scale of work place, the type of industry, the type of work piece, the level of operators involved. If the risks are unacceptable, a risk reduction should be implemented[1][2]. When the risk reduction is conducted by a control system, the safety level of the control system is determined by the risk level according to international standards[3].

The system with high risks which would cause severe hazard should be equipped with a safety-related control system that meets safety requirements for PLe or SIL3. This concept has been becoming popular in the industrial automation. However, the safety-related part of the control system is often constructed with safety control devices complying PLe or SIL3 regardless of the actual risk level.

Although constructing the safety system with devices complying higher PL or SIL level than required PL or SIL is acceptable in terms of safety, productivity and efficiency are compromised by excessive complicate safety system for the low risk work place and cost up because of it.

To facilitate appropriate risk reduction measures for low to middle risk level process, the circuit examples using the optimal safety control devices are herewith proposed.

Keywords:

Safety-related control system; Safety control devices

Introduction

Today, the concept of safety with regards to machine safety is widely recognized and relatively high risk press machines, robots, machining tools and others represented by the mechanical system utilizing industrial robots shown in Figure 1 are risk assessed properly according to the international safety standards and the like and the risk reduction measures are taken using appropriate technology. However, securing the safety according to the international standards for the relatively low risk machines such as small-sized food processing machines, packaging machines and the like has not become widespread yet [2][3][5][6][7][11][12][14][16][17].

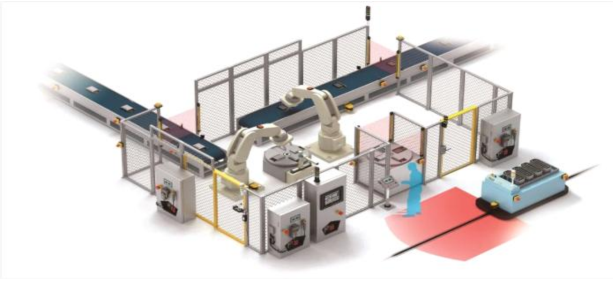
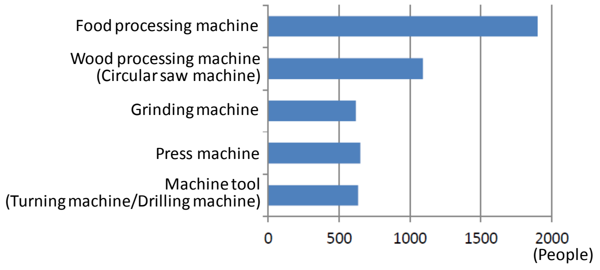


Figure 1: Mechanical system using robots

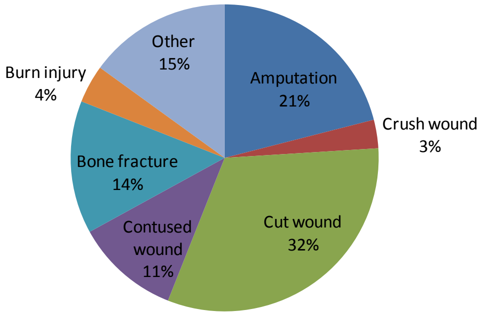
Machine types with high number of accident

As shown in Table 1, there are as many as about 2,000 incidents of industrial accident by food processing machines and the number is especially high compared to other industrial machines such as machining tools and press machines[18]. Also, as shown in Figure 2, the breakdown of the industrial accidents indicates that in addition to serious accidents (amputation and crushing) of about 25%, the not-quite-so-serious accidents (cuts and contusions) of about 40% is distinctively high[18]. Also, it is thought that one of the reasons for this is the fact that the small-sized food processing machines for cutting and mixing are not only used in a large scale environment such as a food processing plant but is also used often in stores and the kitchens of restaurants (tertiary industry). That is, the reason there are many accidents by food processing machines is that there are many machines in the food processing machines that

Table 1: Number of accidents by representative machines (quoted from brochure [18], and modified)



Number of deaths and injuries requiring an absence of 4 or more days in 2012



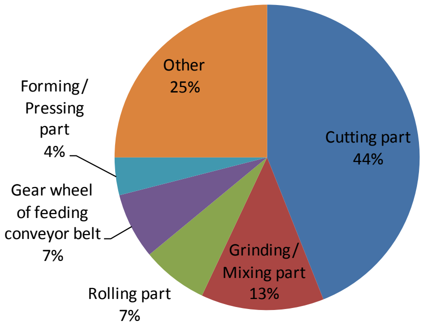
(quoted from brochure [18], and modified)

Figure 2: Percentage of the type of injury and disease caused by food processing machines

have simple functions such as cutting, mixing and so forth that are relatively low risk functions, and because they are simple functions, sufficient safety measures were not built in at the design stage and the securing of safety was left to the users. In addition, it is thought that the another reason is that not only the workers in the plant but also the salespersons at the store and the cooks at the restaurants have the opportunity to use the machines often without understanding the risk of the machines.

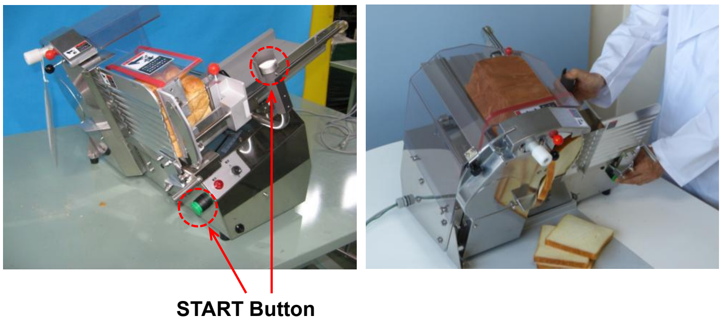
Risk reduction measures for food processing machines

As shown in Figure 3, when the ratio of the accidents are looked at by the moving parts of the food processing machine, the fact that the moving parts for cutting, slicing, grinding and mixing account for nearly 60% of the accidents indicates that the safety measures for these moving parts of the food processing machines are important. However, since these parts in many food processing machines are not just moving parts of the machine but also parts that process food, it is important that the safety measure is implemented so that the foodstuff can be continuously fed to the parts. For the especially small-sized machines, since it is typical that the foodstuff is fed by hand, it is important that the safety measure protects the fingers besides allowing the foodstuff to be fed. It makes the machine useless if it is simply covered by a case or a fixed guard is placed to isolate the moving parts. Therefore, it becomes especially important to construct a system for an interlock and a shutdown by the appropriate safety control in order to reduce the risk to an acceptable level without losing the operability of the machine[4][5][6]. Similar to other machinery, in order to reduce the risk of the food processing machines, safety measures need to be implemented at safety levels that correspond to the risk levels, but many accidents still happen in recent years because the appropriate safety measure is not widely implemented. Under these kinds of circumstance, in 2013 Japan has amended and put into effect the “Ordinance on Industrial Safety and Health” that mandates safety measure for the food processing machines[18].



(quoted from brochure [18], and modified)

Figure 3: Percentage of accidents by movable parts of food processing machines



(quoted from brochure [18], and modified)

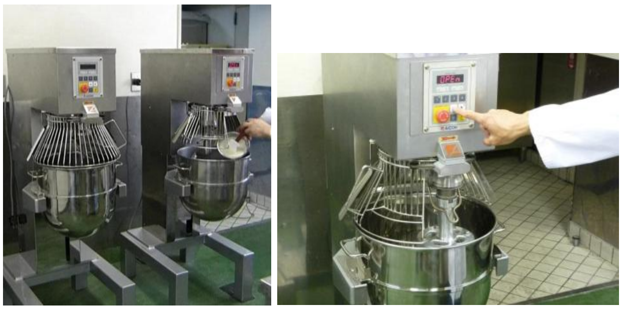
Figure4: Food processing slicer (With two-hand operated control device)

Specifically, it mandates the installation of a cover for the dangerous part of the food processing machine and the shutdown during an operation such as the feeding of the foodstuff and the use of safety equipment and so forth. Especially, safety measures thought to be effective for the prevention of serious accidents such as amputation and crushing are described in the brochure as examples. The following are brief descriptions of them.

Figure 4 is an example of a slicing machine for food processing (bread slicer) with an appropriately installed protective measure. The blade rotates only when the two buttons are being operated by both hands and the blade stops immediately when one hand is released from the button which reduces the risk of the amputation or cutting of fingers[4][7][9].

Figure 5 is an example of a safety device on a food processing mixer. The left figure shows an interlock mechanism that prevents the rotating part from moving if the movable guard is not shut. The right figure shows a function that allows the the mixer to rotate at a low speed when you really want to operate it with the movable guard open only while the button is being pushed, namely, the hold-to-run control device[5][7].

Figure 6 is an example of a combination of 3-position enabling device and above mentioned hold-to-run control device, which is a manual control device that permits the operation of the machine when it is to be operated continuously (operation is permitted when the device is held in a proper condition and the machine is stopped when the handle grip is squeezed or released.) Especially because the 3-position enabling device is effective for securing the safety during low speed operation of maintenance mode of relatively high risk devices, it is applied to the safety equipment that is effective for securing the safety of the operation of high powered robots in a teaching mode[7][10].



quoted from brochure [18], and modified

Figure 5: Food processing mixer (with interlock mechanism, hold-to-run control device)

In this brochure, the objective to reduce the serious accidents such as amputation and crushing by food processing machines is introduced, especially by these protective measures. It is necessary to build and implement a safety system that has the safety level equal to the previously mentioned mechanical system utilizing robots in order to secure the safety from these sources of serious dangers.

However, as shown previously, there are many accidents that are not so serious (cuts and contusions), amounting to about 40%, and from the risk perspective, we can see that there are many sources of danger with lower risk level in the food processing machines compared to the mechanical system utilizing robots, as shown in Table 2[17].

Especially, there are many injuries from the small-sized machines whose severities are limited. However, because these types of devices require feeding of foodstuff and removal of foreign objects by human hands, there is a level of risk that cannot be ignored due to high frequency of access such that it is necessary to implement a safety measure for that risk as shown in the Figure 7.

Though the safety components widely distributed in public, most of those are desighned to correspond with high level risk (corresponding to demand performance level) and there is practically no safety component that is optimal for machines with medium to low risks currently.

Table 2: Comparison of the risk between food processing machine and mechanical system using robots

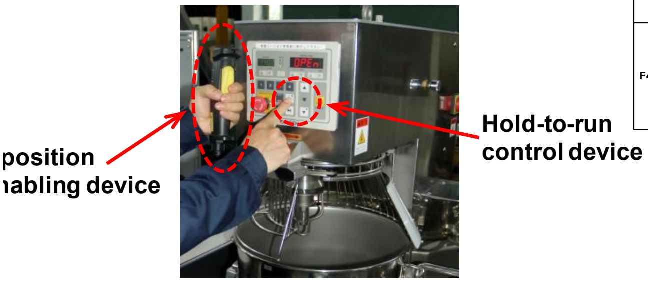
(Risk of mechanical system using robots)

Plant		Workplace		Process (system)	Work			
Kyoto		Production Technology Center		Robot Control Cell / Electric Control Equipment Production	Maintenance Operation (1)			
					Hazard Risk before taking Protective Measures			
No.	Equipment	Hazard	Work Type	Hazard Details	Severity of Injury A	Access Frequency B	A + B	Risk Level
M1	Pendant	Touch panel	Maintenance	Because touch panel does not provide tactile feedback, the operator cannot keep his eyes on the robot's movement (need to confirm operation with touch panel from time to time).	4	4	8	High
M2	Robot module (vertical multi-joint)	Vertical multi-joint robot	Maintenance	Collision of robot and operator	4	4	8	High
M3		Vertical multi-joint robot	Maintenance	Collision of other robot's unexpected motion with operator	4	4	8	High
M4	Robot module (horizontal multi-joint)	Horizontal multi-joint robot	Maintenance	Collision of robot and operator	4	4	8	High
M5		Horizontal multi-joint robot	Maintenance	Collision of other robot's unexpected motion with operator	4	4	8	High
M6	Robot module	Chuck (hand)	Maintenance	Collision with chuck (hand)	4	4	8	High
M7				Caught in the chuck's clutch	1	4	5	Moderate
M8	Jig module	Parts fixation jig	Maintenance	Caught in the fixating jig	4	4	8	HIgh
M9	Parts feeding tray module	Parts feeding tray driving part	Maintenance	Caught by the driving chain of parts feeding tray	4	2	6	Moderate
M10				Caught in the parts feeding tray driving part	1	2	3	Low
M11				Collision with parts feeding tray	1	2	3	Low

(Risk of food processing machine)

Plant			Workplace		Process (system)	Work			
Japan			Food factory		Food machine	Operation			
No.	Equipment		Hazard	Work Type	Hazard Details	Hazard Risk before taking Protective			
	Type	Size				Severity of Injury	Access Frequency	A + B	Risk Level
F1	Food loading machine	Large (for plant)	Rotary blade in hopper	Normal operation	During the feed of material, slipped into the hopper, and caught in the rotating blade to death	8	2	10	High
		Small (for shop)			During the confirmation of the material in the hopper, rotary wing and hand clash	4	2	6	Moderate
F2	Food slicer	Large (for plant)	Cutter blade	Normal operation	After removal of the clogged material, the cutting blade is re-rotated and the hand is cut	8	2	10	High
		Small (for shop)			During slicing operation, the fingertip is cut	3	4	7	Moderate
F3	Food-mixing machine	Large (for plant)	Rotary blade in hopper	Normal operation	During the feed of material, slipped into the hopper, and caught in the rotating blade to death	8	2	10	High
		Small (for shop)			During the confirmation of the material in the hopper, rotary wing and hand clash	3	2	5	Moderate
F4	Frier	Large (for plant)	High temparature oil	Normal operation	During work, accidentally fall into the flyer, to death	8	2	10	High
		Small (for shop)			When throwing in the foodstuffs, oil splashes to hand to burn	2	4	6	Moderate

When the safety component that corresponds to high risk level machines are used on a relatively low risk level safety system (safety control circuit), the functions become too excessive and a more complex than necessary safety control circuit needs to be built when it is designed according to the functions of the safety component. Of course this is not a problem to be on the safe side when safety is the only thing that matters, but it would be difficult to implement because it leads to an increase of space due to unnecessary duplications and increase of the design, the wiring workload and the number of parts. Therefore, ultimately, a generic control circuit is used for control and this author has seen many cases where no safety control circuit is used at all.



quoted from brochure [16], and modified

Figure 6: Food processing mixer (with 3 position enabling device + hold-to-run control device)

As background information, we can point out that many of the manufacturers of the previously mentioned food processing machinery are small to medium scaled corporations and, especially in recent times, there are an increase of requirements for the streamlining of the

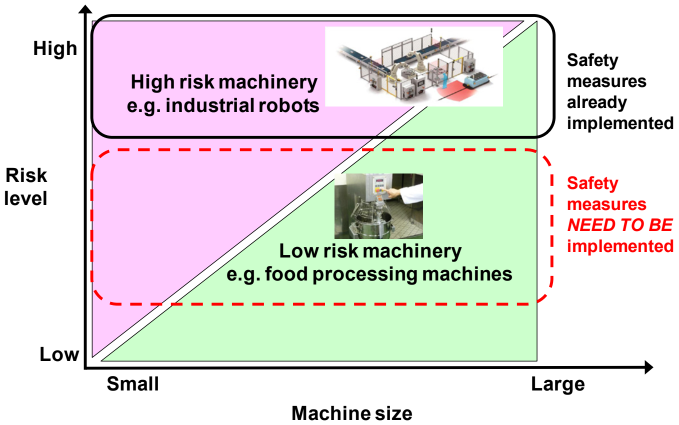


Figure 7: Necessity of safety measures for low-risk machinery

production equipment and down-sizing of the machines for the purpose of using them in stores and kitchens. Especially in the case of food processing machine, food safety (health risk) measures are implemented preferentially and, moreover, when it comes to small-sized machines, there is a trend to avoid the implementation of the safety control circuit because the manufacturers do not want to increase the cost with the safety devices or safety control circuits. Therefore, the safety components that are widely used in public which can handle high performance level – being able to configure a high category level of safety circuit, having the number of terminals to be able to configure redundancy and perform monitoring – cannot fully contribute to the safety of the relatively low risk small-sized food processing machines at present time.

The following are examples of typical safety control circuits according to the size of the risk that they correspond to.

Example of the safety control circuit and safety component according to the risk of the machine

Figure 8 is an example of a safety control circuit that corresponds to high risk of a mechanical system and others that use robots[3][12]. The circuit is configured to be able to generally support up to the performance level (PL) of e, d level and category 4, and is constructed using safety components that can support up to category 4. Connections are made so that redundancy of input and output, check function and so forth are established and the safety component functions are fully utilized. In reality, although it is necessary to take safety measures with a proper method based on the result of a risk assessment, in the cases with serious risks mentioned previously, where cutting machines and mixers for food processing can lead to amputation and crushing of fingers, a safety system that has similar safety control circuit is needed. Figure 9 is an example of a safety control circuit of small-sized machine with relatively low risk among the food processing machines. This is a circuit configuration equivalent to PL b to PL c level and category of 1, but because the safety components being used are able to support much higher PL and category there are unused connections and functions which create waste in terms of cost and space. However, if the circuit is to be configured that is equal to the mechanical system that uses robots having high risk as shown in Figure 8, it causes more complex wiring to be added than necessary for machines that can be sufficiently supported with lower risk measures and the machine manufacturers would hesitate to implement it.

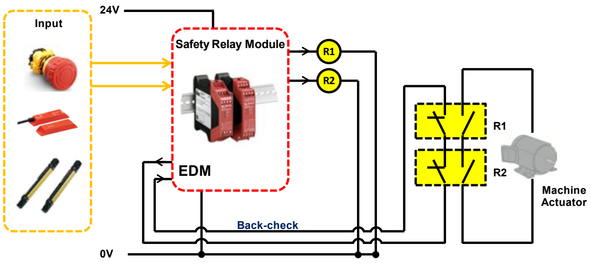


Figure 8: Example of safety control circuit corresponding to high risk

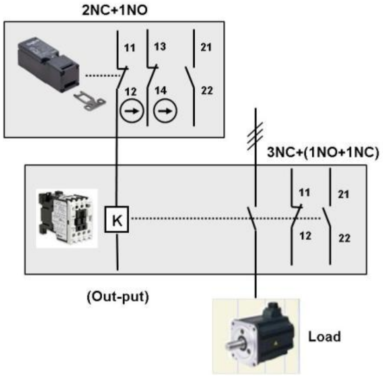


Figure 9: Example of application of components corresponding to high risk to the safety control circuit of a relatively low risk mechanical system.

Figure 10 is an example of the safety control circuit applied to interlock devices and others for the relatively low risk small-sized machines among the food processing machines and it has the optimum circuit configuration for PL and category corresponding to the medium and low risk and uses the optimum safety components for it. Since there are no unused connections or left over terminals, the wiring is simplified and there are space and cost saving benefits.

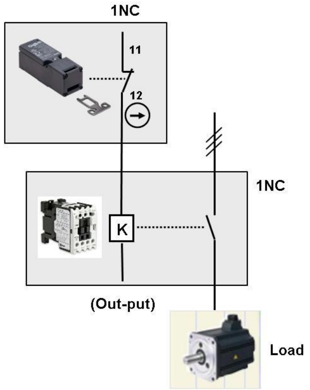


Figure 10: Example of application of components corresponding to low risk to the safety control circuit of a relatively low risk mechanical system.

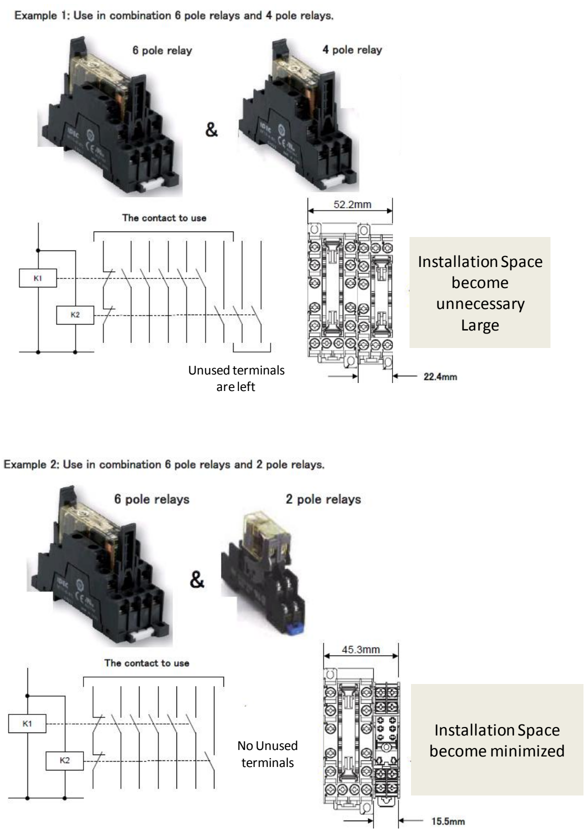

Example 1: Use in combination 6 pole relays and 4 pole relays.
6 pole relay
4 pole relay
&
The contact to use
K1
K2
Unused terminals are left
52.2mm
22.4mm
Installation Space become unnecessary Large
Example 2: Use in combination 6 pole relays and 2 pole relays.
6 pole relays
2 pole relays
&
The contact to use
K1
K2
No Unused terminals
45.3mm
15.5mm
Installation Space become minimized

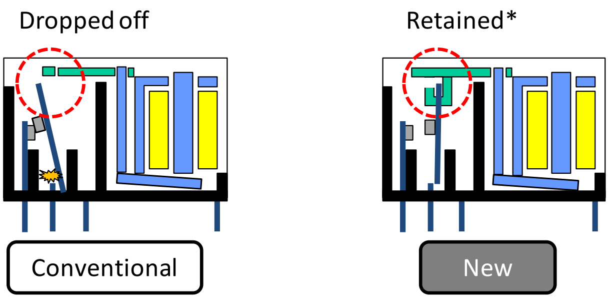
Figure 11: Example of a force guided relay that is appropriate for the safety control circuit of a relatively low risk mechanical system

Safety components that are suitable for the safety control circuit of medium to low risk machines

In the case of the safety control circuit of medium to low risk machines, it can be said that the key to its widespread usage and implementation is in the safety components used to construct the circuit. Here, we will introduce the examples of our new technology on the Force Guided Relays and Door Interlock Switch [5][8].

-New Technology on Force Guided Relay

As shown in the upper figure of Figure 11, the force guided relay widely distributed in the general market is configured with connections of 4 poles or more, and unused terminals are left in this circuit configuration and the installation space become unnecessarily large. As shown in the lower figure, space can be minimized by using two-pole (1NO+1NC) relay and this also leads to the reduction in cost as a result.



* Construction to retain the contact spring by hooking in the projection of the actuator in order to avoid unintended conduction by dropping off of the contact spring when breakage of the contact spring.

Figure 12: Example of the short circuit prevention technology when spring breakage occurs on Force guided relay

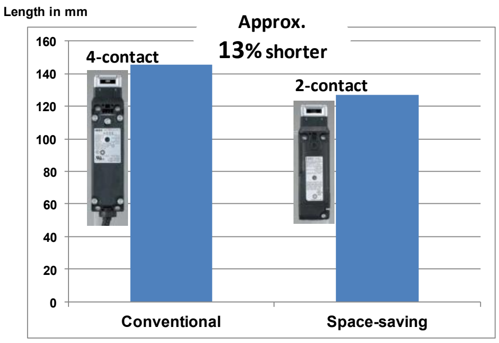


Figure 13: Comparison of length between the conventional construction of door interlock switch and the space-saving construction that is suitable for small machines with medium to low risk machines

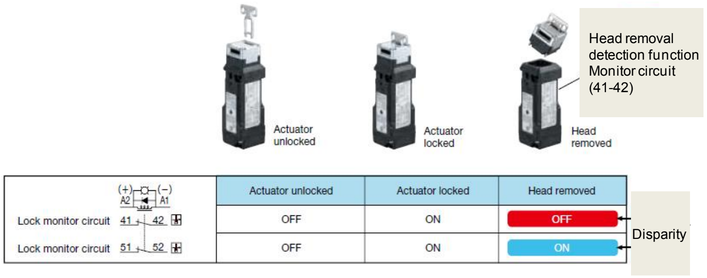
Furthermore, as shown in Figure 12, a new technology for force guided relays is developed that takes safety into consideration, although it does not directly affect the PL and category of the safety control circuit. This structure allows short circuit to be avoided between the same or different poles when the contact spring is broken.

-New Technology on Door Interlock Switch

Figure 13 shows an example of space-saving construction on door interlock switch that is suitable for the safety control circuit of medium to low risk machines. It is important to save space when installing especially on the door of a small-sized machine, and this type of spring lock is effective for definitely securing the lock strength for safety. Also, in order to further assure the safety, a new technology is available to monitor the condition when the operating head becomes detached as shown in Figure 14.

Conclusion

In order to reduce further the industrial accidents, it is essential not only to secure the safety for the high risk level machinery but to focus the effort also for the relatively low risk level machinery. Especially, industrial accidents are easy to occur not only in the plants with food processing machines and the like, but even with the machinery used in stores and kitchens which are of



	Actuator unlocked	Actuator locked	Head removed	
Lock monitor circuit 41 42	OFF	ON	OFF	Disparity
Lock monitor circuit 51 52	OFF	ON	ON	

Figure 14: Example of a door interlock switch technology with a function added to the lock monitor circuit for detecting the detachment of the operating head

relatively low risk level. Also, because these machines are used not only in the developed countries but by various people in various countries including the developing countries, it is impossible to reduce the accidents by just relying on the operator for safety.

Therefore, the safety design of the machine itself becomes important. However, there are not many safety components that are suitable for safety control circuit supporting the low to medium risk levels. The safety component that can support the safety control circuit for the high risk level is overkill for this type of use and unnecessarily increases the hurdle for the implementation of safety control circuit. Therefore, there is a trend not to take the protective measure using the safety control circuit at all. That is to say, situations occur where the safety control circuit is not implemented in the places requiring control by a safety control circuit as pointed out by the results of the risk assessment and a generic control circuit is used for the control instead. The risk assessment result is not taken into consideration in a generic control circuit, and appropriate securing of safety cannot be planned because generic control components are used and their behaviors are not taken into account in the case of malfunction or damage. Furthermore, if interlock is not constructed from an appropriate safety control circuit, there is concern over the drop in the work efficiency with an increase in the number of unnecessary shutdown of the machine resulting in an increase in the non-operation time of the production equipment and reduction of the production efficiency.

In the future, in order to pursue further streamlining of production to be realized by the technological innovation such as IIoT technology, Industry 4.0, Industry Internet and others, it becomes especially important to properly perform risk assessment to realize the securing of work safety even in the changing production environment and properly construct the safety control system. Namely, it becomes increasingly important to properly perform risk assessment by personnel such as a safety assessor who has the sufficient knowledge, skills and abilities for risk assessment of machines and implement appropriate safety measures corresponding to various risk levels using the appropriate safety components[19]. Here, we have focused and elaborated on securing of safety for the relatively low risk machines (safety control circuit implementation of low PL and category) represented by the food processing machines in addition to securing of the safety for the conventional high risk machines, and we believe that this approach is applicable to securing of the safety in other areas as well. In order to promote the securing of safety in the future, we will strive to contribute to the reduction in industrial accidents by encouraging the utilization of the optimum safety component technology corresponding to the risk level along with presenting the optimum safety control system for the use.

References

[1] ISO/IEC GUIDE 51:2014, Safety aspects -- Guidelines for their inclusion in standards

[2] ISO12100: 2010, Safety of machinery -- General principles for design -- Risk assessment and risk reduction

[3] ISO13849-1: 2006, Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design

[4] ISO13850: 2006, Safety of machinery -- Emergency stop -- Principles for design

[5] ISO14119:2013, Safety of machinery -- Interlocking devices associated with guards -- Principles for design and selection

[6] ISO10218-1/-2:2011, Robots and robotic devices -- Safety requirements for industrial robots

[7] IEC60204-1:2005 +AMD1:2008, Safety of machinery - Electrical equipment of machines - Part 1: General requirements

[8] IEC61810-3:2015, Electromechanical elementary relays - Part 3: Relays with forcibly guided (mechanically linked) contacts

[9] IEC 60947-5-5:1997+AMD1:2005, Low-voltage switchgear and controlgear - Part 5-5: Control circuit devices and switching elements - Electrical emergency stop device with mechanical latching function

[10]IEC 60947-5-8:2006, Low-voltage switchgear and controlgear - Part 5-8: Control circuit devices and switching elements - Three-position enabling switches

[11] M. Mukaidono, Machine System Safety Technology in the Age of Globalization, The Society of Safety Technology and Application, The Nikkan Kogyo Shimbun, Ltd., 2000

[12] IDEC, Safety Concept Book, 2014

[13] M. Nobuhiro, et al., « Emergency Stop Switch and Enabling Switch: Safety Function of Human Interface », presented to Human Interface Symposium 2003, pp. 455-458

[14] T. Fujita, et al., « Next-generation Production System using Robots – Productivity and Safety Improvement by Assembly Shop », ROBOT No. 144, January 2002, pp. 46-57

[15] Japan Industrial Safety and Health Association, Ministry of Health, Labour and Welfare, « III-8. Robot-controlled Cell Production System “Assembly Shop” and Risk Assessment », Risk Assessment Data Collection on the Machine System for Safety – Activities at Machine Operation Sites, March 2005, pp. 115-126

[16] K. Okada, et al., « Risk Assessment and Optimization of Safety Protective Measures on Robot-controlled Cell Production System », presented to Human Interface Symposium 2006, pp. 433-438

[17] K. Okada, et al., « Risk Assessment of Robot Cell Production System that Achieved High Productivity and Safety in HMI Environment», presented to Safety of Industrial Automated Systems 2007, pp. 181-186

[18] the Ministry of Health, Labour and Welfare, Brochure for the revised industrial safety and health regulations enforced on October 1st, 2013, in which additional safety requirement for food processing machine

[19] I. Kumazaki, et al., «Safety Assessor Program Assessment»; 5th International Conference SIAS 2007, Japan, Nov.12-13, p.103-110 (2007)

Corresponding address

Ikuo MAEDA,

IDEC CORPORATION, 2-6-64 Nishimiyahara,
Yodogawa-ku, Osaka 532-0004, Japan

SIAS 2015

8th INTERNATIONAL CONFERENCE ON THE SAFETY OF INDUSTRIAL AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

Session 5: Protective devices and systems

Martin Wüstefeld, SICK AG, Waldkirch/Germany

Optical sensors for person detection – Outdoor use

Safety related applications of optical sensors used under outdoor environmental conditions are often requested. Use for person protection on railway stations or as protection equipment on Automated Guided Vehicles (AGVs) – the detection of persons under outdoor conditions is of interest in many different industries. But what does mean “outdoor”, and how is the safety related detection of persons achievable? Optical sensors give excellent performance in person detection in industrial applications under indoor environmental conditions. These are well known and defined in Standards. In “outdoor” application the situation is much more complex. Snow, Fog, Rain are factors with relevant influence on the performance of person detection. Furthermore the known criteria’s of industrial use are not valid in general – on railway stations children have to be assumed or other considerations of persons behavior. These factors have to be considered. SICK does have a long history in Development of Automation Sensors and Solutions in Process Industry with Outdoor use. Based on that the challenge for safety related person detection with optical sensors is presented. The physical effects of outdoor conditions and the actual data base out of Standards will be presented. Examples of actual projects show the challenge and suggestions will be made fort the further approach up to an safety related sensor for person protection under outdoor conditions.

NIR Camera Based Person Detection in the Working Range of Industrial Robots

Sebastian Sporrer, Holger Steiner, Maurice Velte and Norbert Jung

Bonn-Rhein-Sieg University of Applied Sciences
Safety and Security Research Institute

Abstract

Persons entering the working range of industrial robots are exposed to a high risk of collision with moving parts of the system, potentially causing severe injuries. Conventional systems, which restrict the access to this area, range from walls and fences to light barriers and other vision based protective devices (VBPD). None of these systems allow to distinguish between humans and workpieces in a safe and reliable manner. In this work, a new approach is investigated, which uses an active near-infrared (NIR) camera system with advanced capabilities of skin detection to distinguish humans from workpieces based on characteristic spectral signatures. This approach allows to implement more intelligent muting processes and at the same time increases the safety of persons working close to the robots. The conceptual integration of such a camera system into a VBPD and the enhancement of person detection methods through skin detection are described and evaluated in this paper. Based upon this work, next steps could be the development of multimodal sensor systems to safeguard working ranges of collaborating robots using the described camera system.

Keywords:

camera-based person detection; near-infrared; NIR; industrial robots

Introduction

Within the working range of industrial robots, persons are exposed to the risk of severe injuries through bruises, collisions or various harms caused by moving parts of the robot or the end effector. A recent case in Germany [1], where a contractor was crushed to death setting up a robot at a VW motor plant, substantiates the importance of this issue and has brought it to public awareness.

The intrusion of persons into the hazardous area surrounding an industrial robot can have many causes, some of which might be conscious (e.g. collaboration or maintenance), while others might be unconscious (negligence, lack of knowledge, etc.). While unconscious intrusions can be prevented through separation by conventional guards like walls or fences, especially conscious intrusions need different approaches. SICK AG (Waldkirch, Germany) proposed a sophisticated solution, where a combination of laser light curtains and laser scanners is used to safeguard hazardous zones in a safe and reliable way. It separates a potentially hazardous zone into two different zones, allowing manual operations by a human in a less critical area of the hazardous zone [2]. However, fences, walls and light curtains are not flexible in their setup and require high effort to be adapted to an application change. Vision based protective devices (VBPD) using camera systems, such as the SafetyEYE by Pilz GmbH & Co. KG (Ostfildern, Germany), can be used for an image-based observation of hazardous zones. These systems detect the presence and three-dimensional position of foreign objects in this zone safely [3]. Safety zones can be defined via software and are therefore highly adaptable to any changed environment and application. Unfortunately, both of the above mentioned approaches lack the ability to reliably differentiate between humans and other types of objects.

Skin detection based on spectral signatures in the near-infrared spectrum introduces an intelligent way of muting and further enhances the detection performance of a safeguarding system. This technology has been researched at Bonn-Rhein-Sieg University of Applied Sciences (BRSU) for the past decade [4] and results have been presented at previous SIAS conferences [5,6,7]. In the context of ongoing research projects, this specific technology for skin detection is transferred from the use with reflection-responsive point sensors to an active camera system for both safety and security [8] applications. This work is part of the research project “Safe Person Detection in the Working Area of Industrial Robots” (SPAI), funded and accompanied by the German Social Accident Insurance (DGUV). It evaluates the potential of such camera systems for the implementation of a more intelligent muting process for non-collaborative industrial robots. Therefore, this paper describes the concept of integration and design of such a camera system into a VBPD according to current safety standards. The first objective is to adapt the camera system to cover a large area of observation necessary for the designated application. Other objectives are the evaluation of a mixed NIR/RGB stereo vision camera setup and the enhancement of person detection algorithms through reliable pixelwise skin detection. In future work, this system will be an important part of a multimodal safeguarding system for human-machine interaction.

Methods

Skin Detection Through Spectral Signatures

The technology of skin detection is based on the distinction of material surfaces by their spectral signature. A spectral signature is defined as the reflection intensity at well chosen, narrow and distinct wavebands suited in the near-infrared (NIR) spectrum. Figure 1 shows the reflection intensities of different material surfaces and six skin types after Fitzpatrick [9]. The skin types are united into a single skin corridor.

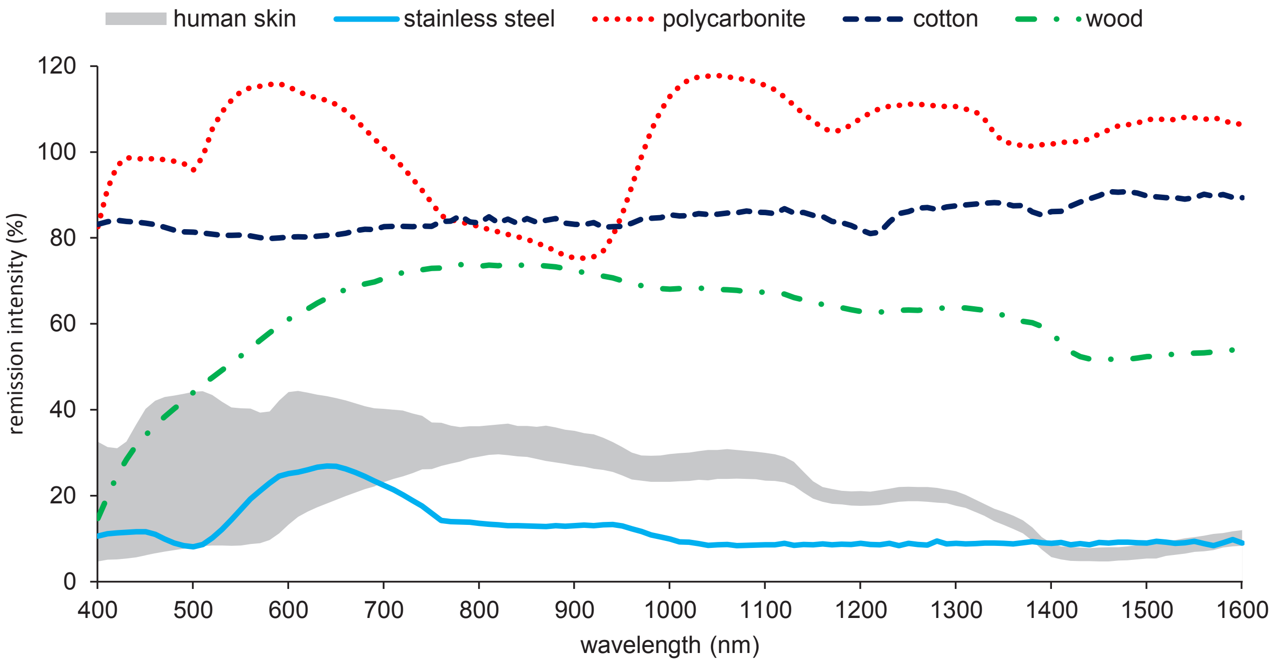


Figure 1: Reflection intensities of different materials and human skin in the visible and NIR spectrum, normalized to a diffuse white reference

Beside a better separability of skin and other materials compared to the visual spectrum, all skin types have a similar characteristic in the NIR spectrum: NIR radiation is primarily absorbed by water, which is a main component of human skin, whereas the melanin content does not have a notable influence in this spectrum. Another cause is the special scattering characteristic of skin: NIR radiation can penetrate some layers of the skin before it is scattered.

Research so far showed that skin and different materials can be distinguished using application-specific sample points of the spectrum, making it possible to realize this technology with convenient products like LEDs and photodiodes, instead of a broadband spectrographic analysis. The acquired signature is finally used as an input vector for a classification model based on simple thresholds combined with more sophisticated machine-learning based classifiers to distinguish between the two classes. This classification model can be implemented on typical microcontroller systems and performs well enough to achieve reaction times of $t = 1\ \mathrm{ms}$.

Active Near-Infrared Imaging

In order to transfer the technology described in the previous section to an imaging system, an active NIR camera system has been developed in previous work [8]. It consists of a special camera sensitive in the NIR spectrum, an LED-based ring light to emit the radiation and a controlling system in the form of an embedded system. Image processing and user interface are realized through application software. In this work, this camera system is modified and extended to fulfill the requirements of safety applications. Figure 2 shows a schematic illustration of the whole system. To satisfy the current safety standard of industrial robot operation DIN EN ISO 10218, the whole system has been designed to meet the requirements of category 3 with a Performance Level $PL_r = d$, both as defined by DIN EN ISO 13849.

To locate persons, the camera system needs to acquire depth data for each corresponding image. In project SPAI, a stereo vision setup has been chosen for this purpose. According to IEC/TS 61496-4-3 a Safety Integrity Level of $SIL = 3$, as defined by IEC 61508, is required. A stereo vision setup and the need for redundancy, demanded by a category 3 system, technically determine a system based on three camera systems, as depicted in Figure 2. To reduce the cost of such a VBPD, it would be beneficial to replace at least one of the NIR cameras with a convenient RGB camera. Therefore, stereo vision with RGB and NIR image sources has been investigated in the context of this work.

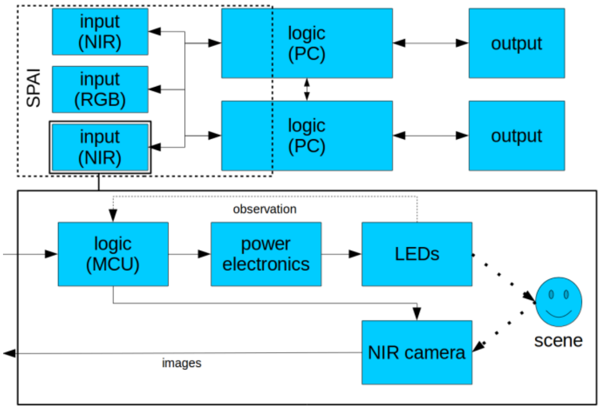


Figure 2: Schematic illustration of an active NIR camera system (bottom) as part of a category 3 VBPD (top); the dashed line indicates the topics covered in project SPAI.

Camera

Conventional camera systems use silicon-based image sensors for data acquisition in the visible range. The photo-sensitivity of silicon only covers a small part of the NIR range. Therefore, cameras based on alternative image sensors have to be used for NIR image acquisition for wavebands $\lambda > 1000\ \mathrm{nm}$. Those cameras use chips made from indium gallium arsenide (InGaAs) and are sensitive to radiation in the range $900\ \mathrm{nm}\ \leq \lambda \leq\ 1700\ \mathrm{nm}$. The current disadvantages of this technology compared to a state of the art camera system for the visual spectrum are its low resolution, high price and the need for active cooling to reduce the noise level. Another difference is the acquisition of distinct “color” channels. Most RGB cameras use an optical band-pass filter pattern, which is applied to the image sensor. This way, a specific color sensitivity can be selected for each pixel. For the commonly used Bayer-pattern, these colors are red, green and blue. A smart calculation method (“Demosaicing”) yields interpolated RGB values for each pixel. Optical band-pass filter patterns for the NIR spectrum, however, are currently still under development, but may be a promising alternative in the future. For now, this task has to be accomplished consecutively by systems based on filter wheels, which are comparatively slow [10] or active illumination [8] as described in the next section.

Ring Light & Controlling System

To acquire images in the relevant NIR wavebands, the whole scene is successively illuminated with radiation of each waveband. Therefore, the radiation sources for these channels on the ring light need to be separately controllable with fast rise and fall times, to minimize the switching overhead. LEDs have been selected for this task. An embedded system is used to activate the different NIR channels of the ring light and trigger the camera to synchronize the acquisition process. Beside this measurement coordination, the controlling system includes the power circuit to drive the LEDs.

The operation with an active light source demands the consideration of radiation safety to preserve the introduction of new risks to the working personnel through the VBPD. With respect to IEC/TS 61496-4-3, the used LEDs should meet the requirements of the exempt group, as defined by IEC 62471.

Preliminary Study

Our previous experiments concerning the separability of skin and workpieces by spectral signatures were based on measurements taken at single fingers or hands. Because of the aim to detect persons by means of their exposed body parts like face, arms and legs, more spectral measurements of those parts needed to be taken to substantiate the proposition. Also, with respect to former applications, some materials like clothes (especially work-clothes) have not been added to the existing database of spectral measurements yet. Hence, a measurement campaign has been carried out, capturing the spectral remission of defined spots on test persons including different skin regions and their clothes. Additionally, special regions like tattoos, pigment disorders and scars have been measured. A NIR spectrometer and a broadband light source have been used to acquire the data. In a second step, NIR images of all test persons have been taken to establish training data for the classification models used to differentiate between skin and other materials.

Person Detection

Person detection is crucial for the aim of project SPAI. Not only the presence and position, but also the silhouette of a person has to be recognized in a safe and reliable way. A first attempt based on convolutional neural networks (CNNs) as proposed by Farabet et al. [11] allows a pixelwise image segmentation, labeling every pixel with its estimated class. To support this method, a skin mask of every multispectral NIR image is calculated based on the classification model, indicating whether a pixel can be considered depicting skin or not [8]. NIR images and associated masks are then used as input data for the classification process.

Cross-Spectral Stereo Vision

To estimate depth-data for each pixel of the acquired image via stereo vision, the disparity between two projections of a single real-world point onto both image sensors has to be determined. Since the problem of finding corresponding points in different spectral ranges is not trivial, a cross-spectral method based on oriented gradient features as proposed by Pingera et al. [12] is used to solve this problem.

Results

Functional Demonstrator

Hardware

Based on the preliminary considerations, a functional demonstrator has been set up for evaluation and proof of feasibility. The system is based on a NIR camera with a frame rate of $f = 100\ \mathrm{FPS}$ and a resolution of $636 \times 585\ \mathrm{pixels}$. The active irradiation is realized by 32 high-power LED units (three different types) with a cumulated optical power of approximately $\phi_\Sigma \approx 6.5\ \mathrm{W}$. Each LED unit consists of 60 LED chips and is equipped with a lens to provide an aperture angle of $\omega = \pm 27°$. With this parts, the functional demonstrator provides an effective frame rate of $f_e = 25\ \mathrm{FPS}$ to acquire multispectral images. The controlling system, used to coordinate the measurement process, has been designed to satisfy the required performance level $PL_r = d$. Figure 3 shows a photo of the functional demonstrator. In addition to the NIR camera and High Power LEDs, the RGB camera used for stereo vision evaluation is depicted. A Microsoft Kinect sensor has been used for comparison.

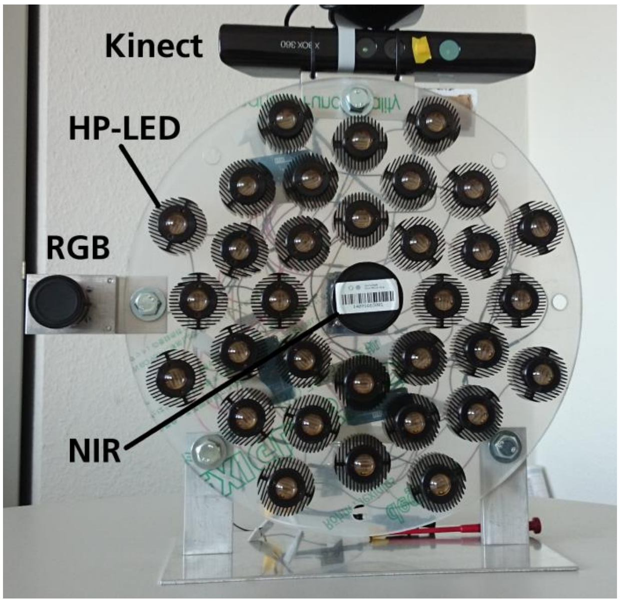


Figure 3: Functional demonstrator of the active NIR camera system

Figure 4 shows images of the same individual at three different distances, but with constant scale. This allows for first assumptions concerning the optical power and resolution of the camera system. At a distance of $d = 2{,}5\ \mathrm{m}$, an arm consists of many pixels, single fingers can be distinguished and the intensity of the skin color is sufficient. At $d = 5{,}5\ \mathrm{m}$, the skin tends to be a lot darker, but is still sufficiently bright to be classified reliably. An arm still consists of about three to five pixels, but single fingers can no longer be distinguished. Features relevant for face detection can no longer be resolved. With the step to $d = 7.5\ \mathrm{m}$ distance, image quality and, thus, detection reliability degrades even further.

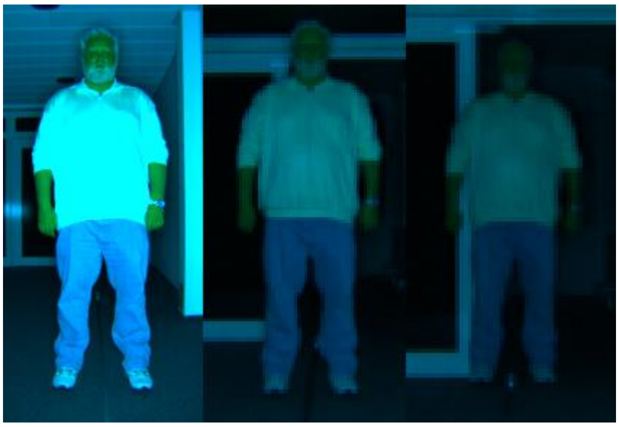


Figure 4: Comparison of the same individual from images acquired by the functional demonstrator at distances $D = \{2.5\ \mathrm{m}, 5.5\ \mathrm{m}, 7.5\ \mathrm{m}\}$ (from left)

Figure 5 shows two samples of depth data acquired by cross-spectral stereo vision with an additional RGB camera (right) and with the Microsoft Kinect system (left). The distance between camera and object is represented by the gray value of each pixel. The depth image of the Kinect system seems comprehensible, because a scene can be perceived by the viewer. In contrast to this, it is not possible to differentiate objects in the depth image acquired by cross-spectral stereo vision.

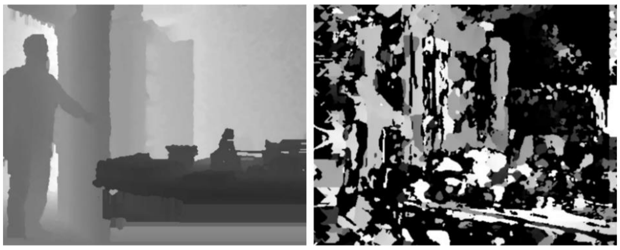


Figure 5: Depth images of the same scene acquired by Microsoft Kinect (left) and NIR/RGB stereo vision

Software

For the actual image fusion and analysis, a personal computer with corresponding application software is used. Providing a graphical user interface for the supervising user, the software is also used to configure and calibrate the whole system and start/stop the measurement and classification process. A live stream is supplied, which can be used to define and manipulate the safety zone in real time. The safety zone can be defined using geometrical primitives like rectangles and ellipses or through an arbitrary polygon. People entering this zone will cause a signal which can be used to stop all ongoing processes of the industrial robot and establish a safe state of the robots extremities. For demonstration purposes, the safety zone changes its overlaid color, as depicted in Figure 6. The definition and manipulation of a safety zone has been protected against tampering with authentication methods.

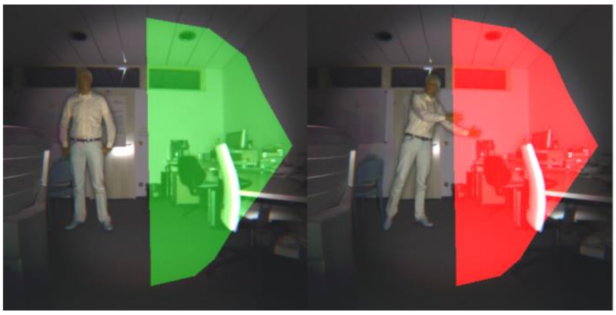


Figure 6: Screenshot of SPAI software without person in safety zone (left) and person penetrating safety zone

Preliminary Study

The similarity of different body parts to each other and to other materials has been analyzed with respect to the spectral data acquired during the measurement campaign. The similarity is measured by the Gower distance d_G, defined as

$$d_G = \sum_{k \in K} \frac{|x_{ik} - x_{jk}|}{r_k} \text{ with } i \in I\,, j \in J,$$

where K is the index set of used wavebands and I and J are the index sets of data samples of the two classes to compare. To determine the distance between the measurements of one class among themselves, $I = J$ is considered valid. The variable r_k denotes the statistical range of measurements in waveband k.

Figure 7 shows a boxplot of the Gower distances of selected skin region pairs. Compared to the distance between all captured material and skin samples, the distance among them is very small and it is safe to say that the different skin regions are much more similar to themselves than to other measured materials. Yet, this analysis does not represent the performance of a trained classifier, which is able to separate all skin samples from all material samples with an accuracy of 100% as shown in [8]. The setup of the camera system used in [8] differs slightly from the SPAI-related setup, but these results can be considered representative.

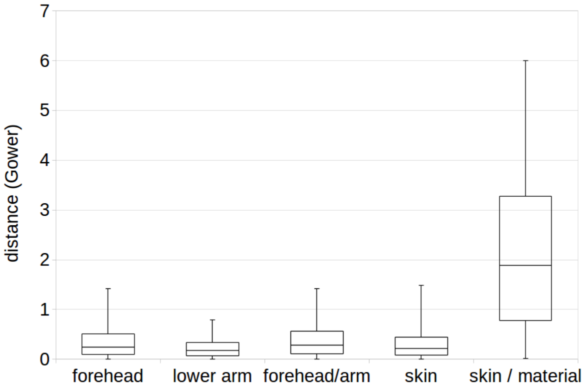


Figure 7: Boxplot of Gower distances between samples of different skin regions and materials

As another result of the preliminary study, the earlier mentioned similarity of different skin types can be visualized (see Figure 8). While there are significant differences in the RGB images, the color tone of each skin type looks very similar in the NIR images, except for barely noticeable variances. Another interesting observation can be made concerning the clothes: color patterns clearly visible in the visual spectrum are not visible in the NIR images.

Person Detection

To evaluate the influence of additional skin information on the person detection performance, classifier models were trained based on different training data sets. The experiments have been carried out within the scope of a master thesis [13] as a small subset of other experiments and configurations examined. While plain near-infrared image data will be denoted as "NIR", the data set with added depth information is called "DNIR". The training set including additional binary skin data images is named "DNIRS" accordingly. The classifiers were trained to distinguish between the three classes "person", "object" and "background" with a 5-fold cross validation and a training set containing 89 scenes and the corresponding NIR, depth and skin images. The images have been labeled manually to determine ground truth data for the supervised learning. The models are compared by their Pixel Accuracy (PA) and Class Accuracy (CA).

$$PA = \frac{\text{amount of correctly classified pixels}}{\text{total number of labeled pixels}}$$

$$CA = \frac{\text{amount of true positive pixels for this class}}{\text{total number of pixels labeled with this class}}$$

The results are shown in Table 1. In case of the person detection, the accuracy could be improved by approximately 53.3%.

Table 1: Accuracies of CNN classifiers using different training data sets

Used training data	PA (%)	CA (%) person	CA (%) object	CA (%) back-ground
NIR	61.8	12.3	66.9	63.7
DNIR	66.6	22.5	69.5	69.8
DNIRS	70.6	65.6	71.1	70.9

Discussion

The functional demonstrator proves the feasibility of an active NIR camera system to observe hazardous areas. While the optical output power and aperture angle of the ring light could be improved by more LEDs and different lenses, currently available InGaAs camera systems have a higher impact on the performance limit of such a system. Ongoing development will probably postpone this limit in the future, especially concerning resolution and frame rate, the latter through integration of waveband filter arrays directly onto the sensor. The method used to acquire depth data via cross-spectral stereo vision did not perform well due to many stereo mismatches resulting in erroneous values. This mode of operation is therefore not sufficient to acquire reliable depth data, and a second NIR camera is needed to solve this task with a binocular approach.

The preliminary study revealed the assumed spectral similarity between different skin regions. A simple classifier based on thresholds is capable of a nearly perfect distinction between materials and skin samples of all measured regions including tattoos, pigment disorders and scars, which are interpreted as skin [8]. More sophisticated classification models, like a Support Vector Machine (SVM), are able to distinguish even between skin and skin-like materials used to create artificial features for deliberate deception in biometrical applications [8].

The detection rate of persons has been enhanced by depth and skin information. If regions of skin are exposed to the camera system, the skin map can be used as a very exclusive information on the presence of persons. A classifier using this information has a natural benefit over those models which do not. Additionally the depth information provides a boost to classifier performance. Unfortunately, the person detection performance of the CNN classifier does not fulfill the requirements of a safe and reliable detection with $CA = 65.6\%$. For this purpose, an accuracy very close to 100% has to be achieved. This improvement could probably be realized with the combination of pixelwise skin detection and dedicated person and limb detection algorithms, which use pattern-based strategies and/or foreground-background segmentation algorithms.

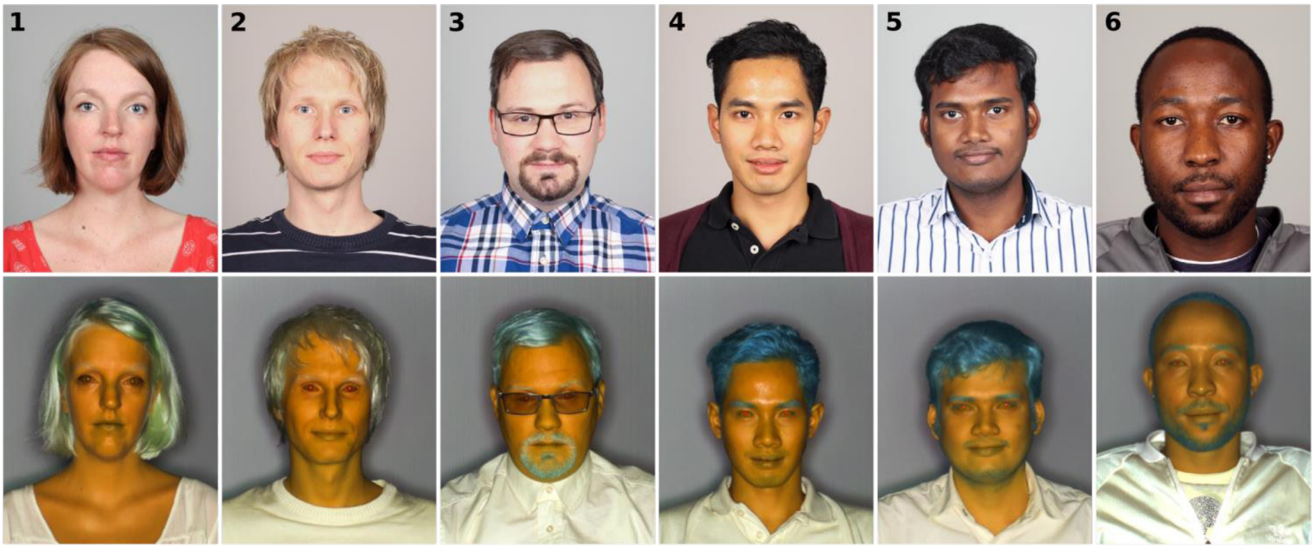


Figure 8: RGB and NIR portraits of individuals from skin type 1 to 6 according to Fitzpatrick [9] (taken from [8])

Conclusion

It could be shown, that the safe and reliable pixelwise skin detection, which has been evaluated in prior research [8], enhances the performance of the selected person detection process. Acquiring distance data for a three-dimensional location through stereo vision with a mixed NIR/RGB camera setup is not profitable and makes the usage of a second NIR camera inevitable. Software-configurable safety zones can be monitored for intrusion of persons, which will cause a safety related alarm signal. Other objects, like workpieces, are recognized and do not cause this signal. In conclusion, the proposed method is a promising new approach to reduce the risks of persons in the working range of industrial robots.

In future work, the practical use of this system will be evaluated through different field studies involving scenes with generic robots and defined experiments to test the system and find possible weak spots and problems. Crucial parts of the system (like resolution and radiation power) have to be optimized and do partly depend on the advances in NIR camera development. Hence, a follow-up project was acquired to deepen the research and expand the safeguarding system to a multimodal approach including a concrete interface to industrial robots. For this new project, strong partners like K. A. Schmersal GmbH & Co. KG (Wuppertal, Germany), the Institute for Occupational Safety and Health of the German Social Accident Insurance (Sankt Augustin, Germany), the Cologne University of Applied Sciences and the University of Siegen have been gathered as a team to design and evaluate such a multimodal sensor system for future applications of (especially) collaborating robots in the context of Industry 4.0. The project is called “beyondSPAI”.

References

[1] M. A. Johnson. (2015, Jul. 1). *Robot Crushes Contractor to Death at VW Motor Plant in Germany* [Online]. Available: http://nbcnews.to/1GPd8dn

[2] SICK AG, “Safety device used in dangerous work area has upper and lower securing systems that generate signals used in determining position of object within dangerous work area,” DE 202004020863 U1, Apr. 6, 2006.

[3] C. Woehler *et al.*, “Method and device for making a hazardous area safe,” WO 2004029502 A1, Apr. 8, 2004.

[4] O. Schwaneberg, “Concept, System Design, Evaluation and Safety Requirements for a Multispectral Sensor,” Ph.D. dissertation, Univ. Siegen, Siegen, DE, 2013.

[5] N. Jung *et al.*, “Field Study Results of a skin detecting Safety Sensor on Circular Saws,” in *Proc. 6th Int. Conf. Safety of Industrial Automated Systems (SIAS)*, Tampere, FI, 2010.

[6] O. Schwaneberg *et al.*, “Push-buttons with Material Classification based on Spectral Signatures,” in *Proc. 6th Int. Conf. Safety of Industrial Automated Systems (SIAS)*, Tampere, FI, 2010.

[7] H. Steiner *et al.*, “Spectral Light Curtains – Novel Near-Infrared Sensor System for Production Machines,” in *Proc. 7th Int. Conf. Safety of Industrial Automated Systems (SIAS)*, Montreal, CA, 2012.

[8] H. Steiner *et al.*, “Design of an Active Multispectral SWIR Camera System for Skin Detection and Face Verification,” *Journal of Sensors*, Article ID 456368, to be published.

[9] T. B. Fitzpatrick, “The validity and practicality of sun-reactive skin types I through VI,” Arch. Dermatol., vol. 124, no. 6, pp. 869-871, Jun. 1988.

[10] T. Bourlai *et al.*, “On designing a SWIR multi-wavelength facial-based acquisition system,” in *Proc. SPIE 8353, Infrared Technology and Applications XXXVIII*, Baltimore, US, 2012.

[11] C. Farabet *et al.*, “Learning Hierarchical Features for Scene Labeling,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 8, pp. 1915-1929, 2013.

[12] P. Pinggera *et al.*, “On cross-spectral stereo matching using dense gradient features,” in *Proc. 23rd British Machine Vision Conf.*, Surrey, UK, 2012.

[13] M. Velte, “Semantic Image Segmentation Combining Visible and Near-Infrared Channels with Depth Information,” Master’s thesis, Dept. Comput. Sci., Bonn-Rhein-Sieg Univ. Appl. Sci., Sankt Augustin, DE, 2015.

Corresponding address

Bonn-Rhein-Sieg University of Applied Sciences
Safety and Security Research Institute
Grantham-Allee 20
53757 Sankt Augustin (Germany)

Phone: +49 2241 865 456
Fax: +49 2241 865 8456
E-Mail: sebastian.sporrer@h-brs.de

Real Time Location Systems for monitoring safety of the machine operators

Marek Dzwiarek[a]

[a] *Central Institute for Labour Protection – National Research Institute, Poland*

Abstract

The RTLS UWB approach has become more and more commonly applied in intelligent manufacturing systems to improve both the work organization and product quality. Upon analysis of the accidents happened one can state that there still exists a need for improving the safety means making use of capabilities of advanced technologies. However, the locating technique cannot protect effectively particular body parts, it may be useful when the need appears for the whole body to penetrate the dangerous zone or the machine operator has no possibility to observe all dangerous zones in the machine. The application of localization systems to start interlocking, access control as well as to the information and warning means can bring about substantial reduction in number of accidents happened in manufacturing industry. At the same time, the systems used in the aforementioned applications should satisfy additional requirements resulting from the safety function performance. There is a lack of standards covering the RTLS systems, therefore when assessing such a system one should apply EN 61496-1 standard.

Keywords:

Real Time Locating System; Safety of Machinery

Introduction

The progress of technology is accompanied by new, ever improving machinery. The development of information processing and telecommunications technologies in particular enables the creation of “smart” manufacturing systems. These systems significantly reduce human participation in the manufacturing process through the automation of the entire process. The processing power of these systems is used mainly to monitor the manufacturing process. They are becoming increasingly used to monitor the safety of system operators. This also increases the safety level during operation of machinery. Yet accidents still sometimes happen when operating machinery. According to the Chief Statistical Office data [1] in 2013 there were over 60 thousand accidents, including 60 fatal accidents, and 240 serious incidents in the industrial processing sector, so mainly during the operation of machinery. According to the National Labour Inspection [2], over 11% of these cases had technical causes, and in particular:

- incorrect selection or bad technical condition of protective devices or lack thereof,
- incorrect signalling of hazards or lack thereof.

This indicates the significance of the development of machinery protection systems. This also applies to the use of the possibilities offered by the most modern IT and telecommunications systems.

Real-Time Locating Systems (RTLS) technologies are among the technologies which are currently developing most rapidly. Among these the use of Ultra-Wide Band (UWB) radio signals is developing particularly quickly. This technology is also becoming widely used in smart manufacturing systems. The newly developed UWB applications were the basis for studies on the possibility of using this technology for ensuring the safety of machinery.

RTLS systems operation principle

The RTLS systems use very varied location systems. Some examples include:

- Active radio-frequency identification (Active RFID),
- Infrared radiation (IR),
- optical location,
- low-frequency identification,
- passive RFID systems,
- ultrasound Identification US-ID,
- ultrasonic ranging US-RTLS.

UWB is a developing wireless communication technology, characterised by high data transmission rates (up to 2 Gb/s) at small distances (range of tens of meters). UWB works at low power levels, thus eliminating interference with other radio communication systems and providing for the construction of devices with low energy consumption.

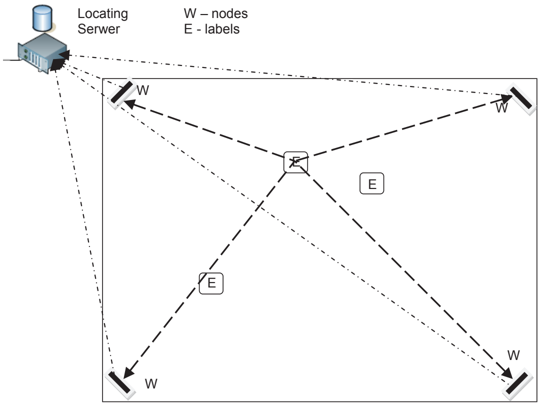


Figure 1: TDOA locating technic

The system works in the 3.1–4.85 GHz and 6.2–9.7 GHz (Direct Spread UWB) or 3.1–10.6 GHz (Multi Band OFDM) bands. The UWB RTLS system includes labels (receiving and transmitting devices), stationary nodes and a location server (fig. 1). The label is located using TDOA technique (Time Difference of Arrival), that is based on the difference it takes the signal to arrive from the label to individual nodes and on the coordinates of the nodes [3]. The use of multiple nodes enables three-dimensional location.

Examples of RTLS UWB system use

The scope of RTLS UWB system use is very wide ([4] and [5]). It includes, among others:

- locating and studying the movement of employees at work, of personnel and clients in shops,
- locating equipment, studying the ways it is used,
- controlling the movement of goods, including hazardous goods,
- analysing goods and client flows,
- locating emergency response workers during rescue operations.

In an UWB technology based systems items may be located with an accuracy of less than twenty centimetres. Emissions of such devices are at a low level, which enables their use also in the frequency ranges which are assigned to other uses of the spectrum. The UWB wide emission band makes them very resistant to interference caused by other narrow-band systems. Relatively simple design of the devices enables their miniaturisation, and low power demand enables them to operate for many months or even many years without the need to replace batteries.

An example use of the system when operating machinery is the monitoring of a car assembly line. A 1.7 km long line includes over 150 assembly stations. At every station the car's elements are being assembled using mechanical tools, e.g. air wrenches. Each tool is equipped with an UWB label. Also the body of each assembled car is equipped with a label. The entire line is monitored by a network of UWB sensors. Effectively the location of over 1000 labels is being monitored. Locating of the labels placed on the car body is intended to monitor the progress of assembly works. The tools are being monitored in order to establish their location in relation to the car body. When the location system establishes that there is an attempt to use a tool at a location where it should not be used, the tool control system is notified and prevents the operation of the tool. This prevents human errors in the assembly process through the use of incorrect tools.

Another example is the use of the location system in aeroplane component manufacturing plants. In this case individual aeroplane parts (fuselage, wings, fuel tanks etc.) are manufactured in various plants all over Europe, and then final assembly is performed in the manufacturing centre. In order to effectively and quickly respond to the orders placed by clients it is necessary that the central manufacturing plant possesses the most current information on the progression of manufacture of individual component parts. The data on the location of parts in the hangars of individual manufacturing plants are collected at the manufacturing centre. This eliminates the delays in the collection of data on the current stage of works and enables promptly responding to the clients' needs.

Another use is the location system installed in one of the steel foundries. In this case a problem of locating casting containers and establishing their contents had to be solved. This application combined the advantages of an UWB location system with an RFID identification system. The UWB system was used for the location of forklifts in the warehouse. All the products were equipped with RFDI labels, which contained information about their identification and weight. This reduced the time necessary to find the required element by a forklift available at the time.

Another example of safety-related applications is a chemical processing plant. It requires the presence of employees near toxic chemical waste dumps. There are significant hazards related to the possibility of toxic vapours accumulating in a restricted space, and with an explosion or fire hazard. In this case it is necessary to immediately organise evacuation of all people at risk. This is made possible by continuous monitoring of their location within the area of the dump.

A similar situation occurs in one of nuclear power plants. In this case the hazard is radioactive radiation within the power plant area. All employees were equipped with dosemeters with WFI system and UWB labels. The dosemeters provide information on radiation intensity, and the location system enables establishing how long the employee was present within hazardous conditions. Thus continuous establishing of the radiation dose is possible. This enables correct organisation of work, so as to ensure that none of the employees exceeds allowable radiation exposure limit values.

The presented selected uses of location systems show their potential in the creation of modern industrial systems. These examples demonstrate uses which are oriented mainly on the quality and size of manufacturing, but they also contain first attempts to use the systems for work safety. So far no reports were made on the use of RTLS systems for machinery safety. The detection of entering a hazardous zone is currently performed by such protective devices as light curtains and beams, laser scanners and pressure sensitive devices. These devices do not monitor the location of the employee. UWB technology based systems may provide an alternative to these devices, enabling the monitoring of employee location at any moment, not only when entering a hazardous zone of the machinery. The demonstrated uses of UWB in smart systems allow formulating an assumption that in the nearest future the use of UWB for reducing risk in the operation of machinery may be expected.

Analysis of machinery related acidents and the preventive use of UWB RTLS

The main source of information concerning the possibility of using protective measure is always information about accidents that have already occurred. In our case the analysis of these events was conducted in order to indicate when the use of an employee location system could prevent an accident. The analysis used data from the manufacturing industry accidents database provided by the National Labour Inspection. These data concerned incidents which occurred in 2012 and 2013 in the manufacturing processing section. For these accidents a detailed analysis of their descriptions was performed. The analysis was intended to indicate cases which could have been prevented through the use of employee location systems. Since the systems enable the location of an entire human body and not its parts, accidents where the victim was in the vicinity of moving elements during normal operation of the machinery were discarded. For further analysis only cases related to the presence of the victim within the area where he or she should not be present when the hazardous parts of the machinery are moving were left. Then the course and causes of these incidents were carefully analysed. It turned out that these cases were related to the following events:

- automatic start of machinery when an employee was present within the hazard zone,
- operator starting the machinery when an employee was present within the hazard zone,
- being hit by a forklift.

The conducted analysis showed that machinery where an accident had occurred was a part of larger manufacturing systems, e.g. automated manufacturing lines. In each of these cases insufficient protective devices were used or procedures were not followed. The use of a location system as an additional protection system, e.g. for blocking the automatic movement of a hazardous move or notifying the machinery operator when employees are present within the hazard zone, could have prevented these accidents. The conducted analysis indicated that when establishing whether a location system should be used to protect the operator, the following operating stations should be considered primarily:

- automated manufacturing system operators,
- operators of machinery where not all hazard zones are visible,
- assembly workers operating on assembly lines,
- forklift operators.

Conclusion

The main principles for the use of protective devices for machinery lead to the following conclusions [6]:

- an accident may occur only when someone or a body part enters the hazard zone,
- such situation is possible when the zones available to an operator reach the hazard zones,
- the machinery designer should make use of all available resources to ensure that no areas common to both hazardous zones and available zones are present in the machinery.

The division of zones available to the operator from the hazardous zones may be performed in two ways:

- removing the zone available to the operator from the hazard zone (barriers, enclosures, walls, nets, doors etc.),
- removing the hazard zone from the zone available to the operator when the operator is present there (protective devices which detect the presence of a human body part in order to execute a safety function consisting in an emergency stop of the dangerous movement).

In state of the art systems sensor devices are being increasingly used to implement the safety function. They are devices which detect the presence of sensors and, as a result, of items on which the sensors are installed [7]. The RTLS system is an example of such device ([3] and [8]). In particular the analysis of accidents which occurred in the 2012 and 2013 have confirmed that there is still a need to improve safety measures using the possibilities offered by state of the art technologies. Although the location technology will not be useful for protection of human body parts, but the cases of selected accidents show it may be very useful when it is necessary for an entire human to enter the hazardous zone. This applies to workstations where:

- during manufacturing operations the operator requires whole body access to the hazardous zone,
- access to hazardous zones is necessary only in case of activities which are not directly related to manufacturing, such as adjustments, repairs, cleaning etc.
- the operator of machinery is not able to see all the hazardous zones of the machinery.

Examples of such workstations include operating stations for:

- automated manufacturing systems,
- large size assembly lines,
- large size machine tools,
- long transport lines,
- transport forklifts.

The use of location systems for halting machinery start, for access control and for notifying and warning about the presence of persons within hazard zones may result in a reduction of the number of accidents in the manufacturing industry. At the same time, the systems used for such purposes should meet additional requirements resulting from the performance of safety functions. Since currently there are no standards concerning the application of RTLS systems, when assessing them the PN EN 61496-1 [9] standard should be applied.

Acknowledgment

This paper has been prepared basing on the results obtained from a research task carried out within the scope of third stage of the National Programme “Improvement of safety and working conditions” partly supported in 2014-2016 – within the scope of state services - by the Ministry of Labour and Social Policy. The Central Institute for Labour Protection – National Research Institute acts as the main co-ordinator of the Programme.

References

[1] Chief Statistical Office. Statistical Yearbook of Industry 2014. http://stat.gov.pl/en/topics/statistical-yearbooks/statistical-yearbooks/statistical-yearbook-of-industry-2014,5,8.html

[2] National Labour Inspection. Annual Report of 2013. http://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAAahUKEwjFkdXUvIDIAhWkwHIKHbIeDLE&url=http%3A%2F%2Fwww.pip.gov.pl%2Fpl%2Ff%2Fv%2F100996%2Fsprawozdanie2013.pdf&usg=AFQjCNFsY1UgnfMDrJNt-olwqdK6CrOaxQ&bvm=bv.102829193,d.bGQ

[3] Gomez, J., Tayebi, A., del Corte, A., Gutierrez, O., Gomez, JM., de Adana, FS. A Comparative Study of Localization Methods in Indoor Environments. Wireless Personal Communications 72/4, 2013; 2931-2944

[4] Hirt, W. Ultra-wideband radio technology: overview and future Research. Computer Communications 26/2003; 46–52.

[5] Ultra-Wideband Radio Technologies for Communications, Localization and Sensor Applications. Reiner T. Reinhard H., Jürgen Sachs J, Ingolf W. and Thomas Zwick, editors. InTech 2013.

[6] Dźwiarek, M. Basic Principles for Protective Equipment Application. In: Handbook of Occupational Safety and Health Koradecka, D., (ed.) © CRC Press, Taylor & Francis Group, LCC, 2010; 579-592.

[7] Seppa, H. The future of sensor networks. VTT Impulse, 2012; p. 20-27.

[8] Guyoun, H. Dongkyoo, S. Dongil, S. et al. Design and Implementation of the Ubiquitous Sensor Network-Based Monitoring System Using RTLS (Real-Time Location System). Sensor Letters 11/9, 2013; 1721-1725.

[9] EN 61496-1:2013 Safety of machinery - Electro-sensitive protective equipment - Part 1: General requirements and tests

Corresponding address

Marek Dzwiarek, Central Institute for Labour Protection – National Research Institute. Czerniakowska 16 str. 00-701 Warsaw, POLAND. e-mail: masdzaw@ciop.pl.

Adaptive, material-dependent height-control for protective hoods on panel saws

Norbert Jung[a], Oliver Schwaneberg[b], Sebastian Sporrer[a], Holger Steiner[a], Iris Groß[a], Tobias Scheer[a]

[a] Bonn-Rhein-Sieg University of Applied Sciences, Sankt Augustin, Germany
[b] Tippkemper-Matrix GmbH, Overath-Marialinden, Germany

Abstract

The proper use of protective hoods on panel saws should reliably prevent severe injuries from (hand) contact with the blade or material kickbacks. It also should minimize long-term lung damages from fine-particle pollution. To achieve both purposes the hood must be adjusted properly by the operator for each workpiece to fit its height. After a work process is finished, the hood must be lowered down completely to the bench. Unfortunately, in practice the protective hood is fixed at a high position for most of the work time and herein loses its safety features. A system for an automatic height adjustment of the hood would increase comfort and safety. If the system can distinguish between workpieces and skin reliably, it furthermore will reduce occupational hazards for panel saw users. A functional demonstrator of such a system has been designed and implemented to show the feasibility of this approach. A specific optical sensor system is used to observe a point on the extended cut axis in front of the blade. The sensor determines the surface material reliably and measures the distance to the workpiece surface simultaneously. If the distance changes because of a workpiece fed to the machine, the control unit will set the motor-adjusted hood to the correct height. If the sensor detects skin, the hood will not be moved. In addition a camera observes the area under the hood. If there are no workpieces or offcuts left under the hood, it will be lowered back to the default position.

Keywords:

bench and sliding table saws; optical safeguard sensor; skin detection; protective hood; automatic height adjustment; safety concept for machinery

Introduction

In previous contributions we have presented our research results on NIR sensors utilizing a reliable skin detection method for safety application by means of the spectral signature of the surface materials [1-3].

In a number of research projects the feasibility of the concept was examined and prototype designs of such sensor systems for different applications were developed.

In this paper we present a dedicated version of the sensor system in an automatic height-adjustable protective hood for bench and sliding table saws.

The approach now covers not only the sensory part of a safety application but a complete protective subsystem.

For this purpose, the sensor is used simultaneously for the contactless surface material classification and the distance measurements to the actual height of the workpiece.

The automatic height adjustment of the protective hood is only unlocked by the safety sensor if regular workpiece materials are fed to the front of the protective hood. If human skin is detected in front of the saw blade, the hood position is not changed and further safety measures could be initialized, like an emergency stop.

In a comparison of the presented concept to previously existing protection devices it is intended to show the benefits in terms of risk mitigation and ergonomics for the operation of table and sliding table saws.

The investigation is based on the examination of the typical operations of the saws. From these considerations it is estimated which application scenarios the system might be confronted with. Based on these scenarios, different designs for sensors and actuators are investigated, which then lead to the assessment with regard to the feasibility and risk mitigation of the overall system.

Analysis of the remaining safety risks by using a manually height-adjustable protective hood

According to the applicable standards the protective hood should prevent all hand injuries. In fact, wrong use still causes a large number of accidents. Wrong height adjustment of the hood can be considered as a mayor cause for accidents, because hands or fingers may reach the rotating saw blade and possible material kickbacks could harm the operator. Further it should be mentioned that wrong height adjustments of the protective hood can lead to an insufficient performance of the dust extraction system resulting in fine-particle pollution at the workplace.

The following assumptions have been made for the operation of the saws:

- The machine is not switched off after each cut, and usually runs for a longer period of time.
- The person using the saw wears no or special gloves
- Leftovers from the cutting are not removed immediately after a cut e.g. before a further cutting on the same workpiece.

Resulting hazard risks with manual height adjustment of the protective hood:

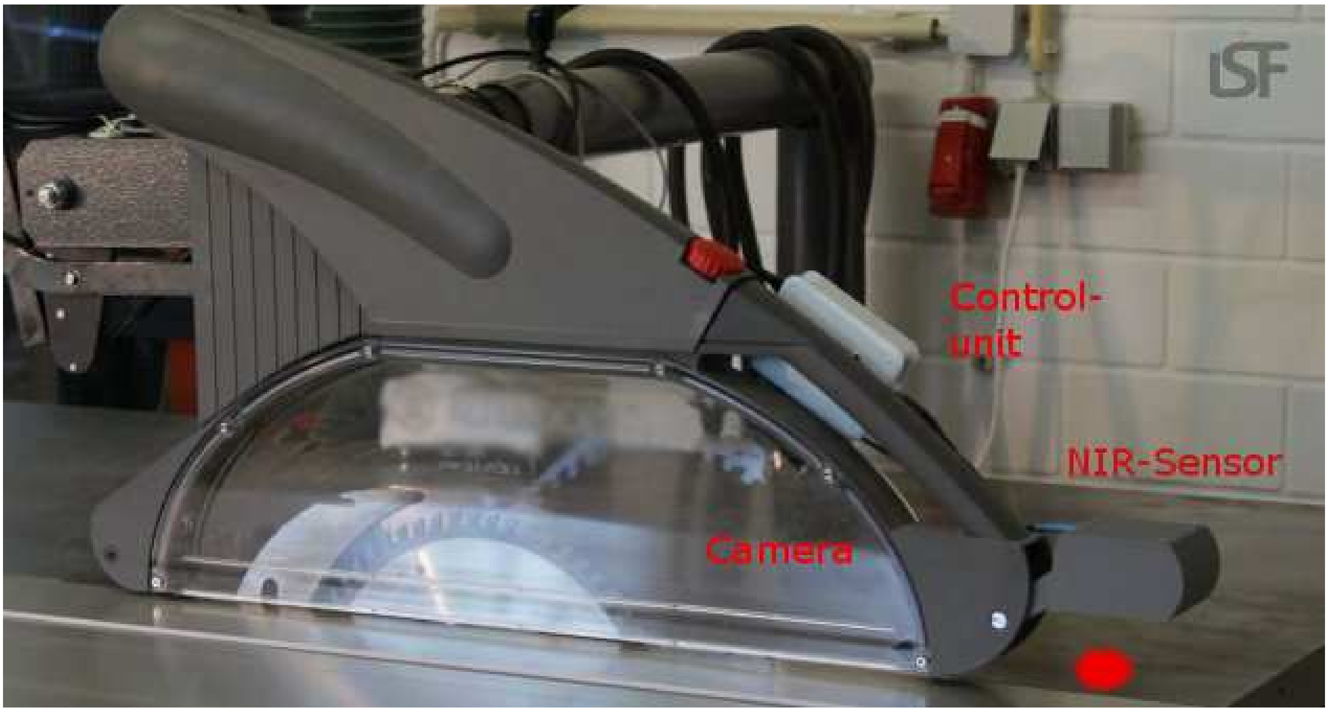


Figure 1: Functional demonstrator of the Smart Hover system

1. Any position higher than the required minimum with respect to the workpiece height might allow touching the saw blade due to a large aperture between the hood and the workpiece. This counts for the material feeding direction as well as from the sides or from the rear side.
2. The hood might remain in the adjusted position after the sawing operation and is not lowered down to the table.
3. Even after a correct manual adjustment of the protective hood for a workpiece a required new adjustment for the next (thinner) workpiece can be forgotten.
4. The protective hood may be locked at the highest possible position and is therefore losing the accident protection function, resulting in a maximum accident risk.

Considered applications:

- Longitudinal and cross cuts: significant accident risk for narrow workpieces
- Concealed cuts: e.g. grooves, rebating
- Cutting wedges: workpiece surface not parallel to lower edge of the hood; material thickness changing during the cutting.

Considered scenarios:

1. Workpieces have a plain top edge parallel to the lower edge of the protective hood; this is the simplest case
2. Workpieces have a top edge not parallel to the respective edge of the protective hood; for the cutting of such a workpiece the correct height determination must be guaranteed. Without additional degrees of freedom to the hood adjustment mechanisms, this means that the hood must be adjusted to the workpiece's highest point within the width of the hood.
3. The protective hood can be lowered after the sawing operation down to the table. Neither relevant cutting aids, yet leftovers from the cut are in the descent area. Workpiece and sections are immediately removed after cutting.
4. Beside the workpiece itself, other objects might be in the descent area. These include relevant cutting aids, as well as remnants that were not removed from previous work. The hood cannot be fully lowered onto the table after the cutting operation.

Comparison to other existing systems

In research projects, e.g. at the Bonn-Rhein-Sieg University, different approaches to sensory monitoring of hazardous areas of manually fed machines were examined. E.g. in the earlier project LBIS [9] a sliding table saw has been equipped with a fast protective shutter inside the protective hood. This approach is also based on the assumption that the height of the hood is not set correctly.

The approach of the automatic height adjustment of the hood in principle is superior, because the saw blade will be kept covered by the hood as much as possible. Furthermore, with a correctly set hood the risk of injury by workpiece kickback is reduced and the effectiveness of the dust extraction system is ensured.

As a relevant commercial example the American company SawStop offers (small) table saws with an integrated protective device. The protective device consists of a capacitive sensor, which is coupled to the saw blade. The sensor can only detect direct contact between skin and blade. At this point, a serious injury may occur within a few milliseconds. Therefore, a very fast reaction is required. SawStop designed a stopping mechanism build of an aluminum wedge, which is directly shot into the running blade. The teeth of the saw blade are wedged in the aluminum and the saw is brought to a standstill within a half-turn. In this case, the absorbed kinetic energy further is used for rapidly lowering the saw blade below the table. Afterwards, the saw blade and the stop mechanism have to be replaced. SawStop offers no large sliding table saws, but the Italian manufacturer Griggio s.p.a. recently presented their UNICA SAFE concept at LIGNA 2015 fair. Unlike the original SawStop machine, the company Griggio claims that a saw blade with a diameter of up to $d_{\varnothing} = 400\ \mathrm{mm}$ at a speed of up to $n = 6000\ \mathrm{rpm}$ is stopped and lowered within $t = 5\ \mathrm{ms}$ without being damaging. Afterwards the saw is again ready to be used without further service. This is a great technological progress, but it is still a radical safety measure at the last moment and it can be assumed that the mechanism puts a great stress on the machine mechanics.

System concept

Setup

The safety system presented here is based on a regular protection hood according to EN 1870-1:2009 [4]. The hood is supplemented by

- an optical sensor pointing onto the extended cutting axis in front of the saw blade. It is able to measure the distance to the workpiece surface and can classify the surface material.
- a compact camera with an embedded image recognition system below the protecting hood. It allows to detect remaining pieces that might block the lowering of the hood down to the table.
- a motorized mechanic to move the protective hood up and down precisely.
- a collision detection and force limitation for the motor moving the protective hood.
- a control unit to coordinate the whole system. This includes a simple image processing and the communication between all mentioned subsystems.

The setup of the functional demonstrator is depicted in Figure 1.

Behavior and functionality

The behavior is derived from the scenarios mentioned above. In addition to the requirements of the default behavior of the scenarios 1 & 3, the scenarios 2 & 4 require a collision detection of the hood when lowering. An optional manual mode might be necessary in scenario 2, since a correct determination of the highest point over the entire cutting edge might not always be guaranteed – e.g. for the handling of wedges.

Before starting the machine it has to be assured that the hood is lowered down on the table i.e. the lowest possible position. Only then the start of the saw blade rotation is released by the control unit.

The lowest position of the protective hood might not be reached, when an obstacle on the table is detected. This exception should be handled by the collision detection at the lower edge of the hood.

When the saw is turned on and a workpiece is fed in front of the saw blade, the hood is always adjusted to the highest recorded point of the workpiece plus $2\ \mathrm{mm} \leq d_{\mathrm{gap}} \leq 4\ \mathrm{mm}$. This gap is required to guarantee optimal airflow and as mechanical tolerance to prevent contact between the hood and the workpiece.

The height of the protective hood is not increased if human skin is detected by the sensor. In case a workpiece is located under the hood, the slit between the workpiece surface and the lower edge of the protective hood must be too narrow for a finger to fit through and reach the saw blade.

In case the hand follows behind a workpiece in direction to the cutting edge, the saw blade rotation can be turned off automatically as soon as skin is detected in front of the protective hood.

In this situation, the penetration of hands into the region under the protective hood might not be effectively prevented, but it takes some time until the fingers could reach the saw blade, so that a normal rotation stop can be fast enough to prevent an injury.

As soon as no more saw work is detected by the camera system, the hood is lowered at a low speed after a defined waiting time. If an obstacle is detected during the lowering, the hood moves up about d_{gap} and remains in this position. It is periodically checked whether a further lowering of the hood becomes possible because the obstacles have been removed.

Required sensor properties

Concepts that use a fast shutter or a fast brake for the blade, require a very fast sensor and in particular an actuator with reaction times in the millisecond range.

The concept presented here allows very relaxed reaction times because, for most scenarios, the correctly adjusted hood prevents that fingers or the entire hand can enter the dangerous area around the rotating saw blade.

The four different types of sensors mentioned above need the following properties to implement the concept:

1. The reliable differentiation between skin and workpieces: using the NIR range (near-infrared wavelength $900\ \mathrm{nm} \leq \lambda \leq 1600\ \mathrm{nm}$) allows contactless skin detection independent from skin type, temperature and ambient light.
2. The precise distance measurement to the workpiece surface by means of triangulation with the same sensor.
3. The collision detection at the lower edge of the hood can be implemented by a force - or a current measurement at the motor for the height adjustment of the hood.
4. The recognition of parts under the hood can be implemented by means of a simple and compact camera mounted under the hood with a control unit e.g. a compact embedded system with low power dissipation

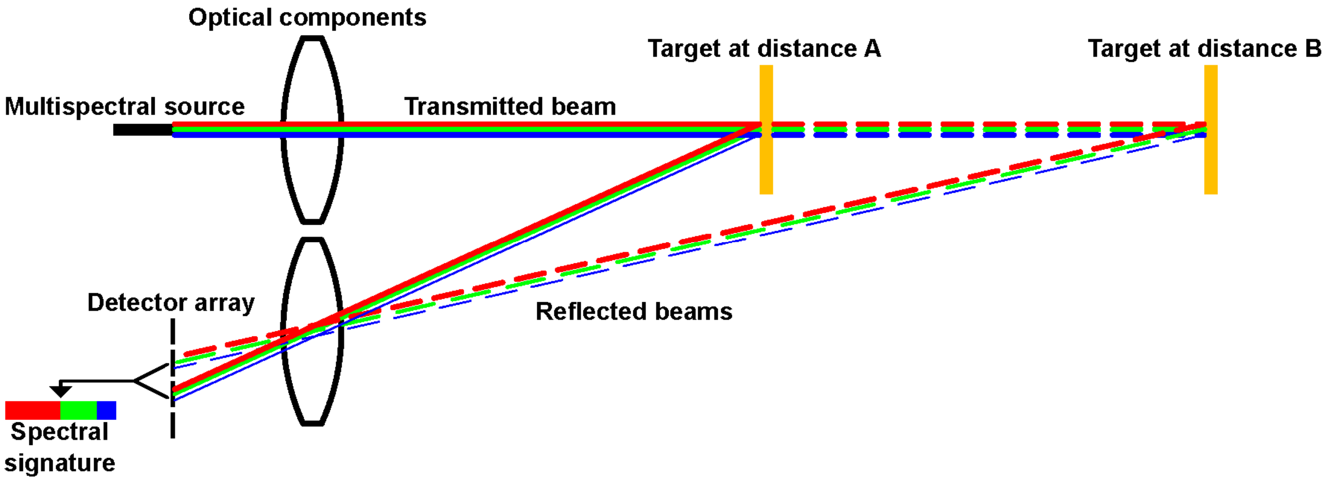


Figure 2: Schematic illustration of the NIR sensor principle [3]

The front roller of the standard hood is replaced by the combined skin detection and distance measurement NIR sensor. The sensor is installed in a way so that the monitored area lies in line with the saw blade. Further, the sensor should be attached above the lower edge of the protective hood in a defined height and inclination. A measurement spot at a distance of $30\ \mathrm{mm} \leq d_{\mathrm{spot}} \leq 70\ \mathrm{mm}$ is monitored in front of the protective hood on the height of the lower edge of the protective hood. This distance will be referred to as a detection distance, and is required in order to give a sufficient reaction time of the mechanical system.

The simple camera system monitors the area under the protective hood with respect to workpieces and tools by means of known image processing algorithms.

Optionally, e.g. a capacitive sensor system can be added for detection of a direct contact at the lower edge of the protective hood. For contact and (redundant) distance determination, also the system can be supplemented by commercially available sensors (e.g. optical, ultrasonic, and capacitive).

In the same sense, the lower edge of the hood optionally can be equipped with pressure-sensitive sensors and the force can limited during the height adjustment by current monitoring – especially while the lowering.

A simple and cheap pressure-sensitive sensor covering the entire lower edge of the hood can consist of a thin elastic tube, which is attached to a pressure sensor. A pressure change in the tube can easily be registered by the control unit.

Further the rear roller of the standard hood can be replaced by another optical distance sensor. By this means, also the end of the sawing process can be monitored at the exit point of the workpiece. However, smaller workpieces may not even be transported up to this point and therefore cannot be monitored.

By all these means only a small area at the front and rear of the hood cannot be observed due to unavoidable concealments. However, if it happens that the hood hits an obstacle during lowering due to concealment, the lowering speed is slowed down or stopped and the system can respond promptly.

Specific optical sensor design considerations

The basic concept behind the NIR sensor has already been introduced in prior works [5,6]. The sensor consists of three main parts: transmitter, receiver and central logic. While the transmitter is used to emit NIR radiation of different wavebands consecutively through different types of LEDs, the remission intensity of each emitted NIR radiation is measured by the receiver. The detection hardware of the receiver consists of several photo-diodes which are arranged in a row. This setup enables the sensor to estimate the distance to the measurement surface through triangulation (see Figure 2). The distance information is internally utilized to generate a distance-corrected spectral signature. A microcontroller-based central logic is used to coordinate the measurement routine and to process the acquired data. As part of a safety function the NIR sensor could trigger within few milliseconds an emergency stop in case of skin detection. Most components inside of the NIR sensor are non-redundant. But because of extensive self-testing features (e.g. temperature and current monitoring) the NIR sensor can be classified as a category 2 system according to DIN EN ISO 13849 [7] and could reach Performance Level $PL = c$ or even $PL = d$.

The material classification performance of the NIR sensor has been evaluated successfully [8]. As expected a perfect separation between skin and wood is possible, because the used NIR wavebands are specifically chosen to distinguish skin from common workpieces. The perfect separation between wood and gloves (e.g. leather, nitrile) which might be used, would require specific adjustments of the sensor settings. In some cases it might not be possible to classify certain glove materials correctly. So care must be taken which gloves might be used and a qualification procedure prior the use of the gloves is recommended.

As mentioned above already, in the considered scenarios the NIR sensor is used in combination with the protective hood. Therefore, the sensor only must be fast enough for the height adjustments, which are quite relaxed time requirements for an optoelectronic sensor. This allows a different sensor design with longer exposure times and oversampling, which is helpful to increase the accuracy of the distance estimation and the material classification. It is assumed that the precision of the distance measurement to the workpiece of about $\pm 1\ \mathrm{mm}$ tolerance is sufficient to guarantee the correct

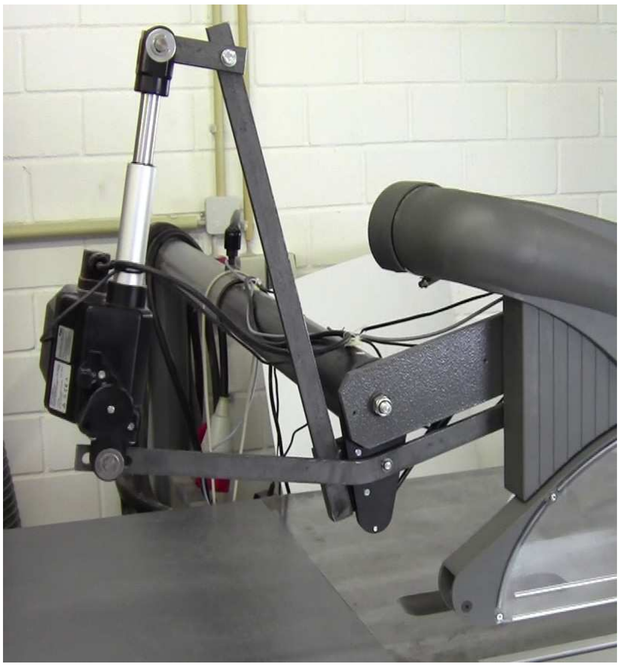


Figure 3: Electrical lifting cylinder and transmission setup

height adjustment. This could be shown in the experiments. Furthermore the mentioned oversampling can be used to decrease noise influence and to eliminate outliners, e.g. as a result from heavy electromagnetic noise. It also should be mentioned that without major design changes it is possible to arrange several of the NIR sensors in a row in front of the protective hood to enhance the detection of uneven workpieces like wedges.

Motorized adjustment of the EN 1870-1: 2009 compliant hood

Only a few externally visible modifications to the existing protective hood have to be made in order to implement the concept. The height of the entire hood above the table is altered by an electric actuator. The lower edge of the hood always remains parallel to the saw table, as defined in EN 1870-1: 2009, 5.3.7.1.3, c. With respect to the workflow the actuator must be able to move the hood quickly enough up and down.

A maximum workpiece height of up to $h = 120\ \mathrm{mm}$ and a maximum feed speed of $v_{\mathrm{feed}} = 0.13\ \mathrm{m/s}$ are assumed for the prototype.

This requires an average adjustment speed of $v_{\mathrm{lift}} \geq 0.53\ \mathrm{m/s}$ for the hood at a detection distance of $d_{\mathrm{spot}} = 30\ \mathrm{mm}$. If the detection distance is increased to $d_{\mathrm{spot}} = 70\ \mathrm{mm}$ the lifting speed requirements are reduced to $v_{\mathrm{lift}} \geq 0.23\ \mathrm{m/s}$.

In the case of the demonstrator's sliding table saw (Altendorf WA 80) the actuators could be integrated quite easily into the existing hood mechanism by replacing the given gas cylinder by a commercial electric cylinder using a spindle drive. However, it was decided to use a modified construction as shown in Figure 3.

The electric cylinder also in this construction is moving the hood upwards and downwards. In the downwards-direction for reasons of squeeze protection there is no closing force generated by the cylinder; only the weight of the hood is balanced. So mechanic injuries to the user are prevented, in case fingers are put underneath the closing hood.

Additionally, the electrical cylinder allows a (zero-current) free movement of the hood as well, in order also to allow quick manual adjustments. It is expected that if the user would have to press the up- and down- buttons for a long time whenever a manual hood is demanded, this might lead to a poor acceptance of the whole installation. So, for the optional manual adjustment, the electric drive might be disengaged.

As mentioned already, the commercial electrical lifting cylinder is a standard type from an established manufacturer and requires no exotic means (electrical power supply: $U = 24\ \mathrm{VDC}$, stroke: $d_{\mathrm{stroke}} = 200\ \mathrm{mm}$, maximum speed: $v_{\mathrm{stroke}} = 21\ \mathrm{mm/s}$, maximum lifting force: $F_{\mathrm{lift}} = 2000\ \mathrm{N}$).

Commercial electric cylinders like the applied one often offer equipment options, which can provide added values to the concept: in extent to the usual limit switches, sensors allow to monitor the absolute position of the spindle. In the simplest case the position is measured by potentiometers. But also more accurate sensors are available, such as optical or inductive encoder, connected to the spindle.

As primary sensor for the position measurement such sensors are not the first choice, because they only can measure the position indirectly whereas the optical sensor does this directly.

Further options might cause extra cost. Hence, it must be considered how the options might be used as redundant sensors and allow e.g. plausibility checks as bargain for the safety.

Camera system details

The very compact camera delivers frames with a resolution of $1920 \times 1080\ \mathrm{pixels}$ at a frame rate of $f = 30\ \mathrm{FPS}$ and the image processing is performed within an application specific region of interest (ROI) which here is a narrow slit within the image. In order to achieve a high image throughput for a short reaction time a simple edge detection is used to detect extra objects within the ROI.

Control unit

As control unit a commercial embedded computer type Raspberry Pi [10] is used, which is connected to the other components. The NIR sensor is connected via USB interface and continuously sends distance and material information. The electric actuator for the height adjustment is directly controlled by the control unit through dedicated electric signals. These signals are decoupled with relays to protect the control unit from high voltages. The relative change in height of the protective hood is monitored by an optical sensor which is measuring the rotation of the spindle in the electric cylinder. This sensor is also connected via USB interface.

Safety assessment: evaluation of risk mitigation through the concept

The consideration is carried out with regard to the differences between the manual and the automatic height-adjustable protective hood.

For usual operation of sliding table saw the accident prevention regulations do not allow wearing (leather) gloves. Hence, for this study the use of gloves is not considered.

For standard scenarios a maximum risk reduction can be achieved if the hand approaches from the front.

For relevant workpiece thicknesses and hand approaches from the side or the rear a potential danger for hand injuries still remains as long as only a single skin detection sensor (in front of the saw blade) is used. At this point, the combination with a second safety concept such as the fast breaking system of the Griggio UNICA SAFE would be good counterpart.

By automatically lowering the hood to the smallest possible level after the cut, the risk of injuries between cuts can be minimized. Even if workpieces remain under the hood after the cut, the risk of injuries can be reduced.

In addition to the increased occupational safety in the considered scenarios, a progress with respect to the ergonomics can be expected because no manual height adjustment of the protective hood is required.

The use of a camera mounted on the inside of the hood may not be robust against pollution by sawdust, which has a bad influence on the visibility conditions of the camera. This refers to the sawing process as well as the constant growth of dust deposits on the visual components of the camera system. Despite that, it is a first approach to solve the problem to recognize remaining workpieces and other obstacles under the hood for the functional demonstrator. As mentioned earlier, it could be enhanced or replaced by other strategies and sensor types to overcome the problem of decreased sight.

Some application scenario still require a special treatment and are not covered with the described concept. While changes of the workpiece thickness in pushing direction by means of the height adjustment a high level of protection can be guaranteed, special solutions for workpiece height changes transversely to the feeding direction must be considered.

In this case, however, at least the level of safety of the manually adjustable hood is guaranteed. No disadvantage compared to the manually adjustable guard has to be expected.

With increased sensory effort the correct function of the automatic height adjustment could also be achieved in those scenarios.

For this purpose, a monitoring over the entire width of the hood must be implemented. This could be realized by a swiveling device combined with a single skin sensor, or by a line sensor around the lower edge of the hood. Another approach for such scenarios is the use of inexpensive auxiliary sensor technology to broaden the measurement base at the lower edge of the hood, such as ultrasonic or conventional triangulation sensors.

The resulting technical and financial overhead nevertheless might be inappropriate since such scenarios seem to represent rather rare use cases.

As an optional safety function, a shutdown of the saw blade rotation during frontal engagement in is possible, which only occurs if the hand is below the lower edge of the guard. This safety function can be implemented as a software function and no additional hardware is required.

Conclusion and outlook

The technical feasibility as well as a benefit in ergonomics, comfort and safety for the concept of an automatic height-adjustable guard for sliding table saws could be demonstrated in the project.

A combined sensor for precise distance measurement and reliable skin detection has been used along with a camera system for object tracking under the hood. The actuator could be realized by a commercially available electric cylinder, which can also be used to detect blockage or collisions with other objects of the hood.

The proposed approach has the advantage that only a few externally visible modifications to the existing protective hood have to be made. Therefore, the distribution as an upgrade kit would be possible to ease the attainment of manufacturers with existing machines. In addition, the use of a camera enables a precise timing for lowering the protective cover in order to prevent a possible collision with obstacles already in advance. The usefulness of the concept has been discussed within a qualitative risk assessment. As a result, the concept can comply with the intended use cases of the machine.

The remaining risk can be lowered furthermore by the combination with a capacitive hand detection system at the saw blade, as presented by SawStop and Griggio.

References

[1] N. Jung *et al.*, Field “Study Results of a skin detecting Safety Sensor on Circular Saws,” in *Proc. 6th Int. Conf. Safety of Industrial Automated Systems*, Tampere, FI, 2010.

[2] O. Schwaneberg *et al.*, “Push-buttons with Material Classification based on Spectral Signatures,” in *Proc. 6th Int. Conf. Safety of Industrial Automated Systems*, Tampere, FI, 2010.

[3] H. Steiner *et al.*, “Spectral Light Curtains – Novel Near-Infrared Sensor System for Production Machines,” in *Proc. 7th Int. Conf. Safety of Industrial Automated Systems*, Montreal, CA, 2012.

[4] *Safety of woodworking machines*, EN 1870-1, 2009.

[5] O. Schwaneberg *et al.*, “Design of an LED-based sensor system,” *Appl. Opt.*, vol. 51, num. 12, 2012.

[6] O. Schwaneberg et al., “Material classification through distance aware multispectral data fusion,” *Meas. Sci. Technol.*, vol. 24, num. 4, p. 045001, 2013

[7] *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*, ISO 13849, 2006.

[8] O. Schwaneberg, “Concept, System Design, Evaluation and Safety Requirements for a Multispectral Sensor,” Ph.D. dissertation, Univ. Siegen, Siegen, DE, 2013.

[9] DGUV-Project FF-FP0289 http://www.dguv.de/ifa/Forschung/Projektverzeichnis/FF-FP_0289-2.jsp

[10] https://www.raspberrypi.org/

Corresponding address

Bonn-Rhein-Sieg University of Applied Sciences
Safety and Security Research Institute
Grantham-Allee 20

53757 Sankt Augustin (Germany)

Phone: +49 2241 865 211
Fax: +49 2241 865 8211
E-Mail: norbert.jung@h-brs.de

Study on appropriate positioning of emergency stop devices equipped in robot work system

Hiroyasu Ikeda[a] Tsuyoshi Saito[a] Toshinori Suzuki[b]

[a] *National Institute of Occupational Safety, Japan (JNIOSH)* [b] *Nihon University*

Abstract

The operation to urgently stop robots by humans is required to be "sure" and "quick." The emergency stop device should be positioned in such a place that ensures easy, quick and safe operation but without referring to detailed positioning conditions. To stipulate the optimum positioning conditions of the emergency stop device, the authors defined the safety conditions of robotic stopping, analyzed the emergency stop operation characteristics of humans and the locus image of serial behaviors related to the robotic stopping characteristics. The measuring apparatus for the emergency stopping performance that allowed overall measurement and evaluation was developed. By using this measuring apparatus, the basic data to examine the appropriate positioning conditions of "quickly" pressing the emergency stop button was obtained.

Keywords:

Emergency stop device; Appropriate positioning

Introduction

The operation to urgently stop robots by humans, which is normally the last resort in case of failure in the protective stopping by using interlock function, is required to be "sure" and "quick." To fulfill these requirements, the emergency stop device should be suitably positioned on the robot or its operation panel. The applicable safety standards require the emergency stop device to be positioned in such a place that ensures easy, quick and safe operation but without referring to detailed positioning conditions.

On the other hand, because the robotic stopping process is triggered by the emergency stop signal generated by human operation, the robotic stop characteristics also affect the positioning conditions of the emergency stop device in addition to the characteristics of human stop operation. However, because it is difficult to clearly define and measure the complete robotic halt state, no standard measuring method has been established.

In view of the above, this paper (1) reviews the positioning conditions of the emergency stop device, and proposes a measuring method for obtaining the positioning conditions, (2) defines the safe state that can substitute for the complete robotic halt state, and proposes a method for measuring the robotic stop characteristics, (3) establishes a measuring apparatus for overall emergency stopping performance by combining these measuring methods because they resort to the image analysis of motion loci, and (4) examines the measurement procedure and parameters through a preliminary test to focus on the emergency stop operation characteristics of humans.

Positioning Conditions of Emergency Stop Device and Measuring Method for Human Motion

Safety Requirements

For the emergency stop device of machines, including industrial robots, the mechanical and electrical safety requirements for the device are stipulated by ISO 13850[1], IEC 60204-1[2] and IEC 60947-5-5[3], and the robotic safety function is deemed to be satisfied by the purchase of emergency stop devices that are conformable to these standards.

On the other hand, the above standards stipulate basic rules that the emergency stop device shall be placed so as to be:

- Clearly identifiable to human eyes, and easily available to humans.
- Safely operated by humans to stop the target machine as quickly as possible.

The "easy operation" of the emergency stop device means the human operation in an ergonomically natural attitude without being disturbed by obstacles. Since the easy operation is limited by the target machine or environment, there are a few specific stipulation examples. As examples of the standard positioning conditions of the emergency stop device, IEC 60204-1 stipulates the height from the floor as 0.6m or more, SEMI S8-0705 stipulates the height from the floor as 838 - 1,638mm, and SEMI S2-0706 stipulates the distance from the working position as within 3m.

To quickly stop the target machine, the "quick operation" of the emergency stop device is required. However, the reliable performance of the quick operation is also required because the machine may not be stopped if the quick operation fails. Since the "quickness" and the "sureness" are characters considered to be conflicting in terms of human operation, the optimum balance between both characteristics has not been stipulated in writing.

Positioning Conditions

In general, the "quickness" of device operation by humans is evaluated by time dimension, and the "sureness" is evaluated by success rate, etc. To analyze the positioning conditions, it is insufficient to use only the timer function and record the output frequency of the emergency stop device. To make up for this insufficiency, this study proposes a method of analyzing and measuring hand motion loci from when a human detects danger to when he ends the operation of the emergency stop device based on the image analysis in addition to the use of the timer function. Since the pre-operational posture and hand motion of humans depend on the positioning conditions of the emergency stop device, the relation between the device position and the initial human operation condition can be judged by simultaneously measuring the time interval between the danger detection by a human and his reactive motion and the motion loci of his hand (arm). Incidentally, though human body characteristics are involved with the positioning conditions, to eliminate the difference in these characteristics, the optimum positioning conditions of the emergency stop device are obtained by the standard distance normalized by the human body height.

To judge the “sureness,” this method can analytically judge whether a human made wrong pressing without touching the device or made pressing too shallow to achieve the full stroke in addition to whether the contact output of the emergency stop device is present or absent. This study aims to establish a measuring system having all above functions this time.

Robotic Stop Judgment and Its Measurement Method

Safety Conditions of Robotic Stop

Since it is difficult to measure the physically complete halt of robotic movable regions, the safe stop state is defined by referring to the “termination of hazardous machine functions” before the complete halt in accordance with ISO 13855[4] (Fig. 1). The state of the “termination of hazardous machine functions” is assumed to be the state not hazardous to humans. To define this state, the force and kinetic energy on a human body, the body region to be contacted, the configuration, material, etc. of the contacting mechanical region are considered. When it is considered that a robot is in contact with the human body skin surface (skin displacement = 0) and then stops and compresses the skin to cause displacement as the reasonably assumed worst condition, the following 2 conditions protect humans from danger (from the viewpoint of humans):

1. The skin displacement is within the allowable range.
2. The danger can be avoided before the allowable displacement range is exceeded.

As the allowable value of 1, Annex B of ISO 13855 specifies 2mm (excluding the head), and the study of the authors indicates 2.1mm (forehead)[5]. As to 2, there is a report[6] on the measurement of the time interval from when a human detects an unexpected robotic motion to when he operates the emergency stop device. The report says that the time interval from when he tactilely detects danger to when he avoids the danger is approx. 0.5s, and it takes longer when he visually does the same. From the above, it may be determined that if the skin displacement made by a robot exceeds the allowable value within the time shorter than the time interval required by a human from when he detects danger to when he avoids it, he fails to avoid it, i.e., he is under fear of hazard.

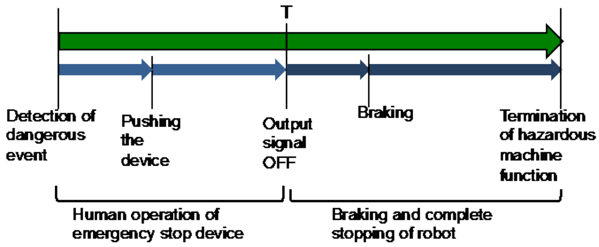

T
Detection of dangerous event
Pushing the device
Output signal OFF
Braking
Termination of hazardous machine function
Human operation of emergency stop device
Braking and complete stopping of robot

Figure 1: Overall emergency stopping performance

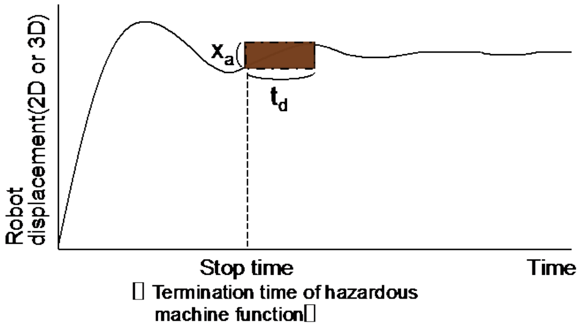


Figure 2: Judgment of robot stop condition

In this study, as one of the safety conditions of robotic stop operation, the authors propose that the “displacement of the stopping process shall be within 2mm (x_a) for over 1s (t_d).”

Stop Judgment Method

Since various robot regions may contact human bodies, it is not realistic to depend only on the robotic internal sensor to monitor the stopping process. If the process from when a robot receives the stop command and starts braking to when the robot converges its motions can be obtained as a time-displacement characteristic among plural regions, the motion locus of each position on an arbitrary line connecting these regions can be obtained. Then, as shown in Fig. 2, when the above safety condition of stopping the robot is preset as a time-displacement judgment window and the target motion loci are consecutively monitored from this window, it is possible to judge stop (i.e., to identify the initial time when the displacement norm is no longer exceeded over the time norm span) and obtain this initial time as a stop time.

Incidentally, while the stopping process of a robotic movable regions forms 3D locus, the amount of displacement from when the robot receives the stop signal to when it is judged stopped (i.e., distance of overrun) is set absolutely to the shortest linear distance as the distance of approach to the human body (or as the amount of displacement resultantly caused to the skin).

Measuring Apparatus for Overall Stopping Performance

The measuring apparatus for realizing the functions described in the foregoing sections is configured so as to allow a human to continuously measure the process from when he operates the emergency stop device to when the robot receives the emergency stop signal and stops. As shown in Fig. 3, the measuring apparatus is composed of 4 units: (a) human operating motion measuring unit, (b) robotic electric response measuring

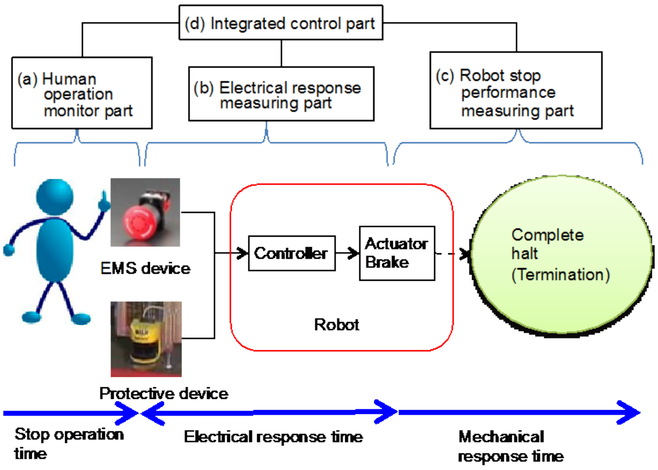

(d) Integrated control part
(a) Human operation monitor part
(b) Electrical response measuring part
(c) Robot stop performance measuring part
EMS device
Controller
Actuator Brake
Robot
Complete halt (Termination)
Protective device
Stop operation time
Electrical response time
Mechanical response time

Figure 3: Overall stopping performance measuring system

unit, (c) robotic stop characteristic measuring unit, and (d) overall control unit. This apparatus can measure all the processes shown in Fig. 1. As major hardware, the apparatus has 2 pairs of stereo cameras (DITECT HAS-220 and HAS-L1) that are mutually connected through an image capture board within the PC. The image data (human motion, robotic stopping process) captured by the cameras is analyzed by using the 3D motion measurement software (DITECT Dipp-Motion PRO) and integrated software running on the PC.

The measuring unit (a) converts the onset of an unexpected robotic motion (creation of the hazardous state) into an electric signal to trigger the recording of the human motion locus until he activates the emergency stop device by using the stereo cameras. The locus of the recorded image can be analyzed by using the motion measurement software with the resolution of ±0.5mm.

The measuring unit (b) with a counter function measures the time required for reaction of the robotic stop circuit (including the time required for response of the robotic control circuit). This unit measures the time until the robotic actuator power shuts off or the braking unit starts with the precision of ±0.1ms by using the operation signal of the human-operating emergency stop device as a trigger.

The measuring unit (c) records the mechanical stopping process of the robotic movable region by using the stereo cameras. This unit functions in the same way as the measuring unit (a), though it uses a high-speed camera for highly precisely recording the low-speed deceleration or stop behavior to achieve the space resolution of 0.1mm. Incidentally, the stop judgment function by using the time-displacement judgment window described in a previous chapter is incorporated into (d) of Fig. 3 as an off-line analysis function using MS Excel. This judgment window can automatically obtain the stop time by repeating generation and judgment while making a displacement at every 10ms. As an example, the stopping performance judgment by using a nursing lift, which takes longer to stop than robots do, is confirmed.

The unit (d) integrates the measurement results of (a)-(c). This unit analyzes the overall emergency stopping performance of robots, including human stop characteristics, and displays the analysis results.

Method Measurement for Obtaining Positioning Conditions of Emergency Stop Device

Measurement Conditions and Preliminary Verification

To clarify the optimum positioning conditions of the emergency stop device according to various robotic operating unit modes and human operating modes, the human stopping operation characteristics should be grasped. Concerning these characteristics, as above described, the “quickness” and “sureness” of the emergency stop operation serve as evaluation indexes. This time, focusing on the quickness, the human emergency stop characteristics are measured to determine the positioning conditions of the emergency stop device.

In this context, to measure the time interval from when danger is detected to when the emergency stop device (OMRON Emergency Stop Button A22E-M-01) is operated by using the functions mainly of the units (a) and (d) among all shown in Fig. 3, the onset of an unexpected robotic motion (creation of the hazardous state) is alerted by manually lighting the LED lamp (Fig. 4), and the measurement of the time required for stopping operation and the recording of the human motion locus start by using the lighting as a trigger. When the human presses the emergency stop button, the trigger to end the stopping operation time measurement and that to end the recording are activated.

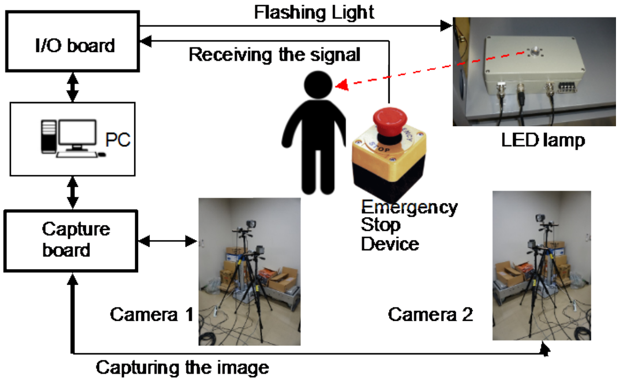


Figure 4: Measuring system part of human stopping process

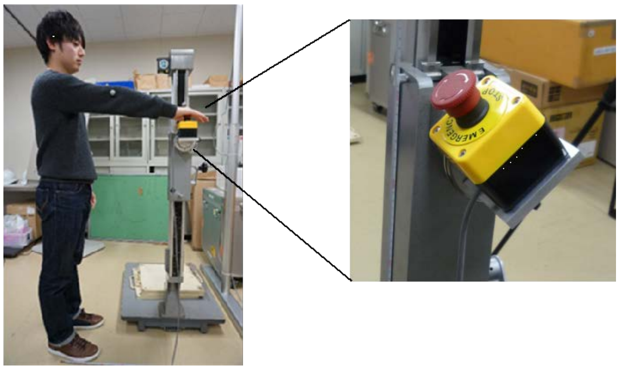


Figure 5: Installation of emergency stop device

To measure the human operational characteristics when the positioning conditions of the emergency stop button are changed, the emergency stop button is tiltably attached to a lifting/lowering mechanism, and the height of the button from the floor and the angle of human button pressing can be adjusted (Fig. 5). The LED lamp for generating trigger signal to urge the human to visually detect the danger and enter the emergency stop motion is positioned at 1.5m before the human and 1m from the floor as fixed positioning conditions. The PC records the behavior of the human arm from when he presses the button upon the lighting of the LED lamp to when the contact output is cut off, and the loci of the markers pasted on the dominant arm of the human (back of the hand, the elbow) are obtained by using the software of (d) in Fig. 3.

To observe the operational time trend of one human according to the position of the emergency stop button, a vertical plane was set beforehand in the range in which he can smoothly press the emergency stop button by his dominant arm in the standing position (both the shoulder and the body remain stayed static), the emergency stop buttons were placed in 9 positions on the plane (upper, middle and lower respectively at left, center and right) to be horizontal to the floor, and the time required for operation was measured. The human with his right arm as the dominant arm was instructed to put his hand initially with its back in contact with his body while its palm squarely facing the vertical plane at the same level as the center of the vertical plane. When the average time required for operation was calculated, it was found as might be expected that, on the same vertical plane, the farther the hand was apart from the center position, the longer the time was required, and the time required for the lower position was longer with the larger amount of visual line from the LED lamp. When compared at the same height on the vertical plane, generally, the right side tended to required longer time than the left side did.

Tendency Depending on Positioning Conditions

Next, the parameters shown in Table 1 were provisionally set to 5 male adults, and measurement was taken to verify the validity of these parameters. The position of each button was evaluated as a value relative to the shoulder height and the arm length. For this reason, the heights from the floor were normalized by the human shoulder heights, and the distances from the human bodies were normalized by the human arm lengths, and they were classified into 3 groups.

The actual measurement results are shown as 3D loci in Fig. 6. This figure gives an example that the button vertically placed at the shoulder height was operated from a position nearer to the button by 0.5m from the front edge of the arm length by moving his arm nearly horizontally at the same level as the shoulder. The time required for stopping operation was 0.44s. Incidentally, when the horizontal distance was only the arm length with no approach, the time required for stopping operation was 0.71s. On the other hand, even with the same button-human distance, the tendency was that the time required for stopping operation was shorter when the motion locus was linear.

Table 1: Measuring parameters of positioning conditions

Positional conditions of EMS (button)	Parameters
Button height from floor	Shoulder height, Shoulder height x 0.71, Shoulder height x 0.46
Button-human distance	Arm length, Arm length x 0.52, Arm length x 0.21
Button angle to floor	0 deg., 45 deg., 90 deg.
Arm position	Lower (natural posture), Shoulder height (palm level)

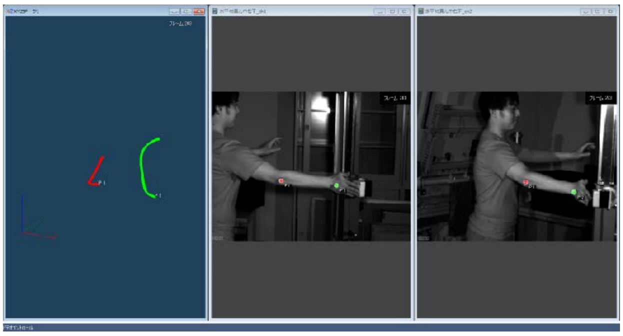


Figure 6: Example of 3D loci and captured motion (red maker: elbow, green maker: back of hand)

When attention is paid to the angle of the emergency stop button to the floor, and the parameters of the button height from the floor, button-human distance, and arm position were fixed, the time required for stopping operation was the shortest when the angle was 45° in over 80% of all trials. Then, the influence of the measurement frequency was investigated. When 5 humans were subjected to trial for 3 times each with the same parameters, and the time required for stopping operation was compared with each other, there was no clear tendency.

1. When the button-human distance was small, the dispersion in the time required for stopping operation with varied parameters was large, but when the distance was large, the dispersion was small. From this, it is conceived that the smaller the button-human distance is, the more influence received from other parameters, but the larger the distance, the less influence received.
2. When the button was tilted at 45° to the floor and the other parameters were fixed, the time required for stopping operation tended to be shorter. However, when the other parameters were varied, the tendency was not clear. Depending on the button angle, the hand approaching angle or the actually pressing button portion might be varied. From this, it cannot be completely defined a specific angle that is easy for pressing.
3. It was likely that the time required for stopping operation gradually became shorter with the same parameters as the number of trials increased because humans accustomed themselves to stopping operation, but no such tendency was seen probably because of fatigue of operation or degradation of human concentration.

Conclusion

To stipulate the optimum positioning conditions of the human-operating emergency stop device, the authors defined the safety conditions of robotic stopping, analyzed the emergency stop operation characteristics of humans and the locus image of serial behaviors related to the robotic stopping characteristics, and developed a measuring apparatus for the emergency stopping performance that allowed overall measurement and evaluation. By using this measuring apparatus, the authors succeeded in measuring the emergency stop operation characteristics to determine the positioning conditions of the emergency stop device and obtained the basic data to examine the appropriate positioning conditions of “quickly” pressing the emergency stop button. In the future, also from the viewpoint of the reliability of button operation, the authors plan to study the optimum positioning conditions.

References

[1] ISO 13850:2015. Safety of machinery - Emergency stop function - Principles for design.

[2] IEC 60204-1 Ed. 5.1:2009 (b). Safety of machinery - Electrical equipment of machines - Part 1: General requirements.

[3] IEC 60947-5-5 Ed. 1.1:2005 (b). Low-voltage switchgear and controlgear - Part 5-5: Control circuit devices and switching elements - Electrical emergency stop device with mechanical latching function.

[4] ISO 13855:2011. Safety of machinery -- Positioning of safeguards with respect to the approach speeds of parts of the human body.

[5] Tsuyoshi Saito, Hiroyasu Ikeda. Measuring System and Analytical Method of Pain Tolerance to Mechanical Stimulus for Safe Design of Human-collaborative Robot. Proc. of SIAS 2005.

[6] Kiyoshi Fukaya, Hiroyasu Ikeda, Shigeo Umezaki and Shoken Shimizu. Evaluation of Danger Perception Ability by Tactile Sense of the Aged. Special Research Report (SRR-No.13-5). National Institute of Occupational Safety and Health, Japan (in Japanese).

Corresponding address

JNIOSH
1-4-6, Umezono, Kiyose, Tokyo, 204-0024 Japan.
ikeda@s.jniosh.go.jp

SIAS 2015

8th INTERNATIONAL CONFERENCE ON THE SAFETY OF INDUSTRIAL AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

Session 6: Practical applications/experiences

Causes of fatal and serious accidents involving machinery in Quebec

Yuvin Chinniah[1]

[1]Polytechnique Montreal

Machine contains hazards of different nature and exposure to those hazards can result in injuries and deaths. In this paper, over 100 accident reports for the period 1990 -2011 are analysed to identify the causes leading to serious and fatal accidents involving machinery in Quebec. An Excel spreadsheet was used to classify the following information: report reference number, date of the accident, industrial sector, time of the accident, machine involved, harm caused, description of the hazard, activity performed at the time of the accident, occupation or job title of the worker, causes of the accidents, existence of an OHS committee in the company, if the worker was alone or not, worker's experience in the activity leading to the accident. The main causes of accident were found to be : (i) easy access to moving parts of machinery (ii) lack of fixed guards and of moveable guards with interlocks (iii) absence of lockout procedures during maintenance (iv) inexperience of workers, (v) bypassing safeguards, (vi) absence of risk assessment, (vii) poor machinery design and (iv) modifications to machinery and its control system. Accidents occurred despite companies having lockout program (policies) since the procedures were not implemented. There were no accidents caused by failures of safety control systems.

1. Introduction

ISO 12100 defines a machine as an assembly fitted with or intended to be fitted with a drive system consisting of linked parts or components at least one of which moves, and which are joined together for a specific application. Machines contain hazards of different nature and exposure to those hazards can result in injuries or deaths. Since workers intervene on machinery in all the phases of its life cycle, they are exposed to hazards. Numerous accidents are related to machinery. The Bureau of Labor Statistics in the US (BLS, 2014) revealed that a total of 717 fatal work injuries occurred as a result of contact with objects and equipment in 2013. This number includes 503 workers who were fatally injured after being struck by objects or equipment. Out of the 503 workers, 245 workers were struck by falling objects and equipment other than powered vehicle and 29 workers were struck by discharged or flying object. 131 workers were caught in or compressed by equipment and objects, including 105 workers being caught in running equipment or machinery. 78 workers were struck, caught or crushed in collapsing structure, equipment or material. The HSE reports that 50% of accident related to moving parts of machines in UK occurred in printing presses and conveyors (HSE, 2006). Bulzacchelli et al. (2008) report that in 2005 just over 1000 (i.e. 18%) of workers fatally injured in the US were by contact with objects and equipment. Bellamy et al. (2007) report that annually about 400 accidents, i.e. 21% of total accidents per year in the Netherlands, are caused by contact with moving parts of machinery. In Canada on average 177 hospitalizations per 100,000 people are reported annually due to agricultural machinery injuries (Brison et al. 2003). A total of 159 machinery related injuries on 2390 farms in the province of Saskatchewan in Canada were reported in 2006 and these agricultural injuries were due to machinery such as tractors (23%), transportation equipment (16%), harvesting equipment (16%), augers (11%) and combines (11%) (Narasimhan et al. 2010). In Canada, national statistics on the number of machinery-related accidents, apart from agricultural machinery injuries, are not available. In the province of Quebec in Canada, between 2000 to 2004, there were 770 agricultural machinery related injuries, which represented 12% of the 6604 occupational injuries in the agriculture sector (CSST, 2006). In Quebec, between 1989 and 2003, 12% of fatal injuries on farms were caused by moving parts of machinery. In 2005, the OHS regulator for Quebec, the CSST, revealed that around 13 500 machinery related accidents and 20 deaths occurred annually in the province (CSST, 2006). Moreover, the CSST has introduced in 2005 a safety of machinery action plan to educate machine suppliers, employers, workers and other associations about the risks associated with machinery. The action plan focused on access to moving parts of machinery. In 2010 the CSST revealed that 3552 workers were injured as a result of an accident linked to a machine. Between 2006 and 2010, on average 12 workers were killed each year as a result of work accidents related to machinery. Due to the action plan of the CSST which began in 2005, the number of annual machinery accidents has dropped significantly. The literature in the field of safety of machinery is rich and consists of machine safety standards, regulations, peer reviewed and non-peer-reviewed journal and conference papers, books, guides, leaflets and checklists. It is important to understand the causes of accidents in order to identify potential solutions to further reduce the number of injuries and fatalities. The literature on machinery related accident reports identifies several causes of accidents as described in (Backstrom et al. 2000), Bulzacchelli et al. 2008), (Shaw 2010), (Blaise and Welits 2010) and (Charpentier 2005). The causes of machinery-related serious and fatal accidents in Quebec have not been studied.

2. Research objective and method

The objective of the paper is to identify the main causes leading to serious injuries and fatal accidents involving machinery in Quebec. In this paper, 106 accident reports of fatal and serious injuries involving machinery in the manufacturing and processing sector covering the period 1990-2011 in Quebec have been analysed. Accidents reports for serious or fatal injuries to workers were available from the CSST website and accessible to the public. The accident reports and their corresponding annexes were downloaded, one at a time, from the CSST website. Generally the CSST accident reports were organised as follows:

- Information about the injured or deceased worker, the name of the worker being removed from the public report.
- Name of the company, its location and size, details on the general organization of the company, information on the products being manufactured or transformed and organization of OHS in the company.
- Description of the machine involved in the accident.
- Description of the accident and events leading to the accident.

- Possible causes of the accident as identified by the CSST inspector(s).
- Contributing factors to the accident.
- Identified causes of the accidents or sequence of events leading to the accident with necessary justifications.

The accident reports also contained photos, schematics, relevant sections from regulations, and relevant sections from machine safety standards. A few accident reports also included, as annexes, separate reports drafted by experts, mostly safety engineers, who had been hired by the CSST. The number of pages for each report and each annex varied. The accident reports ranged from 8 to 32 pages in length. The annexes ranged from 1 to 30 pages. The large majority of reports had one annex and some reports had up to 5 annexes. An Excel spreadsheet was used to classify the following information:

- Report reference number.
- Date of the accident.
- Industrial sector,
- Time of the accident.
- Machine involved.
- Harm caused.
- Description of the hazard.
- Activity performed at the time of the accident.
- Occupation or job title of the worker.
- Causes of the accidents and relevant remarks.
- Existence of an OHS committee in the company.
- If the worker was alone or not.
- Worker’s experience in the activity leading to the accident. .

3. Results and discussions

The main findings from the analysis of 106 accident reports are summarized and discussed in this section.

3.1 Number of fatalities and serious injuries and time of the accident

The 106 accidents resulted in 31 serious injuries (29.2%) involving deep lacerations, loss of an upper or lower limb (crushing, entanglement), as well as 75 fatalities (70.8%) which occurred following serious injuries (i.e. sometime after the accident) or on site (i.e. at the time of the accident). Table 1 shows the consequence of the accidents as well as the parts of the body injured. Workers had part of their bodies, usually upper or lower limbs close to hazards. In many cases workers had entered the hazardous zones and their whole bodies were inside the hazardous zones. Such proximity to moving parts of machinery made it almost impossible to avoid the harm. Every accident caused serious or fatal injuries to only one worker, i.e. there were no multiple casualties.

Table 1: Consequence of the accidents and parts of the body injured

Consequence of accident	Parts of body injured and injuries	Number of accidents
Death	Thorax and/or abdomen – crushed, internal injuries	26
	Head -struck by object, crushed, fractured	18
	Whole body -multiple fractures, entanglement	9
	Arm(s) - crushed and/or detached	8
	Thorax and/or abdomen-hit by projectile or stabbed	6
	Neck - suffocation, strangulation	5
	Face -struck by object	3
Serious injuries	Arm(s) - cut off, crushed or deep laceration	8
	Abdomen- crushed or hit by object	6
	Leg(s)- cut off, crushed or detached	6
	Fingers- cut off	5
	Hand - lacerations	2
	Head – struck by object	1
	Feet-crushed	1
	Whole body-multiple fractures, entanglement	1
	Shoulder-hit by object	1

3.2 Type of industry, machines and hazards

The 106 accidents involving machinery took place in various different industrial sectors, as illustrated by Table 2.

Table 2: Examples of industrial sectors where accidents happened.

Industrial sector	**Number of accidents**
Sawmills	19
Pulp and paper industry	11
Wood transformation sector	9
Food transformation industry	7
Manufacturing metallic products	7
Manufacturing rubber products	4
Cleaning (laundry and industrial)	4
Manufacturing products made of concrete	3
Textile industry (natural and synthetic fibers)	3

Moreover, the type of machinery involved in the 106 accidents was quite different. Conveyors caused 21 fatal and serious accidents. Unguarded nip points between rotating rollers and moving belts of conveyors were the most common hazards associated with conveyors. Saws (e.g. edgers, band saws, circular saws), were involved in 11 accidents. The hazards were rotating and moving sharp blades, as well as projection of logs or pieces of wood in the direction of workers. Material feeding or loading and material unloading equipment other than conveyors were also hazardous. In several accidents, workers were trapped and were crushed between moving part of machinery and fixed structures (e.g. frames, walls).

3.3 Worker's experience

Whenever possible, the worker's experience in the activity carried out when the accident occurred was recorded, as shown in Table 3. It was observed that 30% of accidents involved workers with less than one year of experience and 46% of accidents with workers with less than 5 years of experience.

Table 3: Worker's experience in the activity carried out when the accident occurred

Experience of workers	Number of accidents (%)
More than 1 day and less than 1 week	2(1.9%)
More than1 week and less than 1 month	7 (6.6%)
More than 1 month and less than 6 months	12 (11.3%)
More than 6 months and less than 1 year	10 (9.4%)
More than 1 year and less than 5 years	18 (17%)
More than 5 years and less than 10 years	5 (4.7%)
More than 10 years and less than 15 years	8(7.5%)
More than 15 years	8 (7.5)
Information not available	36 (34%)
Total accidents	106

New workers or inexperienced workers with the machinery they have to operate or to maintain need to be trained properly. The time allowed for practical training should be extended to cover all the different tasks, especially handling of production disturbances for operators and lockout procedures for mechanics.

3.4 Activities (tasks) carried out when accidents occurred

Many accidents occurred during maintenance and the handling of production disturbances, where the operator entered a hazardous zone of machinery. The mechanical hazard was already present (e.g. rotating shafts) or appeared suddenly (e.g. blade starts rotating suddenly). Table 4 summarizes the activities being carried out by the workers at the time of the accidents. It was found that for 12.3% of accidents were linked to the set up phase, 19.8% of accidents to production tasks, 34.9% of accidents to maintenance tasks and 31.1% to handling production disturbances. In 3 cases, accidents occurred when fixed guards, which had been previously removed for maintenance tasks, were being installed back, while the machines were running.

Table 4: Activities at the time of the accident

Tasks		Number of accidents	%
Set-up	Verifying quality, sampling removing defects, optimizing	13	12.3%
Production	Feeding material manually (loading)	15	14.2%
	Operating	3	2.8%
	Removing finished product manually (unloading)	3	2.8%
Maintenance	Sharpening blades	2	1.9%
	Lubricating	3	2.8%
	Adjusting	5	4.7%
	Installing guards	3	2.8%
	Repairing or troubleshooting	14	13.2%
	Cleaning	10	9.4%
Handling production disturbances	Unjamming	21	19.8%
	Removing excess material	3	2.8%
	Picking up material following incident	4	3.8%
	Adjusting and repositioning material	5	4.7%
Access	Circulating	2	1.9%
Total		106	

In 23 accidents, the actions of another worker had contributed to the accident and at the time of the accident, the worker who was killed or injured was not performing the task alone. Table 5 describes the activities performed by the co-workers at the time of the accidents.

Table 5: Activities performed by the co-workers at the time of the accidents.

Activity performed by the co-worker at the time of the accident	**Number of accidents**
Started the machine not knowing that a worker was in the hazardous zone	14
Assisting a fellow worker when the injury of fatality occurred	4
Holding the controls of the machine which was in operation	1
Rearmed the emergency stop which was used to stop the machine without knowing that his action would cause the machine to start	1
Accidentally activated a position limit switch during maintenance	1
Accidentally activated a light beam while cleaning	1
Started the machine by mistake by activating the wrong control switch	1

3.5 OHS committee and OHS management

In Quebec, the regulation on occupational health and safety committee states that when a company has 50 or less workers, 2 workers need to be on the OHS committee. The number of workers on the committee increases up to 11 when more than 1500 workers are employed by information was missing in the accident reports. It was observed that accidents happened despite the existence of an OHS committee or of a program. The committees had not identified the hazard which caused the accident. Moreover, 46 accident reports identified inadequate working methods, lack of supervision or absence of/inadequate occupational health and safety management as part of the causes of the accident. The worker had to perform a task while being exposed to hazards and in the absence of clear instructions, had to improvise to carry out the task.

3.6 Machinery risk assessment

Risk linked to machinery is defined in ISO 12100 as a combination of the severity of harm and the probability of occurrence of that harm. Machinery risk assessment plays an important role in ensuring that workplaces are safe. From the 106 accident reports, it was found that one mechanic died in an accident involving machinery where risk assessment had been previously performed. After the risk assessment, there was no follow up and safeguards were not installed. In a second accident, failure to identify a hazardous zone created when a conveyor was added next to an elevator resulted in an operator being crushed when a box fell from the conveyor and he reached under the elevator while it was descending. The risk assessment in that case was incomplete. For the remaining 104 cases, no risk assessment was carried out by the companies and the hazards were not identified. Actually in most cases, easy access to moving parts of machinery was possible. The absence of risk assessment was not always clearly stated in the accident reports but it could be deduced since in many cases the CSST inspectors asked for risk assessments as part of the corrective measures.

3.7 Machinery safeguards

Safeguards for machinery are guards or protective devices. In the majority of cases, machine related accidents happened because the hazardous zones were not safeguarded, i.e. absence of guards, or safety devices and moving parts of machinery were easily accessible. Following the accidents, the corrective measures identified in the accident reports included: (i) adding fixed guards (21 cases), (ii) adding interlocked guards, including adding proper interlocks to guards which previously allowed access to moving parts of machinery (7 cases) and (iii) adding guard locking, i.e. mechanism which prevent the guard from opening as long as moving parts of machine have not stopped, to machinery which contain parts with inertia and accumulate energy (4 cases).

3.8 Bypassing (defeating) safeguards

In total, 14 accidents were linked to removal of existing guards and bypassing of safety devices. It was found that 6 accidents involved safety devices being voluntarily bypassed and these involved safety position switches for moveable guards (4 cases) and safety light beam (1 case). In one case, the safety position switch was replaced by a proximity sensor which was then bypassed using a piece of metal. Safety switches monitored the position of guards and they were bypassed using tape to indicate that the guards were closed. They were at times disconnected and even prevented from being actuated when the guard was opened by grooving the position detecting edge of the guard. Proximity sensors were bypassed using pieces of metal attached permanently to the device. In one accident, three safety devices on a plastic molding machine were bypassed. The machine was purchased for being operated by a worker who would manually unload the molded product at the end of each cycle. But afterwards it was decided to automate this process and the guards had to be kept opened to enable the robot to reach into the mold area at the end of each cycle. The accident happened during set up for a change in the production. In another accident, a safety light beam was bypassed because dust generated when bricks were made, caused frequent machine stoppage. A young worker was fatally crushed when he entered the hazardous zone to place some bricks which fell off the conveyor and the palletiser moved downwards towards him and crushed him. In an accident in the wood sector, one edger was modified. The device preventing the logs from being projected backwards towards the operator was bypassed. This was carried out to facilitate unjamming activities.

Moreover, it was found that in 8 accidents, guards were removed permanently, temporarily, during night shift or even fixed in an open position with screws and thus exposing workers to hazards. The guards were initially installed by the machine manufacturer or following inspections of the CSST. The guards were removed because: (i) operators complained about lack of visibility, (ii) maintenance personnel found it tedious to install them and remove them to lubricate or repair machinery and (iii) this allowed rapid removal of products which fell down without stopping machines. In one case, the guard supplied by the machine manufacturer was never installed by the company. In another case, a meshed guard covered a hole through which small pellets could pass through and fall onto a screw conveyor. When larger pellets were used, the guard was temporarily removed and a worker had one leg crushed.

3.9 Lockout programs and procedures

It was found that in 33 accidents, the company did not have a lockout program and lockout procedures were not used during maintenance, repairs and unjamming activities, as required by the OHS regulation (RSST). It was found that in 21 accidents, lockout programs existed but lockout procedures were not used during maintenance, repairs and unjamming activities. In 2 cases although lockout programs existed, the lockout placards for the machinery involved in the accidents were not drafted. In a fatal accident in the pulp and paper sector, a mechanic applied lockout before repairing a conveyor. An adjacent pneumatic actuator (bumper) was not de-energized since the lockout placard for this equipment was never drafted. He was crushed by the actuator and the frame of the conveyor. In another accident, the machinery was modified but the placard was not updated. In 2 cases, an incomplete or incorrect lockout procedure was carried out. A worker in the textile sector had her 3 fingers cut off when she placed her hands inside a hazardous zone in carding machinery. She shut off power but the moving parts did not stop immediately because of inertia. The dissipation phase of lockout was neglected. In two cases, hydraulic and pneumatic energies were not controlled. In almost all cases, the CSST inspectors demanded lockout procedures for the machineries involved in the accidents as part of the corrective measures taken by the companies.

3.10 Safety control systems

ISO 13849 and IEC 62061 are two safety control system design standards. Based on the analysis of 106 accident reports, it was observed that no accidents occurred simply as a result of the designer choosing the incorrect performance levels (PLs) (ISO 13849) or incorrect safety integrity levels (SILs) (IEC 62061) for the safety control system. No serious and fatal accidents were caused because the performance level or safety integrity level was too low. There were 3 reports where the performance levels of the safety control systems were mentioned. It was reported that the control systems were not designed to the required performance levels, based on the level of risk. However, in each case, modification or bypassing of the existing safety control system was also reported. In one accident, in the pulp and paper industry, a standard programmable logic controller (PLC) controlled safety functions on a paper machine. Modifications of the PLC program led to a fatal accident. A worker suffered fatal injuries while intervening on the paper machine with the moveable guard opened. An operator, who did not see the worker, pressed on the start button. Since he found that the machinery did not start, he pressed on reset and pressed on start a second time. The worker had his foot on a roller, which started to rotate and entrapped the worker. The PLC program of the paper machine was changed a few days before the accident without any risk analysis. The new modified program contained a flaw which allowed the rotation of the roller in spite the moveable guard being in the open position. In another accident, the operator of a printing press was killed. He pressed onto the safety bar to stop the machine and reached into the hazardous zone, not knowing that the safety function was invalid because the original softer spring in a pressure safety bar, was replaced earlier by one with higher stiffness. The worker unfortunately did not press onto the safety bar with sufficient force to generate the stop signal. The reason behind changing the spring was that the presence sensing bar was triggering frequent machine stoppage due to its acceleration.

Conclusions

For the first time, a study on serious and fatal accidents linked to moving parts of machinery in Quebec was carried out. 106 accidents reports (31 serious and 75 fatal) related to moving parts of machinery were analysed. Conveyors and different types of saws caused 32 accidents. It was found that 12.3% of accidents were linked to the set up phase, 19.8% of accidents to production tasks, 34.9% of accidents to maintenance tasks and 31.1% to handling production disturbances. The main causes of accidents were found to be: easy access to moving parts of machinery; lack of fixed guards and of moveable guards with interlocks; lockout procedures not applied during maintenance, repairs and unjamming activities; inexperience of workers; bypassing safeguards (guards and safety devices); absence of risk assessment by companies; poor machinery design in terms of location of lubrication points, control panels and tension setting points for conveyors;

unsafe working methods, poor supervision and absence of instructions to workers on how to intervene safely on machinery and modifications to machinery and to its safety control system.

References

Backstrom, T., Doos, M., 2000. Problems with machine safeguards in automated installations. International Journal of Industrial Ergonomics 25, 573-585.

Bellamy, L.J., Ale, B.J.M., Geyer, T.A.W., Goossens, L.H.J., Hale, A.R., Oh, J., Mud, M., Bloemhof, A., Papazoglou, I.A., Whiston, J.Y., 2007. Storybuilder-a tool for the analysis of accident reports. Reliability Engineering and Systems Safety 92, 735-744.

Blaise, J.C., Welitz, G., 2010. Operating on machinery out of mode production: principles and accidentology. In: Proceedings of the 6th Safety of Industrial Automated System Conference-SIAS 2010, Tempere, Finland.

Brison, R.J., Pickett, W., Hagel, L., Issacs, C., Lawson, J., Hartling, L., Alberg, N., Rennie, D., 2003. Hospitalized Agricultural Machine-Related Injuries. Agricultural Injuries in Canada for 1990-2000, Canadian Agricultural Injury Surveillance Program (CAISP) (Chapter 10).

Bulzacchelli, M. T., Vernick, J.S., Sorock, G.S., Webster, D. W., Lees, P.S.J., 2008. Circumstances of fatal lockout/tagout related injuries in manufacturing. American Journal of Industrial Medicine 51, 728-734.

Charpentier, P., 2005. Safety of machinery:Experience feedback on automated accidents from the EPICEA data base. In : Proceedings of the 4th Safety of Industrial Automated System Conference-SIAS 2005, Chicago, US.

CSST (Commission de la santé et de la sécurité du travail du Québec) and UPA (L'union des producteurs agricoles) (2006). La prévention des accidents liés aux pièces en mouvement, DC300-436 (06-11).

HSE, 2006. Analysis of RIDDOR Machinery Accidents in the UK Printing and Publishing Industries, 2003-2004, HSL/2006/83, UK.

Narasimhan, G.R., Peng, Y., Crowe, T., Hagel, L., Dosman, J., Pickett, W., 2010. Operational safety practices as determinants of machinery-related injury on Saskatchewan farms. Accident Analysis and Prevention 42, 1226-1231.

Shaw, S., 2010. Machinery Accidents-Contributory factors. In: Proceedings of the 6th Safety of Industrial Automated System Conference-SIAS 2010, Tempere, Finland.

US Bureau of Labor Statistics. 2014. National Census of Fatal Occupational Injuries in 2013.

Corresponding address

Yuvin Chinniah
Department of Mathematical and Industrial Engineering
Polytechnique Montreal
2500, chemin de Polytechnique
Montreal (Québec) CANADA H3T 1J4
yuvin.chinniah@polymtl.ca

The "Feedback method", a tool to better understand the real work activities with the contribution of end users of machinery.

Fabio Strambi[a] , Massimo Bartalini[a], Stefano Boy[b], Claudio Stanzani[c]

[a]A. USL 7-Siena, [b] ETUI-Bruxelles,[c] SindNova-Roma

Abstract

The “Feedback Method” has been designed specifically to collect the contribution of the end users of machinery for a reconstruction and understanding of how the work is actually performed. The acquired knowledge can help to improve technical standards, as well as the design, manufacturing and use of machinery.

The "Feedback Method" has been applied successfully - in collaboration with public authorities, market surveillance authorities and inspection bodies, social partners organizations and technical institutes - to different types of machines: woodworking machinery, forklift trucks, telehandlers, angle grinders, combine harvesters and tractors in seven european countries proving to be trans-nationally comparable.

The information collected with the "Feedback Method" can be used by: standardization committees and working groups of CEN, ISO to become aware of the problems relating to the real use of specific machines in different work contexts and thus to be able to draw up new or to revise existing standards accordingly; designers and manufacturers to produce better, more comfortable and safer machines and to provide precise instructions for their use; employers buyers to choose the best available machinery on the market; end users, employers, artisans and workers for training purposes and for defining appropriate work procedures; market surveillance authorities and inspection bodies to enhance their knowledge and improve the efficiency of their interventions and advices

Introduction

The European system of worker health and safety risk prevention and improvement on the worksite is based upon application of the so-called “Social Directives” (89/391 EEC) and subsequent or related directives,) as well as the “Product Directives” (such as, for example, the “Machinery Directive”- 89/392/EEC, - 2006/42/EC) [4], intended to ensure the free circulation of products, machinery and equipment within the European Community while ensuring high standards of intrinsic safety. For the purpose of permitting machine manufacturers, including very small undertakings, to comply with legislation while facilitating the application of the essential health and safety requirements contained in the Directives, the European Commission issues the so called “mandates” [17] to European Standards Organizations (ESOs), such as the CEN and CENELEC, for the elaboration of technical standards.

Standards are drafted in technical committees and their associated working groups, in which stakeholders make their own expert contributions on behalf of the various national technical bodies. In addition to the essential contributions from manufacturers measures are in place to ensure that other interests can contribute to the standardisation process, like end users (consumers, workers, etc.).

Periodic revision of each standard is required every 5 years, for the purpose of ensuring the updating necessary for adaptation to the advance of technology.

Nevertheless, despite objective improvements in levels of safety, many accidents within the European Union are still caused by the use of machinery, including machinery built in compliance with criteria defined according to current technical standards.

One of the more critical aspects remain the design and the further improvements of each technical standard taking account of the contribution of the end users; they are the precious source of information on the strengths and weaknesses of each machine when daily used in the different working context.

The workers/end users participation to the standardisation process is provided and recommended in many standards.

To this end, EN 614-1:2009 [5] stipulates that “for the assessment of ergonomics requirements and criteria, a careful analysis of feedback from the use of the machinery (e.g. end users' complaints, near-miss accident reports, accident reports) is strongly recommended. Feedback helps to identify measures and improvements for future design”.

This “strong” recommendation does not however explain with precision how the feedback is to be provided, but refers to reported complaints, near-miss accidents or accidents. Such data, however, do not always contain all the information required to review the machine design. As laudable and as worthy of maximum attention as such information is, it does not provide a global framework on the actual use of the machine and problems that may arise, and does not shed light on many problems erroneously considered “minor” but which, with time and intensive use, may become more serious.

EN 614-2:2009 [6], indicates that: “Final evaluation of the machinery and the tasks performed under operative conditions serves to provide feedback for forthcoming designs and to establish compliance with this and other relevant standards”

Often, the standards provide for the involvement of workers from the design phase through the use of prototypes, models and/or laboratory simulations.

Whenever possible [6], operators should be involved in these simulations and thus bring their own experience to the evaluation. The models and simulations have to be demonstrated to the operators in order to ask for their comments. They also have to be involved in the trials as test persons. The feedback from the operators can be obtained in various ways. The following methods are suitable for this purpose and shall be used where appropriate:

- group discussions;
- interviews,
- questionnaires;
- checklists;
- observational studies;
- analysing critical incidents.

If there is a project group, the task design shall be evaluated by it.

The results of the evaluation process shall be documented. If the established requirements have not been fulfilled, re-design of the tasks or the machinery or both shall be carried out".

In this respect, it is worth pointing out that simulations with machinery models and prototypes are:

- often confined to pre-defined environments which cannot reflect the actual work environment with its multiple variables;
- limited in temporal terms, whereas prolonged use of the machinery may in time lead to problems;
- limited to restricted circles of users that are not and cannot be considered as reliable and sufficiently heterogeneous samples of a population of real users.

The very fact of using machinery in a laboratory, and thus in a simulated context, inevitably conditions the ways it is used and the worker's capacity to respond, so the latter's impressions of the machinery will not be at all reliable.

It is not possible to foresee or to imagine, in the laboratory simulation, the contingent situations which may occur during the actual use, even when considering the variations that may occur in time, such as for instance, production time, need for supplies, administrative savings, unforeseen events, abnormal use, simplification of procedures, etc.

In reality, only the end-user in the field who has gained sufficient experience has the "means' to provide appropriate feedback that can be used for design improvements.

A number of observations made in ISO 6385:2004 [13], are of fundamental importance: "Where equivalent or similar systems already exist, this will also entail the identification of information regarding ergonomics problems occurring with these existing work systems, either from existing sources or from studies conducted for the purpose. Appropriate ergonomic methods and techniques for this purpose imply the use of evaluation tools for working conditions, observations on the spot, interviews, etc.;" "It is also necessary to continue to monitor the effect of the system in order to safeguard against longer-term deterioration in the performance or health of the users. The overall evaluation shall be carried out when the process is stabilised. This evaluation should consider the quality of work in order to create a healthy basis within working situations for long-term effective performance of workers".

Importance is accorded to the evaluation of the working conditions through observation at the workplace and the need to plan studies to that end with the involvement of workers in the actual environment of use. The standard moreover notes the need to evaluate the work systems, especially for ergonomic purposes, in time, and then to monitor the effects on the workers once put in use.

EN ISO 12100:2010 [14] that lists the information for risk assessment that has to be collected from the experience: "1) any accident, incident or malfunction history of the actual or similar machinery; 2) the history of damage to health resulting, for example, from emissions (noise, vibration, dust, fumes, etc.), chemicals used or materials processed by the machinery; 3) the experience of users of similar machines and, whenever practicable, an exchange of information with the potential users."

The same standard provides a schematic representation of the risk reduction process which includes a three-step iterative method. Each step reaches its conclusion by asking whether the planned risk reduction is attained. In reality, the answer to such a question is once again confined within the design process, whereas it could be provided in a more exhaustive and more concrete manner through the collection of experiences from actual users of not only similar machines but of the same machines already in use.

CEN 414-2004 guide [2]: "Safety of machinery —Rules for the drafting and presentation of safety standards", "Determination of the necessity for standardisation and/or for revision" asks if "Is there sufficient feedback on the use of the existing safety standard?"

The method for obtaining such feedback is not specified nor in this guide neither in other existing standards.

In 1997 the European Trade Union Confederation (ETUC) commissioned, through its own European Trade Union Institute (ETUI) a research study to develop a method capable of collecting the knowledge of workers who are expert users of machinery through job reconstruction with the various machines in the different very small and small European enterprises – a method that would yield concrete results within a reasonable period, with limited resources and with validated, verifiable and updatable instruments.

The results of this research were published [21] and described the "Feedback Method" designed by Fabio Strambi and developed together with Massimo Bartalini and collegue. This method is derived directly from the method used to conduct an ergonomic analysis of the organisational structure of work [16] [19] [22], to better understand the real work activities with the contribution of the workers, to identify critical points, and to make suggestions and provide solutions, which has been tried and tested in safety research studies and campaigns financed by the European Commission of Coal and Steel in the 1980s [20].

The "Feedback method", is a tool to study both the aspects involving ergonomics and safety requirements of the work activities with the use of machinery [15].

Methods

The "Feedback Method"(Fig. 1)

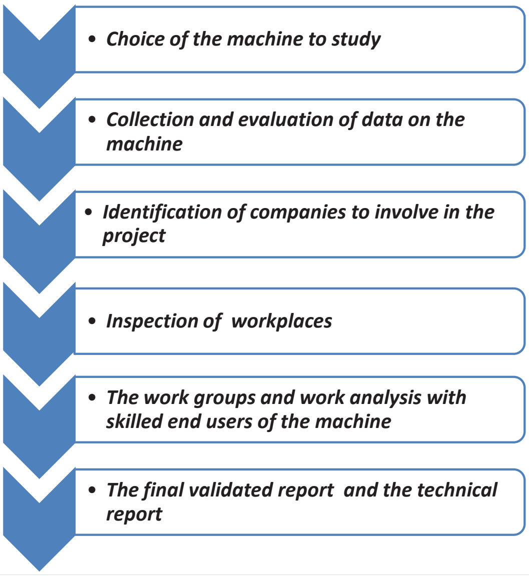

Choice of the machine to study
Collection and evaluation of data on the machine
Identification of companies to involve in the project
Inspection of workplaces
The work groups and work analysis with skilled end users of the machine
The final validated report and the technical report

Figure 1: "Feedback Method" flow chart.

Choice of the machine to study

The definition of a new standard or a revision of an existing one may represent a good motivation to choose the machine to analize by the means of the "Feedback Method".

Also the presence of a lack of the safety systems or of the ergonomics requirements of a machine together with the knowledge of the causation of major or fatal accident during its use may suggest to apply the "Feedback Method".

Sometimes the large diffusion of the machine and the specific interest of some stakeholders to acquire informations on how the real work with a specific type of machine is performed is the starting point for a study with the "Feedback Method".

Collection and evaluation of data on the machine

Safety experts/ researchers/ergonomists collect data concerning:

- diffusion of the specific machine in the different geographical area/ member state
- specific technical standards, reports, guidelines and any literature available, etc.
- accidents at work & incidents, included examples of relevant cases;
- market surveillance;
- instruction handbooks of machines from different manufacturers;
- other…

A dossier is collected to give evidence of the existing knowledge and experiences concerning ergonomics and safety of the machine

Identification of Companies to involve in the Project

Trade Unions, Employers Associations and safety experts collaborate to identify the companies that use the machine and are interested in participating to the study.

A collaborative atmosphere between employers/workers representatives and ergonomists is a prerequisite for a successful study; meeting on site are recommended.

Inspection of workplaces

Forms are compiled during inspection, containing the following details:

- general data of the company;
- work environment and work methods of the machine;
- technical features of the machine;
- accidents and near misses involving the machine;
- training provided to workers assigned to operate the machine.

The information collected is used during the work analysis that is carried out in working groups.

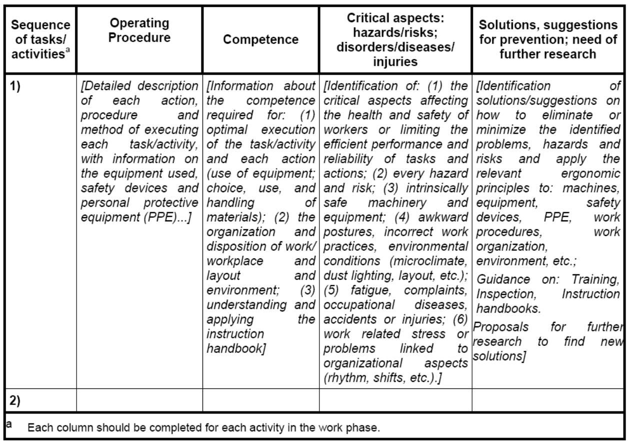
Each working group includes a selection of workers (skilled end users of the machine), from different companies, selected during the inspection.

The work groups and work analysis with skilled end users of the machine

Safety experts/ergonomists (facilitators) involved in the previous activities guide 7 to 9 skilled workers through each step of their own work activity, carried out with the machine. The work phases are drafted on a work group's form (Fig. 2). The basic operational tasks and activities are analysed for each work phase.

Main goals at this stage are:

- assessment of operating procedures and specific competencies requested to the operators;
- identification of risks, critical aspects and the possible need for a further investigation;
- gathering of suggestions for the improvement of safety and prevention.



Sequence of tasks/ activities[a]	Operating Procedure	Competence	Critical aspects: hazards/risks; disorders/diseases/ injuries	Solutions, suggestions for prevention; need of further research
1)	*[Detailed description of each action, procedure and method of executing each task/activity, with information on the equipment used, safety devices and personal protective equipment (PPE)...]*	*[Information about the competence required for: (1) optimal execution of the task/activity and each action (use of equipment; choice, use, and handling of materials); (2) the organization and disposition of work/ workplace and layout and environment; (3) understanding and applying the instruction handbook]*	*[Identification of: (1) the critical aspects affecting the health and safety of workers or limiting the efficient performance and reliability of tasks and actions; (2) every hazard and risk; (3) intrinsically safe machinery and equipment; (4) awkward postures, incorrect work practices, environmental conditions (microclimate, dust lighting, layout, etc.); (5) fatigue, complaints, occupational diseases, accidents or injuries; (6) work related stress or problems linked to organizational aspects (rhythm, shifts, etc.).]*	*[Identification of solutions/suggestions on how to eliminate or minimize the identified problems, hazards and risks and apply the relevant ergonomic principles to: machines, equipment, safety devices, PPE, work procedures, work organization, environment, etc.;* *Guidance on: Training, Inspection, Instruction handbooks.* *Proposals for further research to find new solutions]*
2)				

[a] Each column should be completed for each activity in the work phase.

Fig. 2: "Feedback Method" form used by the work group

Facilitators, following the scheme of the "Feedback Method" form, lead the group through the analysis of the ergonomic aspects related to the work with the machine. Active participation of all group members is highly encouraged. Facilitators keep a record, in writing, of the consensus of the group on each single statement.

In each group, workers describe their work experience, focusing on risks of procedures and operations related to their work assignment.

The final validated report and the technical report

At the end of the meeting the facilitators write a draft of the final report that is submitted to all participants. These are requested to give their feedback with an approval or a proposal for amendments.

Once all participants have validated the draft, the researchers/ergonomists prepare a final report on the study and a technical proposal for the amendment of the standards.

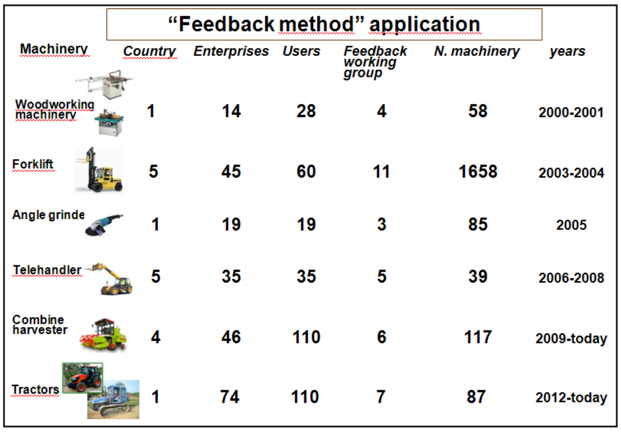
Suggestions for designers, manufacturers, employers-buyers, end-users and market surveillance authorities are also drafted.

Results

The "Feedback Method" has already been tested in different contexts with specific studies focused on various types of machinery. National public institution, market surveillance authorities, research institutes, trade unions, employers associations, individual expert end users, artisans and self employed persons and technicians, as well as ergonomist and occupational health physicians, have taken part to the application of the Feedback method" to these machines:

- woodworking machinery, circular saw [10], single-shaft vertical spindle molding machines [7];
- frontal forks forklift trucks [9];
- telehandlers [8];
- angle grinders [11];
- combine harvesters [12];
- tractors [3];

In the following figure (Fig. 3) is reported an overview of the "Feedback Method" application.



"Feedback method" application

Machinery	Country	Enterprises	Users	Feedback working group	N. machinery	years
Woodworking machinery	1	14	28	4	58	2000-2001
Forklift	5	45	60	11	1658	2003-2004
Angle grinde	1	19	19	3	85	2005
Telehandler	5	35	35	5	39	2006-2008
Combine harvester	4	46	110	6	117	2009-today
Tractors	1	74	110	7	87	2012-today

Figure 3: "Feedback Method" application.

Some examples of the main results obtained are hereunder described as reported in the Ergomach web site (https://ergomach.wordpress.com):

- Driver's cab and lubrication for Combine Harvesters
- Visibility for Telehandlers
- Pedals and restraint systems for Fork Lift Trucks
- Steps, hoist coupling and control, and cab for Tractors
- Use of controls for Angle grinders

Each example contains a description of the problem and of a possible improvement suggested by the end users.

Also the related specific detail of the form compiled by the "Feedback Method" work group of the end users is presented.

Combine Harvester:

Access to the driver's cab.

Users report that in certain working situations the first step may be too high, particularly on hillside combine-harvesters, making it appreciably difficult to climb onto and off the machine. In addition, some ladders are fitted with handrails that cannot be used easily owing to the absence of holding points. Ladders of the telescoping type also require substantial force to be lifted into the closed position, and present a greater risk of falling from the platform.

Possible improvements suggested by the end users

Use of ladders with a lower first step, fitted with suitable handrails with an adequate number of convenient holding points. Avoidance of the use of telescoping ladders, or at least reduction of the forces required for their use, thereby avoiding the risk of loss of balance.

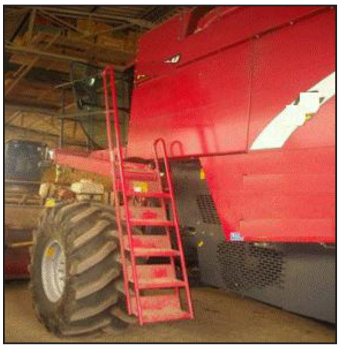


Figure 4: Combine harvester - ladders

Table 1: Extract from the "Feedback Method" form Combine – access to the driver's cab

Sequence of tasks/activities	Access to the driver's cab
Operating procedure	the operator enters the driver's cab using ladders and access platforms. The ladders, if not fixed, must be rotated or retracted by the operator into the position for work. They must be returned to their position for proper use by the operator when alighting.
Competence	Knowledge of the procedures for using the access ladder

Critical aspects: hazards/risks; disorders, disease - injuries.	Risk of falling owing to poor support, slipping or loss of hold. In certain operating situations (self-levelling machines parked on a slope), the height of the first step may be excessive, making it difficult or impossible to reach. Some types of ladders have handrails that are not easy to use owing to the lack of holding points. Telescopic ladders may present shear points if they are not properly opened. Some ladders require considerable effort in order to be lifted into closed position, and present a major risk of falling from the platform. Some types of platform do not provide sufficient room for movement, and lack protective guard rails.
Solutions, suggestions for prevention; need for further research	Reduce the height from the ground to the first step or make it adjustable, especially when the machine features a self-levelling system. The handrails must be suitable for use at all positions on the ladder: Sufficient convenient holding points must be provided. The telescopic ladder must be isuch that it cannot be used unless it is completely open. The ladders must permit use with minimal effort and with no risk of loss of balance. The access platforms must provide the operator with sufficient room to move safely and for the access door to the cab to be opened easily.

Lubrication

On some machines, the various lubrication points cannot be reached easily, requiring the operator to assume inappropriate or inconvenient positions and presenting a risk of injury to the head on fixed parts of the machine. The operators also report a greater risk of slipping or falling from higher points, owing to the need for the greasing equipment to be operated with both hands, thereby preventing the operators from supporting themselves using the normal holding points provided.

Possible improvements suggested by the end users

The users suggest improving the position of the lubrication points, reducing their number, relocating them to where they can be easily reached, and reducing the lubrication intervals.

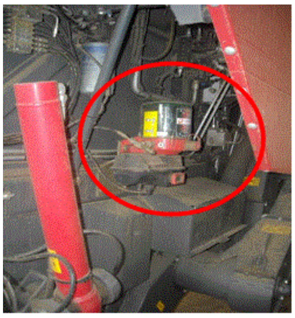


Figure 5: Combine harvester – lubrification point

Table 2: Extract from the "Feedback Method" form Combine – Greasing

Sequence of tasks/activities	Greasing
Operating procedure	The lubricant is injected at the various points indicated by the manufacturer by means of manual grease guns.
Competence	Knowledge of the lubrication points and the intervals required.
Critical aspects: hazards/risks; disorders, disease - injuries.	In some machines, the greasing points are located at a height and/or are not easy to reach, thereby increasing the risk of falling. It should be borne in mind that the worker uses both hands to operate the grease gun and cannot hold on to the handholds normally provided. On some machines, the greasing points are at inconvenient locations, requiring unsuitable positions to be assumed with unstable support and the risk of injury to the head on the fixed parts of the machine, or of slipping.
Solutions, suggestions for prevention; need for further research	Improve the position of the greasing points, even if only by regrouping and making them easily and safely accessible. Workers report the risk of losses in pipes with reduced lubrication efficacy, while ensuring that visual inspections are conducted during lubrication. Identify technical solutions that reduce the frequency of required lubrication.

Cab

During the work, excessive noise and dust is generated, and driving over uneven ground with the threshing apparatus running also gives rise to high vibration levels. Harvesting is frequently performed during the summer months, and is likely to be performed in high temperatures.

Possible improvements suggested by the end users

The operators indicate that well designed cabs equipped with air-conditioning and filters would reduce the exposure to noise, dust and extreme microclimatic conditions to acceptable Levels.

Figure 6: Combine harvester – Cab

Table 3: Extract from the "Feedback Method" form Combine –Treshing - Cab

Sequence of tasks/activities	Threshing
Operating procedure	The cutting height and the cutting and threshing speed are selected on the basis of the crop to be harvested (e.g. quantity of laid crop). They are adjusted by the operator using controls in the cab. The sifting units are started, then the cutting header, and then the machine is set in motion.
Competence	The user's manual for the machine is a vital source of basic knowledge needed for operation of the controls. Training is required for the avoidance of operating errors.
Critical aspects: hazards/risks; disorders, disease - injuries.	Excessive noise and dust are generated during the activity. Movement on uneven ground and the threshing equipment also cause considerable vibration. The threshing activity is often carried out during the summer period, possibly requiring work in hot weather.
Solutions, suggestions for prevention; need for further research	The operators indicate that well-designed cabs fitted with air-conditioning and filtering equipment reduce nuisance from noise, dust and extreme microclimatic conditions to within acceptable levels. The seats in the machines do not transmit excessive vibration. The operators hope that the fitting of adequate driver's cabs to all machines will become mandatory.

Cleaning of windows and mirrors

The glazed areas of the cab and the rear-view mirrors require frequent cleaning. Owing to the height of the harvesters, this task is associated with a risk of falling as a result of slipping or loss of grip, not least owing to the lack of adequate positions in which the tasks can be performed.

Possible improvements suggested by the end users

The positions from which access can be gained to the glazed areas of the cab must be improved by the provision for example of easily accessible platforms with handrails, which ensure optimum stability during the cleaning work and permit safe access to the entire glazed area of the cab.

Table 4: Extract from the "Feedback Method" form Combine –Cleaning windows and mirrors

Sequence of tasks/activities	Cleaning of windows and mirrors
Operating procedure	The glazed surfaces of the cab and the rear view mirrors must be cleaned externally as and when required and at least once per day. The area to be cleaned must be accessed via the header conduit, raised from the ground specially for that purpose. In some machines, the design of the cab requires the cutting header to be used for access.
Competence	Knowledge of the instructions in the operation and maintenance manuals.
Critical aspects: hazards/risks; disorders, disease - injuries.	Risk of falling or losing support owing to the need to access locations by assuming positions without sufficient stability, especially the upper part of glazed surfaces and the rear-view mirror not reachable from the cab access platform.
Solutions, suggestions for prevention; need for further research	Improve the automatic cleaning devices for glazed surfaces and mirrors by ensuring easily accessible positions that guarantee improved stability during the cleaning work and also safe access to the entire glazed surface of the cab. The use of antistatic detergents is recommended to reduce the deposit of dust.

Engine inspection

Checking the fluid levels and the serviceability of the engine requires access to the upper engine platform, with a greater risk of slipping and falling.

Possible improvements suggested by the users

Installation of secure walkways for access to the engine area, with a device connected to the access ladder which switches off the engine when the ladder is placed in position.

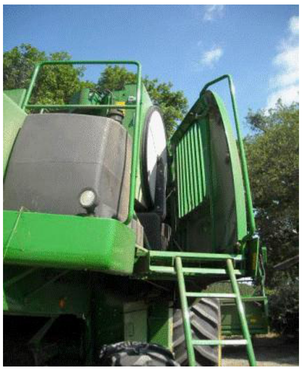


Figure 7: Combine harvester – Access to engine

Table 5: Extract from the "Feedback Method" form Combine – Engine inspections

Sequence of tasks/activities	Engine inspections
Operating	Performance of operating inspections

procedure	and checking the levels of engine fluids require access to the upper platform of the engine.
Competence	Knowledge of the intervals and of the inspections to be carried out. Knowledge of the manufacturer's instructions for accessing and standing safely on the engine platform.
Critical aspects: hazards/risks; disorders, disease - injuries.	Major risk of falling if the manufacturer's procedures are not followed. Risk of slipping when the access ladder and the platform are used.
Solutions, suggestions for prevention; need for further research	Establish secure means of access to the engine area, possibly from the platform of the driver's cab, so that the operator does not have to alight from the cab and gain access using another ladder (thereby avoiding the possibility of using unsafe access routes to reduce the working times).Some machines are equipped with a device connected to the access ladder which switches off the engine when the ladder is placed in position. Improve the steps, the handholds, the rails and the anti-slip features present on some models.

Telehandler:
Use of CCTV

Poor visibility during manoeuvring and during take-up of material on the forks is a key factor in the risk of collision or of persons being hit by the vehicle.

Possible improvements suggested by the end users

The adoption of auxiliary systems for improving visibility (such as CCTV) proposed by the users would reduce the risk to which the workers are exposed (Photograph 1: CCTV camera mounted on the forks).

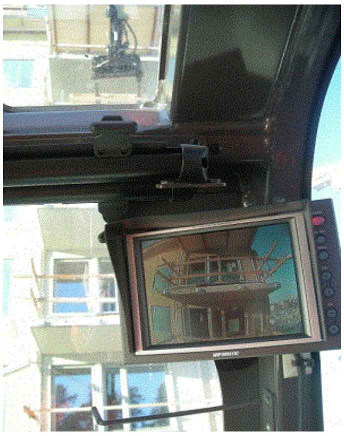


Figure 8: Telehandler – CCTV

Table 6: Extract from the "Feedback Method" form Telehandler - Visibility

Sequence of tasks/activities	Forward travel
Operating procedure	For movement of the vehicle, the arm is lowered to the rest position, forward gear is engaged, and the accelerator is depressed. The vehicle's direction of travel is determined by means of the steering gear according to the desired form of manoeuvre. With the aid of the mirrors and to some degree by leaning out of the window, the driver can observe the entire space surrounding the vehicle.
Competence	Knowledge of the position and form of operation of the forward/reverse selector, the controls for the arm, and the accelerator pedal. Training in and knowledge of the clearance around the vehicle. The clearance is not clearly visible in all directions from the driving position.
Critical aspects: hazards/risks; disorders, disease - injuries.	Incorrect manoeuvre with a risk of collision or of hitting pedestrians. Visibility to the right of the vehicle is reduced when the arm is raised. Risk of collision/hitting pedestrians.
Solutions, suggestions for prevention; need for further research	Systems must be in place which enhance visibility to the right of the vehicle. Precise definition of the methods for assessing the visibility from the driving position, and adoption of auxiliary systems for ensuring adequate visibility around the vehicle should this not already be the case.

Fork Lift Truck
Pedals

The workers report the specific risk of forklift truck pedals being operated incorrectly when vehicles from different manufacturers with pedal systems differing in their conceptual design are used alternately. Should action be taken in an emergency, in particular, instinctive operation of the pedals could result in serious error.

Possible improvements suggested by the end users

According to the users, the problem could be resolved by definition of a system of pedals and of a standard location for them for installation on all types of truck. Such a standard should make reference to the normal position of pedals in cars.

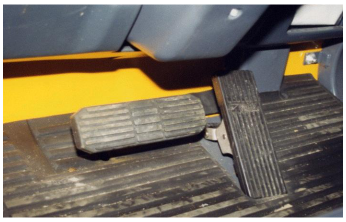


Figure 9: Fork lift – pedals

Table 7: Extract from the "Feedback Method" form Fork lift truks - Pedals

Sequence of tasks/activities	Travel with or without load
Operating procedure	Operation of the accelerator pedal.
Competence	Knowledge of and training in the use of the forward/reverse and brake pedals.
Critical aspects: hazards/risks; disorders, disease - injuries.	Error in operation of the pedals. The workers report a risk of the pedals being operated incorrectly when fork-lift trucks from different manufacturers are used alternately owing to the differences in conceptual design of their pedals.
Solutions, suggestions for prevention; need for further research	Definition of a system of pedals and of a standard location for them for installation on all types of truck. Such a standard should make reference to the expected position of pedals in cars, which are normally universal. Where action is taken in an emergency, instinctive operation of the pedals would involve a lower risk of error.

Restraint system at the driving position

Failure to use restraint systems at the driving position exposes workers to a higher risk of accident, possibly fatal, should the vehicle tip over. The users report that the safety belt restraining the wearer only at the waist is not used owing to its incompatibility with the need for the worker to enter and leave the vehicle continually.

Possible improvements suggested by the end users
The restraint systems for the workers at the driving position must be such that their use cannot be circumvented, and they must be effective and easy to use. Alternative systems are suggested, such as swivelling side bars or other containment structures which can be installed at the driving Position.

Table 8: Extract from the "Feedback Method" form Fork lift trucks – Restrain system

Sequence of tasks/activities	Layout of the driving position and initiation of movement.
Operating procedure	Accessing the seat and use of the restraint/safety device (fastening of the safety belt, use of the side bars, other devices, etc.)
Competence	Raising of awareness of use of the restraint systems at the seat that are intended to protect the driver in the event of an accident such that he remains within the safety cell formed by the roll-over cage.
Critical aspects: hazards/risks; disorders, disease - injuries.	Greater risk should the restraint systems at the driving position not be used. Risk of fatal accident should the vehicle tip over, owing to the driver leaving the safety cell.
Solutions, suggestions for prevention; need for further research	The restraint system at the driving position must be effective and be such that its use cannot be circumvented. The restraint system at the driving position must be straightforward to use, since given the fairly high frequency with which the vehicle is accessed and left, the obstruction to the work which it would otherwise present would result in its not being used. In this respect, it is reported that seatbelts providing restraint solely at the waist are not suitable. They are frequently not used. Alternative systems are proposed, such as swivel side bars or other containment systems. Finally, the manufacturers are advised to consider a range of systems, in order to enable the restraint or containment system to be installed that is best suited to the type of work to be carried out.

Tractors
Steps

Drivers frequently have mud on the soles of their shoes when accessing the driving position. The risk of slipping and falling off the tractor is greater.

Possible improvements suggested by the end users
The workers propose that gridded steps with strongly treaded surfaces be installed.

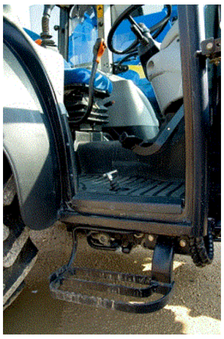


Figure 10: Tractor – Steps

Hoist with quick release coupling

During coupling of the attachments, the tractor must be brought close to the attachment several times to enable the latter to be connected to the rear hydraulic hoist. Owing to visibility problems, several manoeuvres are necessary for the tractor to be lined up with the attachment, with the driver repeatedly leaving and climbing back onto the vehicle; the procedure may also be performed by an operator on the ground, with an associated risk of being hit.

Possible improvements suggested by the end users.

To facilitate coupling of the attachment to the tractor, all hoists must be fitted with a quick-release coupling mechanism.

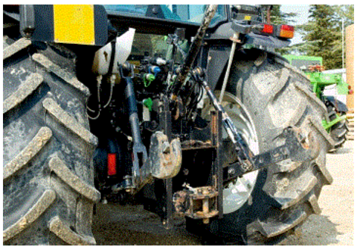


Figure 11: Tractor – coupling

Rear controls for the hoist

Operation (raising and lowering) of the hoist must also be possible by means of suitable controls located at the rear of the tractor close to the hoist.

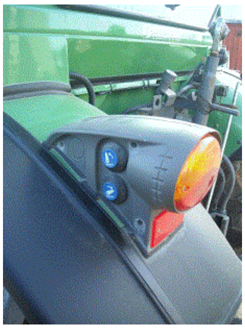


Figure 12: Tractor – rear controls

Cab

Many tasks are concentrated in the winter months, and work regularly involves the spreading of phytosanitary products. During the summer months, many soilworking tasks are performed. The workers report low temperatures in winter and high temperatures in summer during the performance of the tasks, and also exposure to noise, dust, vibration and chemical substances.

Possible improvements suggested by the end users

The users suggest that the fitting of cabs to tractors, whether wheeled or tracked, be mandatory. The cab must be fitted onto the tractor platform in order to reduce vibration and be equipped with air-conditioning, soundproofing, heating and with air filtration equipment suitable for excluding the dust and chemical substances.

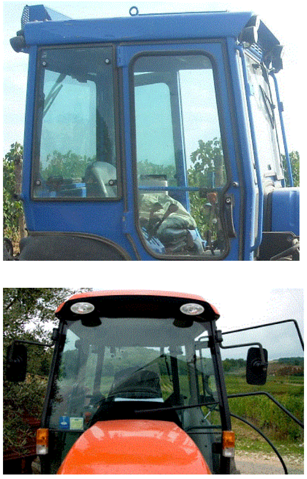


Figure 13: Tractor – Cabs

Angle Grinder
Controls

The users report that in certain working situations with the angle grinder in operation and the switch locked in the On position, the tool continues to rotate should the operator lose control of it, thereby presenting a hazard. Incidents have been reported in which the worker fell upon the angle grinder and it continued to rotate, injuring the worker.

Possible improvements suggested by the end users

Use of controls for the angle grinder which bring it to a halt should control be lost.

Figure 14: Angle Grinder - Foto: Fein Italia Srl

Table 9: Extract from the "Feedback Method" form Angle Grinder - switch "on"-"off"

Sequence of tasks/activities	Extended use of the angle grinder
Operating procedure	Should the angle grinder be used continuously or for long periods, the switch may be locked in the "On" position for this purpose. Actuating the switch again on any angle grinder disables the lock function and causes the machine to be switched off.
Competence	Training in the use of the switch for proper and swift de-energization of the machine.
Critical aspects: hazards/risks; disorders, disease - injuries.	A risk exists of contact with the tool whilst it is rotating at high speed should the worker lose control of it (the tool slips out of the hand).Loss of control may occur in a range of situations, through a slip, as a result of recoil caused by problems during cutting, through the worker falling or losing his balance, etc. Reports have been received of serious occupational accidents caused by situations such as the working falling upon the angle grinder whilst it was still running.
Solutions, suggestions for prevention; need for further research	Should the operator lose control of the tool, it should be de-energized and the cutting disc should very quickly stop rotating. A need is suggested for a device which stops the angle grinder within a short space of time when control is lost and the operating button therefore released.

Other main issues highlighted during the analysis of the work activities and of all the elementary tasks done using the different types of machine may be synthesized as under reported.

Critical aspects and suggestions for an improvements of the intrinsic ergonomics aspects and safety requirements of the machine and of its standard.

Standard makers, designers and manufacturers are primarily concerned.

- Stability- many major/fatal accident are caused by an overturning of different types of machine during activity on the field (Fig. ….) . The existing standars don't cover enough such a risk and additional solution are needed. The adoption of inclinometer/ alarm system, or other technical solutions are urgent.

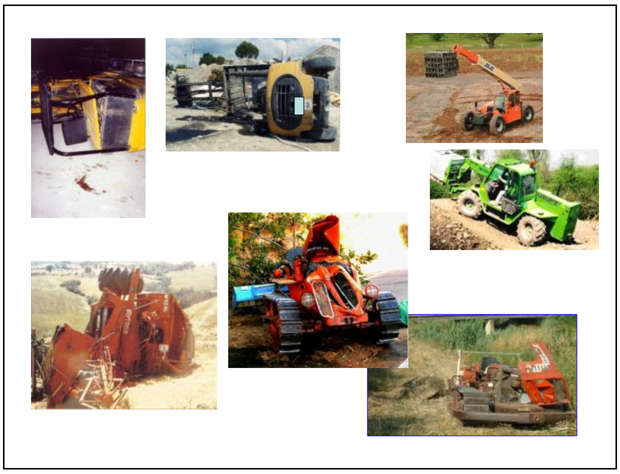


Figure 15: Stability

- visibility. a limited visibility during the work with telehandlers, fork lift trucks, combine harvesters and tractors is one of the main safety concern described during the "Feedback Method" work groups by the end users participants who suggested many possible solutions: better design of the cab, of the tools and of the machine and/or adoption of auxiliary system, CCTV included as illustrated in Fig.16.

Figure 16: Visibility: critical aspects and possible solutions.

- usability of protection devices Even if efficient the protection devices are not used by workers when representing an obstacle to the work activity and the productivity.The end users feedback is ineludible to understand how the real work is performed. In Fig … some examples of critical protection devices.

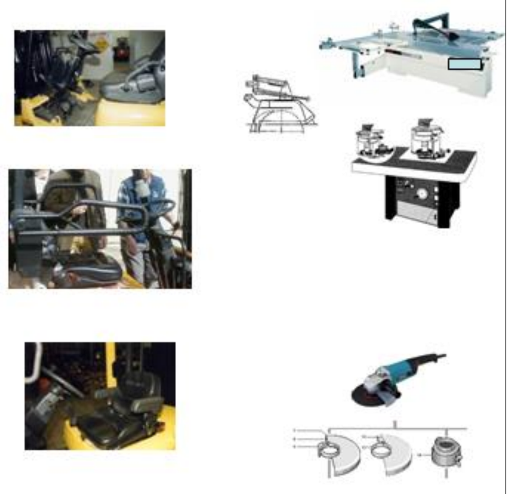


Figure 17: Protection deevices examples

- unification and improvement of control. Fig .. shows that different control systems are adopted for the same action in the same type of machines so determining an adjunctive risk of accident due to human error.

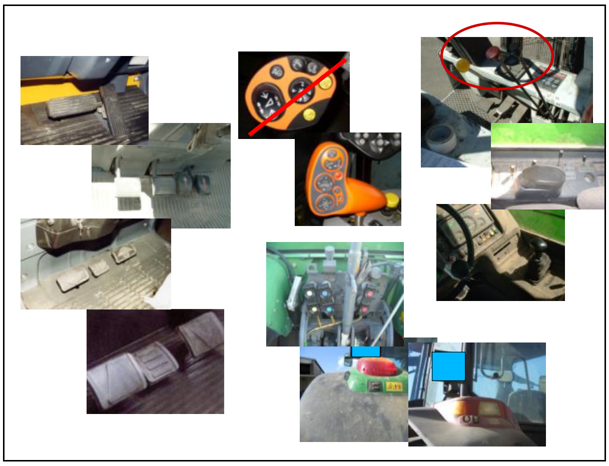


Figure 18: Unification of controls

- suitable dimensions; accessibility very often the dimensions and the accessibility are items not only related to ergonomics but also to the safety aspects and may be cause, if neglected, of accidents and sometimes foster also severe accidents

Further relavant aspects even if not directly linked to the design of the machine and its intrisic safety requirements are:

- Attachments, equipment and installation: with special attentio to their interface with the machine
- Maintenance: relevant safety and ergonomics aspects for both to preserve the original

requirements of the machine and to guarantee the activity performed by the maintenance workers)

Special attention of all the "Feedback Method" work groups of the different machines was paid to the need of improvements of the contents of the “use and maintenance handbook” (information and training, tutoring..) directed to standard-makers and manufacturers underlining:

- readability of the text
- completeness of the information on:the safe use of different type of tools (running, handling and fitting)
- Instruction to execute particular activities
- Problems associated with electrical supply and accessories
- Statement of noise emissions,vibrations and pollution produced in conditions for the intended or foreseeable use

In the reports of the different work group are always treated other arguments like: residual risks management, mode of machine use and worker behaviour/training/consciousness, details about work organization, spaces, additional protection, personal protective equipment, design and managing of special kind of activities

Discussion

Standardization process doesn’t facilitate the direct participation of end users and we risk losing an important opportunity to improve the application of ergonomic principles in the technical standards.

The “Feedback Method” has been designed and developed to gather the direct contribution of end users, to give informations and suggestions to designers, manufacturers and also to employers for the improvement of standards and health and safety of work [1] [18] [22] [23].

The “Feedback Method” has been developed to supply a concrete answer to difficulties of end users in transferring their knowledge and suggestions inside the standardization system. It provides a reliable and concrete method to all interested subjects (standardisers, designers, manufacturers and employers) for gathering the experience and knowledge of workers/craftsmen that use the machinery every day.

The “Feedback Method” fills in a gap in the technical standards; it provides a method that in many field studies (with the involvement of users of different companies and in different UE member states) has demonstrated to be low expensive and extremely reliable for:

- comparability of results obtained in different contexts and countries for similar machines;
- wealth of suggestions even for machinery of simple manufacture and usage (for example angle grinders) and specific answers to particular problems of context (for example, climatic differences, differences of manufacturing processes, etc.);
- simplicity of the method that, based on a deep technical knowledge of the standards and the literature concerning each specific machinery, needs only a short preliminary training for the operators who are going to apply it;
- applicability in small and medium enterprises (the method has been experimented mainly with workers/ coming from small and medium enterprises and even with the participation of craftsmen and small businesses employers).

The involvement of European Trade Union Institute and institution as Kan, HSE, ISPESL/INAIL, market surveillance bodies, Ministry, and Social Partners association in the “Feedback Method” applications during 10 years ha demonstrated its validity and value.

Conclusion

The “Feedback Method”confirms the need to integrate machinery design with information based on the real experience of machinery operators so as to improve its quality and reliability.

The application of “Feedback Method” to machinery highlights what lessons standards bodies could learn from participatory approaches to equipment design based on the knowledge that final users possess on the equipment they work with.

Application of the The “Feedback Method” method makes it possible both to collect contributions from machinery users for the improvement of the specific reference standard and at the same time to prepare a system to monitor the effectiveness of any improvements introduced. In connection with this method an optimal solution would be the establishment of “observatories”, located in several Member States, able to collect reactions from users of the same machine in different production sectors. Already exiting network of people able to apply feedback.

Such a system of continuous feedback, between standard-setters and users, is therefore the only viable method – derived moreover from human physiology – of achieving and maintaining an improvement in safety and in health safeguards for machinery users/workers, by means of a continuous adaptation of the standards.

Using this method it is possible for worker representatives or, more generally, for representatives of consumers and users to set about collecting indications for improvements in various types of machinery.

The recommendations can then be forwarded to the appropriate technical commissions and committees.

The key factor for the effectiveness of the method, however, is the human factor and above all else the full cooperation of expert users and technicians. They must not only be familiar with the machine under investigation but also be able to guide the working group, collect the information and express it in suitable language for the formulation of proposals to be addressed to the standard-setters and manufacturers.

References

[1] S.Boy “A European system to improve machinery safety by drawing on users' experience”. ETUI; Brussels, 2006.

[2] CEN Guide 414 “Safety of machinery - Rules for the drafting and presentation of safety standards”, 2004.

[3] Commission Directive 2014/44/UE amending Annexes I, II and III to Directive 2003/37/EC of the European Parliament and of the Council on type-

approval of agricultural or forestry tractors, their trailers and interchangeable towed machinery, together with their systems, components and separate technical units.

[4] Directive 2006/42/EC of the European Parliament and of the Council on machinery,17 May 2006.

[5] EN 614-1:2006+A1:2009 "Safety of machinery - Ergonomic design principles - Part 1: Terminology and general principles".

[6] EN 614-2:2000+A1:2008 "Safety of machinery - Ergonomic design principles - Part 2: Interactions between the design of machinery and work tasks".

[7] EN 848-1:2007+A1:2009 "Safety of woodworking machines - One side moulding machines with rotating tool - Part 1: Single spindle vertical moulding machines".

[8] EN 1459:1998+A2:2010 "Safety of industrial trucks - Self- propelled variable reach trucks".

[9] EN 1726-1:1998+A1:2003 "Self-propelled trucks up to and including 10000 kg capacity - Part 1:General requirements".

[10] EN 1870-1:2007+A1:2009 "Safety of woodworking machines - Circular sawing machines - Part 1: Circular saw benches (with and without sliding table), dimension saws and building site saws".

[11] EN 50144-2-3:2002 "Safety of hand-held electric motor operated tools - Part 2-3: Particular requirements for grinders, disk type sanders and polishers".

[12] EN ISO 4254-7:2009 "Agricultural machinery - Safety - Part 7: Combine harvesters, forage harvesters and cotton harvesters".

[13] EN ISO 6385:2004 "Ergonomic principles in the design of work systems".

[14] EN ISO 12100:2010 "Safety of machinery - General principles for design - Risk assessment and risk reduction".

[15] ISO/TR 22100-3:2014 Implementation of ergonomic principles in safety standards – Bridging document.

[16] B.Maggi, A.Grieco "Il metodo delle congruenze organizzative per lo studio dei rapporti tra lavoro organizzato e salute. Un esempio di applicazione nel settore metallurgico" – Atti del Convegno "Aspetti emergenti dei rischi della metalmeccanica leggera", pag. 161. Poggibonsi, Italia, 1986.

[17] Mandate to CEN and CENELEC for standardisation in the field of machinery. M/396 EN. Brussels, 19 December 2006.

[18] F.Strambi, M.Bartalini, R.Cianotti, M.N.Tini, C.Stanzani "Feedback: a method to collect the contribution of machinery users in order to improve the quality of design standards". Proceedings ISSA. Nice, 2006.

[19] F.Strambi, G.Battista, A.Franzinelli "Salute e lavoro nel settore estrattivo: esperienze di formazione alla sicurezza" - Atti del convegno "Materiali lapidei, tematiche di prevenzione e produzione", pag. 257. Morbegno, Maggio 1987.

[20] F.Strambi "Ergonomia e sicurezza in miniera: il contributo dell'azione comunitaria europea" – Atti del Convegno Nazionale "Lavoro e salute in miniera ed in cava". Massa Marittima (GR), 5 e 6 Dicembre 1991.

[21] F.Strambi, C.Stanzani, M.Bartalini, M.Cucini "Ergonomia e norme tecniche di sicurezza: il contributo degli utilizzatori". Editore Franco Angeli. Milano, 2001.

[22] F.Strambi, F.Valentini, G.Battista "Esperienze di formazione alla sicurezza nel settore lapideo" – Atti del Congresso Internazionale "Sviluppo produttivo e rispetto delle risorse umane nell'estrazione e lavorazione dei materiali lapidei", pag. 228. Siena, 14 Novembre 1986.

[23] F. Strambi, M. Bartalini, S. Boy, R. Gauthy, R. Landozzi, D. Novelli and C. Stanzani - End users "Feedback" to improve ergonomic design of machinery . A Journal of Prevention, Assessment and Rehabilitation, Volume 41, Supplement 1/ 2012, pagg. 1212-1220 (DOI: 10.3233/WOR-2012-0305-1212)

Crawling beneath and bypassing of three-dimensional detection zones on machines – Can the normative provisions be applied to modern protective devices such as camera systems?

Michael Hauke[a], Birgit Naber[a], Thomas Bömer[a], Markus Koppenborg[a], Dr Michael Huelke[a]

[a] *Institute for Occupational Safety and Health (IFA), Sankt Augustin*

Abstract

Adequate safety distances protect operators against hazards on machinery. These distances may be enforced by technical means, for example by electro-sensitive protective equipment (ESPE). Depending upon the technology, this equipment may be able to monitor detection zones of different geometries. The existing normative provisions govern only ESPE with a one-dimensional or two-dimensional detection zone (such as light barriers or laser scanners). Modern items of ESPE such as camera systems are characterized by having three-dimensional detection zones that can be adapted flexibly to the hazard zones. Owing to unavoidable measurement errors however, a minimum distance must be observed between the detection zone and fixed perimeter elements such as the floor or walls. Does this result in a gap through which undetected bypassing of the detection zone is possible?

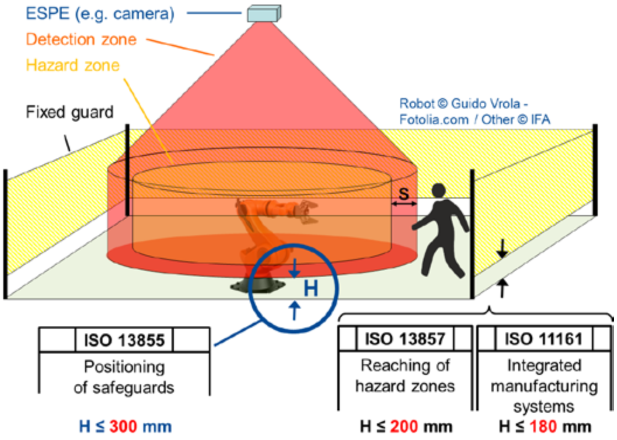
This problem was studied systematically on 43 schoolchildren serving as test subjects and a height-adjustable measurement facility. The majority of test subjects were able to crawl undetected for a distance of 2 m beneath detection zones with the maximum height of 300 mm above floor level, the height defined in the standards. Similar results were obtained for bypassing of the detection zones to the side along a wall. This paper is intended to stimulate discussion of the results with regard to their relevance for industrial practice and clarification of the normative provisions.

Keywords:

bypassing, crawling zone, access beneath or to rear of safety zones, safety distances, electro-sensitive protective equipment (ESPE), non-contact, protective devices, machines, hazard zones, detection zone, safety zone, camera system, vision system, work zone, approach, position, velocity, resolution, usability, ergonomics, manipulation, robots, laser scanners, circumventing, access

Introduction

Electro-sensitive protective equipment (ESPE) is used in order to safeguard hazard zones on machinery (see Figure 1). EN ISO 13855 [1] governs the location of protective equipment and the required safety distances (S); as yet however, it has largely been geared to ESPE with one-dimensional or two-dimensional detection zones (light barriers, light curtains, laser scanners, etc.). Modern camera-based ESPE is also able to monitor three-dimensional detection zones. In order to assure adequate availability however, such three-dimensional detection zones must observe a minimum distance from fixed perimeter elements such as the floor, walls or fences. The principle of operation would otherwise cause the perimeter elements to be detected as objects within the detection zone, thereby leading to unwanted tripping. The distance H between the boundary of the detection zone and the fixed perimeter element must however be engineered so small as to prevent crawling beneath the detection zone or bypassing it to the side. Undetected bypassing of the detection zone in the direction of the hazard zone cannot otherwise be excluded. Further standards [2, 3] setting out similar requirements for guards are listed in Figure 1 and Table 1.



Robot © Guido Vrola - Fotolia.com / Other © IFA

Figure 1: Floor clearance of three-dimensional detection zones (H = maximum clearance between floor and detection zone; S = safety distance)

The Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) was tasked by the German Social Accident Insurance Institution for the woodworking and metalworking industries (BGHM), test and certification body lifts, safety components and machines, with studying the following problems:

Can the distance H between the detection zone and fixed perimeter elements such as the floor, walls or fences be increased for modern forms of ESPE with three-dimensional detection zone?

This increase was based upon the assumption, which was be tested, that crawling beneath a more extensive detection zone is more difficult than crawling beneath a light beam.

What speed of motion (crawl or bypassing speed) must be assumed in this context?

The speed of motion is relevant for the following reason: adjacent to the borders of the detection zone, in which the probability of objects being detected is adequate, lies a tolerance zone. Within the tolerance zone, the probability of objects being detected is inadequate. The statistical scatter of the sensor data leads to an object present for longer within the tolerance zone having a greater probability of being detected. The assumed speed of movement and the resulting duration of presence within the tolerance zone are therefore important parameters for the statistical analysis.

Table 1: Overview of current normative requirements

Reference	Application	Requirement
EN ISO 13855, Section 6.2.2 a) [1]	**Light curtain**, maximum height H of the lowest light beam above the reference plane (e.g. the floor)	**H = 300 mm for industrial applications** (persons aged 14 and over), **H = 200 mm for non-industrial applications** (including children aged up to 14)
EN ISO 13857, Table 7 [2]	**Fixed guard**, reaching through slotted apertures	Slotted apertures of width greater than 180 mm permit access to the entire body
EN ISO 11161, Section 8.5.2 [3]	Integrated manufacturing systems, design of guards	The distance between guards and the floor must not exceed 200 mm.

Methods

Crawling beneath the detection zone

Crawling beneath three-dimensional detection zones was performed in a pilot study involving ten adults from the IFA and a follow-on main study involving 43 young people (two school classes) aged at least 14 (representing the worst-case scenario to EN ISO 13855, Section 1, Note 2). The test subjects had the task of crawling beneath three-dimensional detection zones of two different lengths and of five successively decreasing heights above the floor.

The length of the detection zone to be crawled under in the direction of movement (described below as the "detection zone length") was measured in two different variants:

- 0.2 m as the minimum reasonable detection zone length: modern, camera-based 3D ESPE products have a detection capacity of 200 mm, i.e. objects with a dimension of at least 200 mm are reliably detected (suitable for detection of persons).
- The maximum detection zone length of 2.0 m is selected in consideration of the length of the human body: at lengths greater than this, the process of movement is repeated during crawling beneath the detection zone, so results are not expected to differ.

For the main test, the test pattern shown in Table 2 was followed, involving eight passes of successively increasing difficulty. A possible training effect was deliberately tolerated, since this is also to be expected in industrial practice. The task of crawling beneath the detection zone was to be performed with the primary objective of not violating the detection zone and with the secondary objective of crawling as quickly as possible.

Table 2: Test arrangement of the detection zones showing lengths and heights above the floor

Height H in mm	Length = 0.2 m	Length = 2.0 m
400		1. Measurement
350	2. Measurement	3. Measurement
300	4. Measurement	5. Measurement
250	6. Measurement	7. Measurement
200	8. Measurement	

The course of the test is outlined in Figure 2. Track 1 shows the start, track 2 the finish at 0.2 mm into the detection zone, track 3 the finish at 2.0 m into the detection zone.

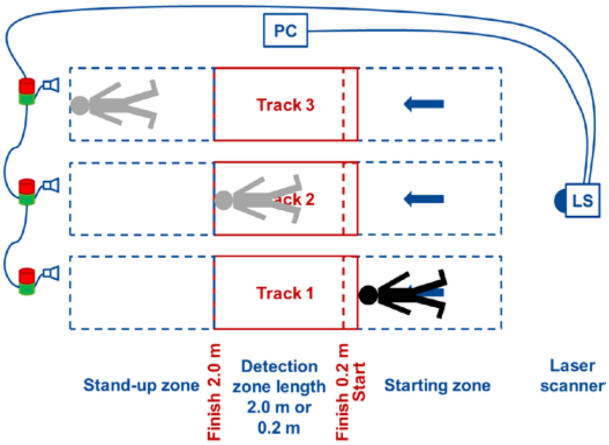


Figure 2: Arrangement of the tracks and test procedure

Figure 3 shows the arrangement of the main test. This enabled three parallel tracks with separate optical and acoustic feedback (round flashing lights and buzzers) to be implemented. When a violation ceased again during measurement, the signal was also cancelled (automatic reset). In addition to reducing the overall time required for the test, simultaneous crawling by multiple test subjects led to a competition situation that provided additional motivation for the test subjects.

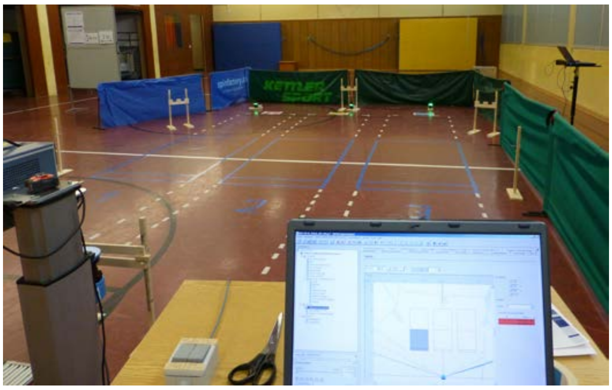


Figure 3: Test arrangement in a school sports hall

For the required sensing of the detection plane, a laser scanner (Sick AG Waldkirch, type LMS 500-20000) was employed mounted upon a height-adjustable stand (see Figure 4).

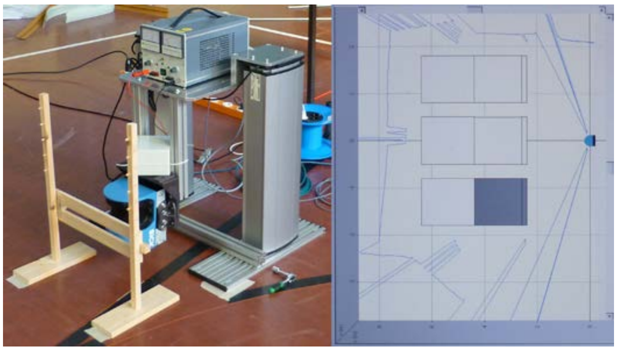


Figure 4: Height-adjustable laser scanner and screenshot of the analysis software

This measurement arrangement had the following advantages:

- Automatic monitoring of the plane true to +/- 15 mm
- Logging of violations of the detection zone
- Automatic changeover of the detection zone length
- Precise height adjustment by electrically extending columns

To compute the crawl speed, the instant of the collective starts and of individual reaching of the finish were logged manually on a separate PC (Figure 3, upper right corner). Compared to industrial floors at workplaces on machinery, crawling on the floor of the school's sports hall was easier and more comfortable. The results obtained here therefore represent an estimation on the safe side for real-case industrial environments.

Bypassing to the side

In a second step, the test involving the adult test subjects from the IFA was extended to consider bypassing of the detection zone to the side between the detection zone and fixed vertical perimeter elements such as walls and safety fences.

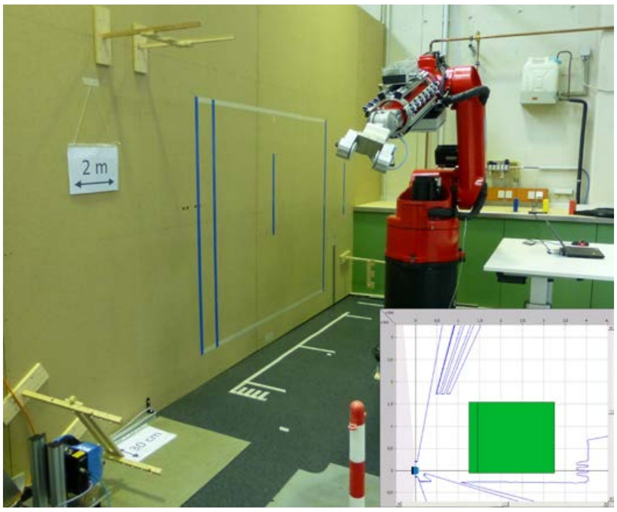


Figure 5: Test arrangement for bypassing to the side and screenshot of the analysis software

Bypassing to the side was tested at the IFA's site along a vertical wood-panelled wall (see Figure 5). The distance between the detection zone and the wall ("width") was varied in this case with the values shown in Table 2 in the same way as the distance between the detection zone and the floor ("height") during the crawl test. For this purpose, the laser scanner was mounted on an optical bench at right angles to the wall. For measurement of the bypassing speed, the test subjects began the test standing with their backs against the wall directly in front of the starting line. According to the length of the detection zone, measurement ended once a finishing marker was reached at a distance of 1.0 or 2.5 m beyond the starting line (the starting and finishing lines are shown marked in blue in Figure 5).

In order for possible influences of physical stature and fitness to be taken into account during crawling beneath detection zones and bypassing them to the side, the body height was measured by means of an anthropometer and waist girth by means of a tape measure to DIN 33402-1 [4]. The test subjects also completed a questionnaire concerning physical fitness with questions regarding their own assessment of their enjoyment of sport, their physical fitness and mobility, and also regarding the sports that they actively practised, with what frequency, and how formally. Further information on the questionnaire and the respective results is available at the IFA.

Test subject collective

The ten test subjects from the IFA, i.e. those conducting the pilot study on crawling beneath the detection zone and the test on bypassing it to the side, were all male and had an average height of 179 cm (min.: 170 cm, max.: 193 cm). The majority of the test subjects were above the 50th percentile of 175 cm of the population of Germany in accordance with DIN 33402-2 [5]. The test subjects had an average weight of 77.7 kg (min.: 61 kg, max.: 86 kg). This value is below the 50th percentile of 79 kg in accordance with DIN 33402-2.

43 test subjects took part in the main study. Of these, 24 were male, 19 female. Their ages ranged from 14 to 17 (average 15.4 years ± 0.7). They were recruited from two Year 9 school classes (N_A = 24; N_B =19) at a school located close to the IFA in Sankt Augustin. The individual values for body height and waist girth were compared with anthropometric reference values for children and young people in Germany (KiGGS, 2013) [6] for the relevant age group. The resulting distributions of the percentiles are shown in Figure 6, and indicate that the group is a representative random sample that is a little shorter (dark blue columns) and has a slightly greater waist girth (light blue columns) than the statistical population (black line).

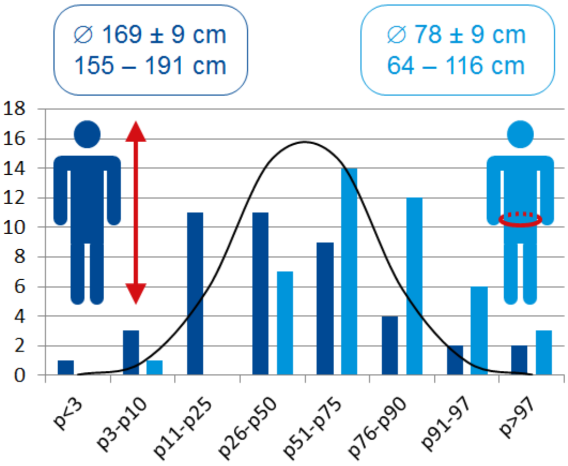


Figure 6: Body height and waist girth of the test subjects in the main test (percentiles)

The test subjects were very cooperative and disciplined during all tests. Only where H = 250 and 200 mm did some test subjects complete the pass as quickly as possible after establishing that they had no chance of crawling beneath these low heights. Participation by two classes in the same year created an element of competition that led to additional motivation among the test subjects.

Results

Violations of the detection zone

It was frequently observed that after violating a detection zone during one pass, a test subject did not violate it during a subsequent pass under more difficult conditions (i.e. a lower height of the detection zone above the floor, or greater length). Sporadic outliers were one cause; a clearly noticable training effect was another. Figure 7 therefore shows, individually for each test subject, the lowest height/smallest width in the various tests at which the test subject was able to crawl beneath the detection zone or bypass it to the side undetected. Differentiation by detection zone length is shown by the colour: light blue indicates that at the height/width in question, only the short detection zone length was successfully completed, whereas dark blue indicates that the long detection zone length was completed successfully.

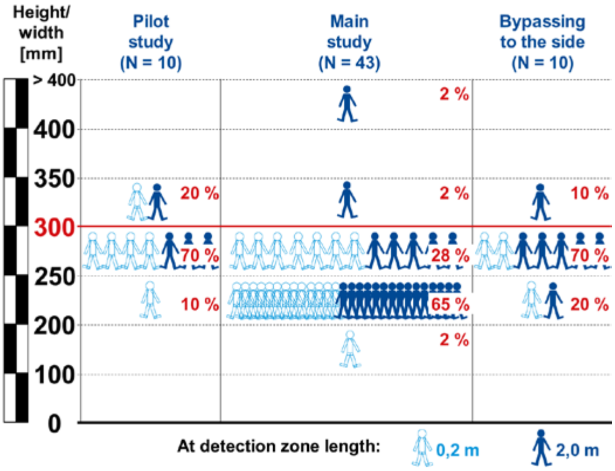


Figure 7: Lowest individually navigated height or width

Virtually no detection zone violations occurred in any tests at heights/widths exceeding 350 mm. Violations of the detection zone were noted in the pilot test only once the height above the floor had been reduced below 350 mm. Eight of the ten test subjects crawled beneath a detection zone height of 300 mm over a length of 0.2 m without violating the detection zone; of these, only four were able to do so for the same height over a length of 2 m. One test subject successfully completed a further pass at a height above the floor of 250 mm and length of 0.2 m.

The results of the main study showed clearly that almost all test subjects (41 of 43) were able to crawl beneath a height of 300 mm. A height of 250 mm was also not an obstacle for the majority (29 of 43). Not until the height above the floor was reduced to 200 mm was only one test subject still able to crawl beneath the detection zone. The test subject concerned had unusually small body dimensions.

The results for bypassing to the side were very similar to those for crawling beneath the detection zone. Nine of the ten test subjects were able to bypass a gap of 300 mm to the side undetected. Of the adults, two were able to bypass a gap of 250 mm, and none a gap of 200 mm.

In addition to the description of the detection zone violations, calculations were conducted for analysis of the variance. These are shown in greater detail in [7, 8].

Duration and location of the detection zone violations

The duration of detection zone violations was studied more closely during the main study and during bypassing to the side. The proportion of detection zone violations of longer duration was seen to rise with increasing difficulty of the test (smaller gap, longer detection zone). At H = 200 mm, 42 of the 43 young people violated the detection zone for at least two seconds. Only one test subject failed to violate the detection zone at all.

Analysis of the covariance of the results showed the duration of detection zone violations to be particularly influenced by the height of the detection zone above the floor, its length, and the subjects' waist girth. Specifically, the test subjects with a greater waist girth violated the detection zone longer when the height of the detection zone above the floor was lower and the length of the zone greater. Where the persons were physically capable of passing beneath the detection zone, the length of the zone was of only secondary importance.

Evaluation of the positions at which the detection zone was violated revealed an accumulation immediately at the starting-line, particularly at the detection zone heights/widths of 250 mm and 200 mm. Under these circumstances, the test subjects were apparently incapable of bypassing the detection zone at this height or width at all, owing purely to their body dimensions. As a result, the detection zone was violated continually over its entire length. Further violations of the detection zone in the direction of crawling appear to be more evenly distributed, exhibiting no accumulations over longer crawl distances.

Speed of movement

The pilot study showed that the crawl speed fell significantly with decreasing height of the detection zone above the floor. The difference between the two detection zone lengths was not significant. All crawl speeds lay between approximately 0.1 and 0.4 m/s.

The crawl speed in the main study was also analysed for covariance. One observation was that test subjects crawled significantly faster at greater detection zone heights above the floor, and that test subjects with greater enjoyment of sport were faster. On long detection zones, crawling was slower at lower detection zone heights than at medium heights.

Figure 8 shows the descriptive results for the main study for crawling beneath the detection zone as a mean value (light blue bars) with standard deviation (error bars). Whether or not the detection zone was violated in a pass had only a very small influence upon the crawl speed.

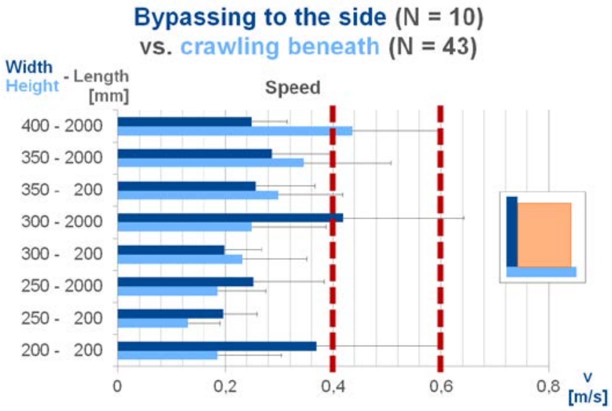


Figure 8: Statistics for the crawl and bypass speed v

The crawl speeds lay between approximately 0.1 and 0.6 m/s. Within the interesting height range of H ≤ 300 mm, the mean value plus standard deviation permits the maximum speed (worst case) to be estimated at approximately 0.4 m/s. The crawl speed observed here is approximately double that observed in the pilot study. This difference could be attributable to differences between the test subject collectives (for example in terms of age and mobility) and differences in floor properties (concrete floor vs. sports hall floor).

The speed of movement for bypassing of the detection zone to the side was determined in the same way and is also shown in Figure 8 (dark blue bars). The maximum speed for bypassing of the detection zone to the side can be estimated following the same principle at up to approximately 0.6 m/s. The speed of movement for bypassing to the side can thus be assumed to be approximately 50% higher than for crawling beneath the detection zone.

Discussion

The collective of 43 test subjects studied in the main test is representative in terms of their body height and waist girth. The pilot study and main study of crawling beneath the detection zone yield similar results. The supplementary test of bypassing to the side also yields comparable results, except with regard to the speed of movement. The main results of the tests can be summarized as follows:

- Almost all test subjects (41 of 43 and 9 of 10) were capable of crawling beneath a detection zone height of 300 mm or of bypassing a gap of 300 mm to the side.
- A height of 250 mm was also not an obstacle for the majority of the young test subjects (29 of 43). Of the ten adults, only one was able to navigate this gap successfully. Not until the height H was lowered to 200 mm was only a single young test subject still able to crawl beneath the detection zone.
- At heights of H ≤ 300 mm, the crawl speed can be estimated from the main study as being up to 0.4 m/s (on the safe side). For bypassing to the side, the corresponding value is 0.6 m/s.

Conclusion

An increase in the maximum distance H currently stated in EN ISO 13855 between the detection zone and fixed perimeter elements such as the floor or walls does not therefore appear justified.

The project results were also published in a DGUV informative publication issued by the woodworking and metalworking expert committee [9]. This publication also states that the design principles for detection zones and the dimensioning of safety distances in the current version of EN ISO 13855 can also be applied to three-dimensional detection zones. Plans are for the results of the study to be submitted to the responsible standards committee.

References

This article was first published in German language in Technische Sicherheit Vol. 4 (2014) No 7/8 pp. 38-42 (www.dguv.de/medien/ifa/de/pub/grl/pdf/2014_096.pdf).

[1] EN ISO 13855:2010, Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body

[2] EN ISO 13857:2008, Safety of machinery – Safety distances to prevent hazard zones being reached by upper and lower limbs

[3] EN ISO 11161:2007 + A1:2010, Safety of machinery – Integrated manufacturing systems – Basic requirements

[4] DIN 33402-1:2008, Ergonomie - Körpermaße des Menschen - Teil 1: Begriffe, Messverfahren. Berlin: Beuth 2008

[5] DIN 33402-2:2005 + Berichtigung 1:2007, Ergonomie - Körpermaße des Menschen - Teil 2: Werte. Berlin: Beuth 2005, 2007

[6] *Neuhauser, H.; Schienkiewitz, A.; Schaffrath Rosario, A.; Dortschy, R.; Kurth, B.M.*: Beiträge zur Gesundheitsberichterstattung des Bundes. Referenzperzentile für anthropometrische Maßzahlen und Blutdruck aus der Studie zur Gesundheit von Kindern und Jugendlichen in Deutschland (KiGGS). 2nd extended edition. Berlin: Robert Koch-Institut 2013 (www.rki.de/DE/Content/Gesundheitsmonitoring/Gesundheitsberichterstattung/GBEDownloadsB/KiGGS_Referenzperzentile.pdf?__blob=publicationFile)

[7] *Naber, B.; Hauke, M.; Nickel, P.; Koppenborg, M.; Huelke, M.*: Schutzeinrichtungen mit 3D-Schutzräumen an Maschinen: Überprüfung der Unterkriechbarkeit. 60th Congress of the GfA, pp. 82-84. Dortmund: Gesellschaft für Arbeitswissenschaft 2014 (www.dguv.de/webcode/m642197)

[8] *Naber, B.; Hauke, M.; Nickel, P.; Koppenborg, M.; Huelke, M.:* Unterkriechen von 3D-Schutzräumen an Maschinen: Ist die Anhebung des Schutzraumabstands zum Boden möglich? Psychologie der Arbeitssicherheit und Gesundheit, pp. 55-58. Kröning: Asanger 2014

[9] DGUV-Information des Fachbereichs Holz und Metall No 072 „3D-Schutzraum: Anordnung der BWS“. Mainz: 2014 (www.dguv.de/webcode/d131683)

Corresponding address

Institute for Occupational Safety and Health (IFA), Alte Heerstrasse 111, 53757 Sankt Augustin, Germany,
www.dguv.de/ifa

Current situation of safety assessor and safety basic assessor (SA/SBA) qualification system: Reduction of accidents achieved by a Japanese company and recommendation by Japanese Ministry of Health, Labour and Welfare

Toshihiro Fujita[a], Masaru Shiomi[a], Kimitada Ishikawa[a], Shunsuke Nonaka[a], Hiroo Kanamaru[a], Masahiro Tochio[b], Masahiko Ariyama[b], Koji Sagawa[b], Hiroyuki Takaoka[c], Akikazu Kuroda[c], Masao Mukaidono[d,e]

[a] *Nippon Electric Control Equipment Industries Association (NECA)*
[b] *Japan Certification Corporation (JC)*
[c] *Asahi Glass Co., Ltd.*
[d] *Meiji University*
[e] *The Society of Safety Technology and Application, Japan (SOSTAP)*

Abstract

A lot of standards for machinery safety have been developed as ISO or IEC standards, and new standards are being developed. Many manufacturers and users of machines find it difficult to understand the international standards and practical methods to establish safe system. Hence, the Nippon Electric Control Equipment Industries Association, Japan Certification Corporation, and the Society of Safety Technology and Application, Japan, established the safety assessor (SA) and safety basic assessor (SBA) qualification systems in 2004 and 2009, respectively, to develop a workforce that understands international safety standards and machine safety.

The system has been adopted in diverse companies including automobile industry, with SA/SBA certification rising to 8,364 people (921 companies) in the last decade. Recognizing increase of assessors and good reputation, Japanese Ministry of Health, Labour and Welfare cited the SA/SBA in its April 2014 notice for education of design and manufacturing engineers. The SBA system has spread to seven Asian countries and expand globally in future.

Asahi Glass Co. Ltd. (AGC), a world-leading glassmaker, has applied these systems for its engineers and external engineering companies who manufacture the machines installed in Japan and abroad, thus reducing the number of accidents.

This paper describes the outline and current situation of the SA/SBA qualification system, and the case of AGC that adopted the system and reduced the number of accidents.

Keywords:

safety assessor, safety basic assessor, safety knowledge, qualification system, risk assessment, safety in machinery operation

Background and qualification systems of Safety Assessor/ Safety Basic Assessor

In manufacturing sites with industrial automation system introduced, it is important that machinery used in the sites is appropriately designed and risks are reduced to an acceptable level through risk assessment in order to reduce accident. To this end, as shown in Fig.1, it is important to appropriately implement risk assessment. Consequently, details of the above are stipulated in international standard on machinery, ISO 12100 (Safety of machinery-General principles for design-. Risk assessment and risk reduction). The content of this standard and rules for safety is accepted worldwide by machine designers and users involved in manufacturing [1].

In Japan, the concept of machinery safety as above has been currently accepted nationwide. However, in the begining of 2000, the level of recognition on the content of various international safety standards and mutual relations were still low. Therefore, in Japan, safety

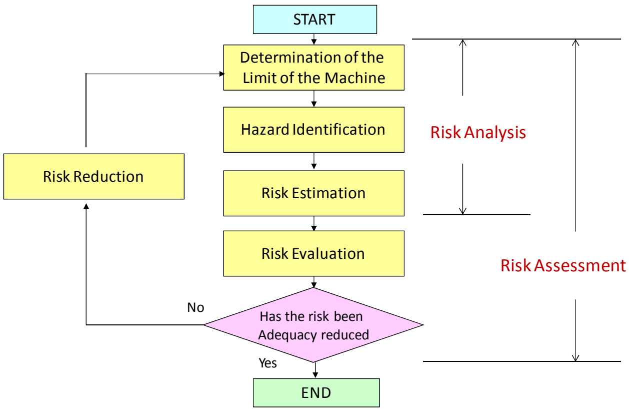


Figure 1: Procedure of risk assessment

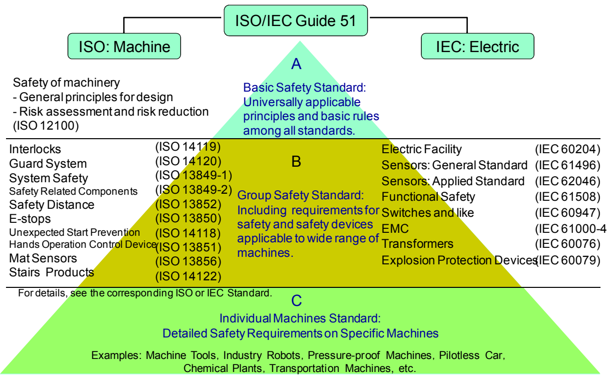

ISO/IEC Guide 51
ISO: Machine
IEC: Electric
A
Safety of machinery
- General principles for design
- Risk assessment and risk reduction
(ISO 12100)
Basic Safety Standard:
Universally applicable principles and basic rules among all standards.
B
Interlocks (ISO 14119)
Guard System (ISO 14120)
System Safety (ISO 13849-1)
Safety Related Components (ISO 13849-2)
Safety Distance (ISO 13852)
E-stops (ISO 13850)
Unexpected Start Prevention (ISO 14118)
Hands Operation Control Device (ISO 13851)
Mat Sensors (ISO 13856)
Stairs Products (ISO 14122)
Group Safety Standard:
Including requirements for safety and safety devices applicable to wide range of machines.
Electric Facility (IEC 60204)
Sensors: General Standard (IEC 61496)
Sensors: Applied Standard (IEC 62046)
Functional Safety (IEC 61508)
Switches and like (IEC 60947)
EMC (IEC 61000-4)
Transformers (IEC 60076)
Explosion Protection Devices (IEC 60079)
For details, see the corresponding ISO or IEC Standard.
C
Individual Machines Standard:
Detailed Safety Requirements on Specific Machines
Examples: Machine Tools, Industry Robots, Pressure-proof Machines, Pilotless Car, Chemical Plants, Transportation Machines, etc.

Figure 2: Hierarchic Structure of Safety Standards on Machinery Safety

standards of IEC and ISO were summerized as three-layered standard group system for easy understanding as shown in Fig.2, where ISO 12100 was positioned as a top rank (A standard) to specify general rules for designing security-oriented machinery. Further, based on this basic safety machinery, the second layer and the third layer were respectively regarded as group safety standards (B standards) and further safety standards on individual machines (C standards) so that the concept for machinery safety was reasonably understood[2] [3].

However, though international standards were thus systematically summerized, it was difficult for general machine manufacturers and users to understand the content of standards reading them though and conduct risk assessments and machinery designs in line with those standards, even though experts of machinery safety can.

Therefore, a personnel qualification system for developing engineers and managers to understand safety technologies was built, for the purpose of securing understandable actual content of safety technologies and machinery safety base on international standards and recognition on understanding levels of engineers using layered system. The system was launched under the initiative of Nippon Electric Control Equipment Industries Association (NECA) as the standard/certification research and development project of Ministry of Economy, Trade and Industry (METI), in cooperation with Japan Certification Corporation (JC) and The Society of Safety Technology and Application Japan (SOSTAP) chaired by Dr. Masao Mukaidono, Professor Emeritus of Meiji University. Specifically, ‘‘Safety Assessor Certification System“, qualification program for machinery designers and safety managers, was launched in 2004 [4]. In addition ‘‘Safety Basic Assessor Certification System“ was additionally founded in 2009 as a basic qualification for wider range of non-technological personnel such as operators, general managers, managers, and also personnel involved in sales, general affairs, purchasing division and human resources. Both systems are operated mutually in cooperation [5].

Layered structure of Safety Assessor Certification System and Safety Basic Assessor Certification System and the outline are shown in Fig.3. Qualifications are listed in the order of deeper understanding expertization. They are called Safety Lead Assessor (SLA), Safety Assessor (SA), Safety Sub-Assessor (SSA) and Safety Basic Assessor (SBA). Namely, Safety Assessor Certification System is divided into three levels, and Safety Basic Assessor has one level as a beginning course. In addition, for easy understanding of expertization levels as an image, they are expressed as Gold, Silver, Bronze and Aluminum from the top, following in colors of the Olympic medals.

In this system, Safety Sub-Assessor at bronze level shall have basic knowledge on safety required for validity confirmation on safety, Safety Assessor at silver level shall have comprehensive competence for judging the validity of safety in addition to basic competence, through acquiring expertize and training classes, and Safety Lead Assessor at gold level, summit, shall have a comprehensive competence to judge the validity of safety as a third party through acquiring expertize and taking training classes. This system allows acquisition of skills in phases and systematically (Fig.3). Those qualification holders are obliged to submit reports on their annual activities to maintain qualification levels they have. Meanwhile, the Safety Assessor Certification Committee checks the content to judge them that they have competences. In renewal of their qualifications in every fourth year, follow-up classes are provided to support their knowledges on safety, in order for them to maintain and update the latest level of safety knowledge.

‘‘Safety assessor qualification system“ is the system for developing certifying experts who conduct risk assessment based on international safety standards for

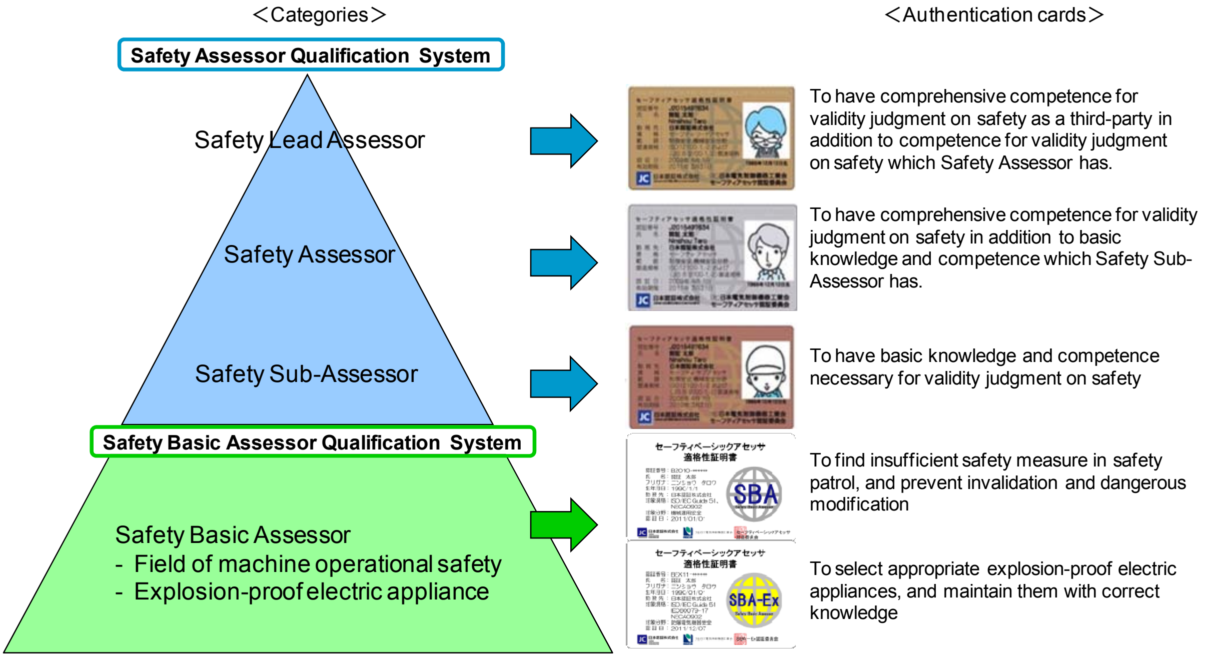

＜Categories＞
＜Authentication cards＞
Safety Assessor Qualification System
Safety Lead Assessor
Safety Assessor
Safety Sub-Assessor
Safety Basic Assessor Qualification System
Safety Basic Assessor
- Field of machine operational safety
- Explosion-proof electric appliance
To have comprehensive competence for validity judgment on safety as a third-party in addition to competence for validity judgment on safety which Safety Assessor has.
To have comprehensive competence for validity judgment on safety in addition to basic knowledge and competence which Safety Sub-Assessor has.
To have basic knowledge and competence necessary for validity judgment on safety
To find insufficient safety measure in safety patrol, and prevent invalidation and dangerous modification
To select appropriate explosion-proof electric appliances, and maintain them with correct knowledge
SBA
SBA-Ex

Figure 3: Conceptual hierarchy of Safety Assessor and Safety Basic Assessor Certification System

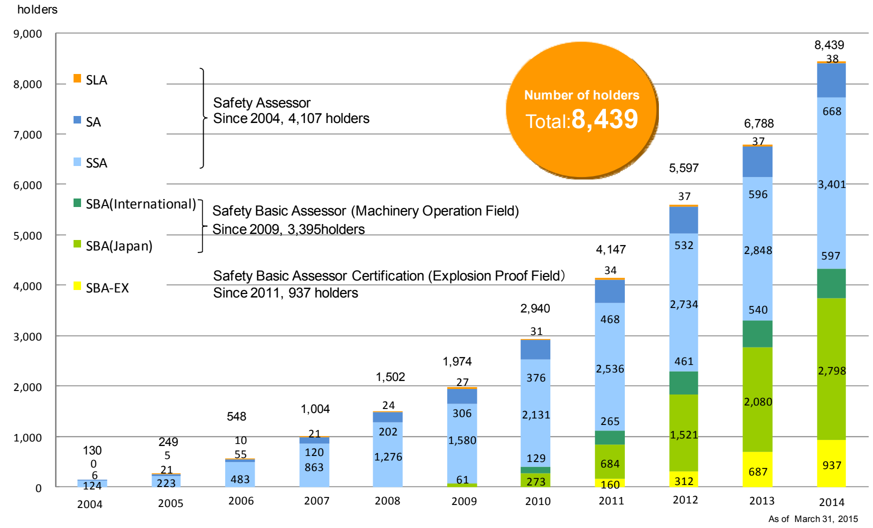


Figure 4: Trend of total number of qualified to Safety Assessor and Safety Basic Assessor Certification System

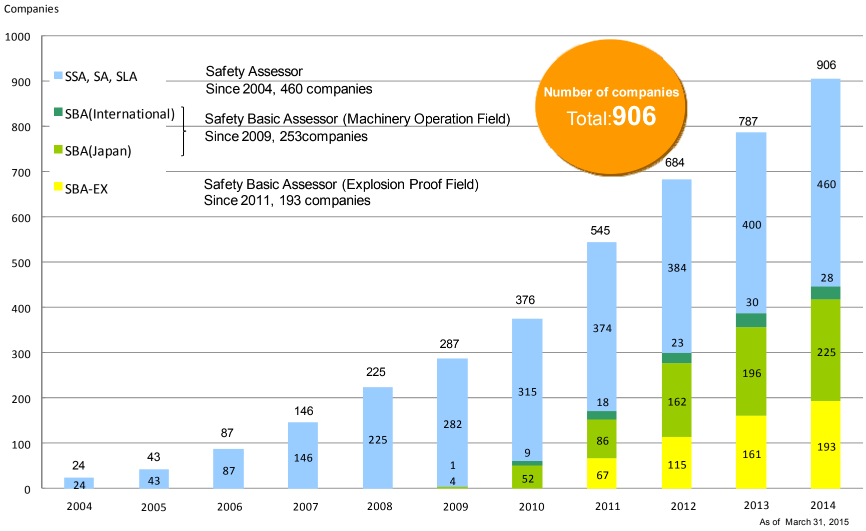


Figure 5: Trend of total number of companies adopting Safety Assessor and Safety Basic Assessor Certification System

their related corporations to build "zero-risk" environment at manufacturing sites, logically explain and report the result, and recommend appropriate measures [6] [7].

Meanwhile, to build up safety in manufacturing sites which are diversified and sophisticated, it is insufficient to rely on developing experts on machinery safety. It is the Safety Basic Assessor Qualification System (SBA) that was founded in 2009 for expanding its target to not only engineering personnel such as machinery safety designers and safety managers but non-technological personnel such as operators, general managers, managers, and also personnel involved in sales, general affairs and personnel as a basic qualification. This system was established in response to machine user companys' requests that it is important to disseminate ubiquitous concept and fundamental knowledge on safety to a wide range of occupations and classes. The purpose is to develop personnel with safety knowledge in wide range of fields at the level of safety patroling by acquiring knowledges on safety and safe operation of machinery where expertize based on international safety standards are taken into account [8].

In addition, there still happen fire and explosion accidents in factories and plants handling combustible gas and inflammable liquid. It is an urgent matters to secure explosion-proof electrical facilities. It is frequently requested that it is necessary to establish a system to educate explosion-proof technologies. Therefore, qualification for the field of explosion proof was established together in Safety Assessor Qualification System (SBA-Ex) in 2011 (Fig.3) .

Increase in the number of SA/SBA qualified persons and companies to adopt them

Since the foundation of the SA system in 2004, the concept of the SA/SBA qualification system has been bringing a great impact and sympathy mainly in Japanese manufacturers, and the number of qualified persons dramatically increased after the period when the system was recognized. Further, the system is globally developed in ASEAN countries (China, Taiwan, Korea, the Philippines, Thailand and Indonesia) besides Japan.

Change in the number of SA/SBA qualification holders since 2004, with classification of companies which have SLA, SA, SSA qualification holders in the aggregation are shown in Fig.4. When the system was just launched, from 2004 to 2006, some 200 persons anually passed examinations for those qualifications. Since around 2010, new qualification holders of more than 1,000 persons has been annually created. Thus, the present number of qualification holders is 8,439 persons. The breakdown of them represents: 38 for SLA (Gold), 668 for SA (Silver), 3,401 for SSA (Bronze) and 4,332 for SBA (Aluminum). The SBA qualification system was launched in 2009 and their number of qualification holders in Asia has begun to increse since 2010, and the number of this qualification holders in Asia other than Japan reaches 597 persons. The SBA-EX qualification specialized in the field of explosion proof was started in 2011, and the number of this holders at present reaches 937 persons.

Fig.5 shows change in the number of companies which create SA/ SBA qualification holders. The number of those companies, as of 2014, is 906 (as of the end of

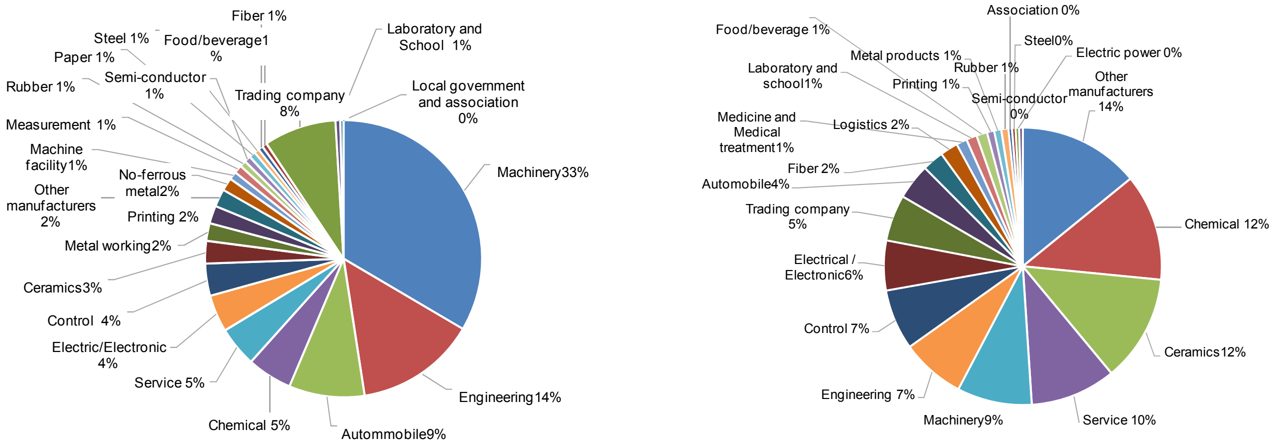


Figure 6 (a): Classification of company with SLA, SA and SSA qualification holders

Figure 6 (b): Classification of company with SBA qualification holders

Figure 6: Fields of companies which have SBA qualification holders

March, 2015), and the number has been annually incresing by 100 companies, which are regarded as having new SA/ SBA qualification holders.

Fields of companies which have SA/SBA qualification holders are shown in Fig.6. The classification of companies with SLA, SA and SSA qualification holders is shown in Fig. 6 (a), and that of companies with the SBA qualification holders in Fig. 6 (b). Fig. 6 (a) shows that the percentage of machinery manufacturer, engineering and automobile-related companies have large share of more than 50%. Meanwhile, as shown in Fig. 6 (b), SBA (Aluminum) qualification holders are hired in companies in extensive fields. It is understood that needs for understanding of the content of international standards and correct practice of risk assessment is incresing in companies. Further, Table 1 shows the latest 4 annual number of examinees and successful candidates. In case of 2014, 1 applicants passed the examination (pass rate of 25%) among 4 examinees in SLA (Gold), 83 applicants passed the examination (pass rate of 49%) among 171 examinees in SA (Silver), 775 applicants passed the examination (pass rate of 78%) among 988 examinees in SSA (Bronze) and 1,025 applicants passed the examination (pass rate of 97%) among 1,052 examinees in SBA (Aluminum). Average rate of successful applicants in past 4 years is 22% for SLA (Gold), 41% for SA (Silver), 70% for SSA (Bronze) and 92% for SBA (Aluminum) [9].

Companies producing actual SA/SBA-qualified persons specifically listed up by field are described below: For details, refer to the homepage of JC where names of all companeis are shown.

Automobile manufacturers: HONDA MOTOR, HONDA Engineering, HONDA R&D, Fuji Heavy Industries, NISSAN Motor, YAMAHA Motor and TOYOTA Motor

Automobile parts manufacturers: DENSO, DENSO WAVE, JTEKT, SHOWA, AISIN AW, AISIN Seiki, SHOWA-SEIKO, F.C.C., JATCO and TOYOTA Industries

Machine manufacturers: TOSHIBA-Machine, AMADA, The Japan Steel Works, Shintokogio, KUBOTA, IHI, SHINMAYWA, Kawasaki Heavy Industries, HITACHI Construction Machinery, JTEKT, MAKINO Milling Machine, SHIMA SEIKI, EBARA, Nachi-Fujikoshi, KOMATSU NTC, HORKOS, HIRATA and Okamoto Machine Tool Works

Precision machine manufacturers: Konica Minolta, RICOH, SHIMADZU, ULVAC, OLYMPUS, CANON, HORIBA, ESPEC, SEIKO EPSON, NIDEC COPAL and TOWA

Chemical manufacturers: KANEKA, KURARAY, KUREHA, DAIKIN Industries,TSUMURA, ASAHI KASEI, KAO, Shin-Etsu Chemical, SEKISUI CHEMICAL, Taiyo Nippon Sanso, Nitto Kogyo, Nitto Denko, Nippon Carbide Industries, HITACHI Chemical and NICHIA

Engineering companies: SANKYU, Nippon Steel and SUMIKIN Texeng., ASAHI Kogyosha, SHINRYO, Sansei Technologies, SUNSTAR Engineering, TORAY

Table 1: Result of examinations for each fiscal year

		Applicants	Successful Applicants	Pass rate
2011	SLA	11	3	27%
	SA	315	96	30%
	SSA	671	467	70%
	SBA	773	707	91%
2012	SLA	10	3	30%
	SA	173	85	49%
	SSA	693	459	66%
	SBA	1,332	1,185	89%
2013	SLA	7	0	0%
	SA	196	87	44%
	SSA	767	487	63%
	SBA	1,113	1,010	91%
2014	SLA	4	1	25%
	SA	171	83	49%
	SSA	988	775	78%
	SBA	1,052	1,025	97%

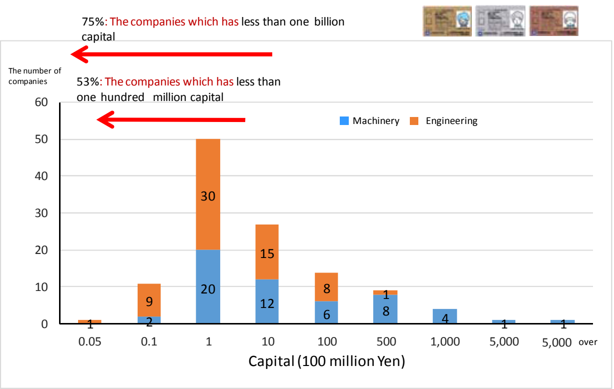


Figure 7 (a): The number of companies where SA certificates holders are working
**classify based on capital (e.g. machinery/ engineering)*

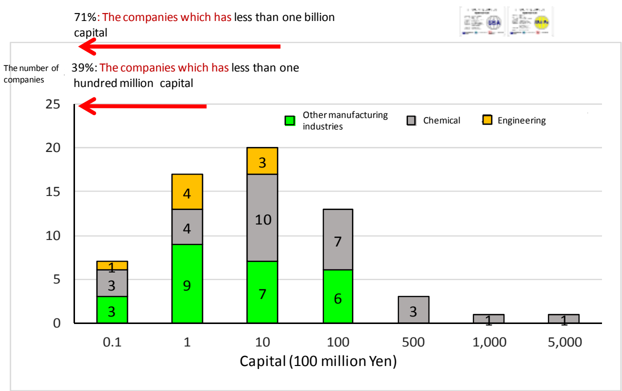


Figure 7 (b): The number of companies where SBA certificates holders belong
**classify based on capital (e.g. machinery/ engineering)*

Figure 7: Results of the research on the distribution of companies with qualification holders by capital

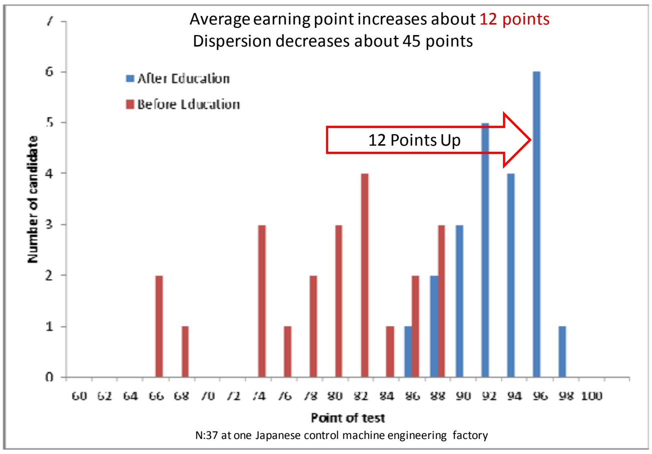


Figure 8: Before/After of SBA Educations on Knowledge level of workers

Engineering and MITSUBISHI Chemical Engineering

Thus, it is understood that the system is utilized by many Japanese key industries for manufacturing.

Further, one especially particular note is that SA/SBA qualified persons are highly used not only in major companies as listed above but in small-and-midium sized companies. Results of the research on the distribution of companies with qualification holders by capital through sampling are shown in Fig. 7. Fig. 7 (a) shows the distribution of companies, by capital, with SA qualified persons in industries related to machinery and engineering, where companies with capital of 1 billion yen occupy 75%, and companies of 100 million yen in capital occupy about the half, 53%. Thus, it is understood that very large number of small-and-midium sized companies need those qualification holders. The distribution of various manufacturers, engineering and chemical-related companies, by capital, to which SBA qualified persons belong is shown in Fig.7 (b). It is noted that companies with capital of 1 billion yen or less occupy 71% and those with 100 million yen or less occupy 39%. In other words, it shows, also in SBA qualifications, that the qualification system is widely introduced meeting needs not only of major companies but small-and-midium sized companies.

Considering from increases in the number of companies which adopt the SA/ SBA qualification systems and in the number of qualification holders, as shown from Fig. 4 to Fig. 7, educational trainings in the field of safety technology can be considered to be significantly effective in improving the knowledge level, in terms of giving chances to appropriately learn standards of machinery safety. The comparison of marks of examinees before and after education for acquisition of the SBA qualification, as shown in Fig.8, can be considered to show that the understanding level of concepts on safety technologies and risks were dramatically improved after the lecture, by 10 point increase in the average, as well as the dispersion of examinee's marks decreased, and trainees' levels of knowledge got closer to even. It will be the background for wide adoption of the SA/ SBA qualification system by many machinery manufacturers and users that the system is achieving effects visually understood.

Relationships between the notification of Ministry Health, Labour and Welfare, and the SA/ SBA systems

As understood by Japanese situations for past ten years, the importance of machinery safety based on international safety standards is more and more increasing also in Japan.

Therefore, in order to enhance measures fo industrial accidents caused by machinery, Ministry of Health, Labour and Welfare promoted "Research on dangerous and hazardous properties of machinery" and developed "Guidelines for the basis of comprehensive safety Standard of Machinery". In 2012, it was obliged to make efforts on given "notice on hazardous properties of machinery" to transferers and acceptors of lent machines. The situation of the promotion of obligation to use best efforts on providing residual risk information is shown in Fig. 9. It is described that it is necessary for machine designers and users to communicate on risks. As shown in Fig.9, machine designers and manufacturers implement risk assessment and protective measures and provide information on residual risks to corporation users of machines. And

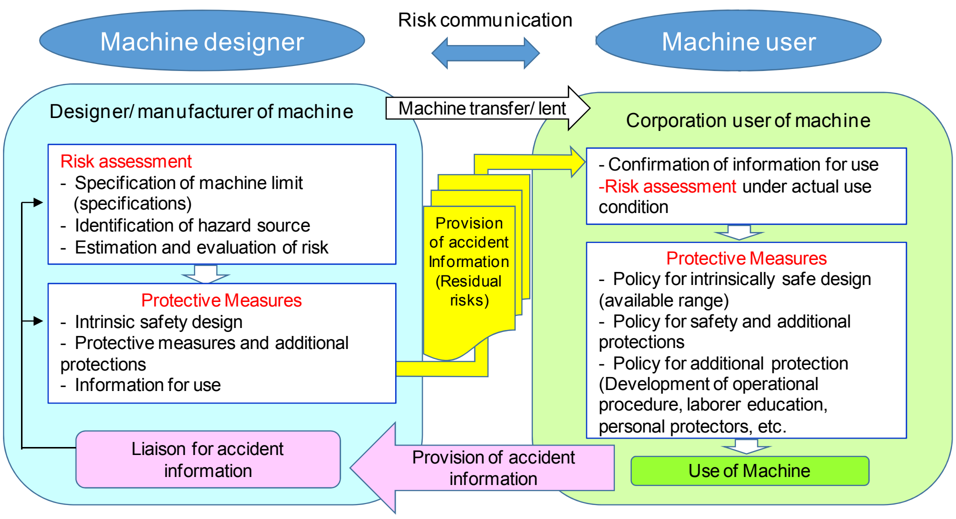

Machine designer
Risk communication
Machine user
Designer/ manufacturer of machine
Machine transfer/ lent
Corporation user of machine
Risk assessment
- Specification of machine limit (specifications)
- Identification of hazard source
- Estimation and evaluation of risk
Protective Measures
- Intrinsic safety design
- Protective measures and additional protections
- Information for use
Provision of accident Information (Residual risks)
- Confirmation of information for use
-Risk assessment under actual use condition
Protective Measures
- Policy for intrinsically safe design (available range)
- Policy for safety and additional protections
- Policy for additional protection (Development of operational procedure, laborer education, personal protectors, etc.
Liaison for accident information
Provision of accident information
Use of Machine

Figure 9: Promotion of obligation to make efforts on provision of accident information by Industrial Safety and Health Law

corporation users implement risk assessments and protection measures as users. In the case that an accident should occur, the accident information is provided to the machine manufacturer This is a series of event.

In order to promote safety of machinery through those standards and guidelines, it is neccesary for both machine manufacturers and users to have personnel with knowledge on machinery safety. Therefore, Ministry of Health, Labour and Welfare issued LSB notifications of 0415 No. 3 “Education on machinery safety to design engineers and manufacturing technology managers” and 0415 No. 1 “Items calling for special attention regarding education on machinery safety to design engineers and manufacturing technology managers”, and operation guide of education on machinery safety, as well as promoted further prevention of industrial accidents through education for developing human resources [10] [11].

As purposes of issuing the said notifications, following matters are described in the operation guide of education on machinery safety:
Industrial accident because of machines used at industrial site occupies some 1/4 of total industrial accidents. Serious accidents such as pinched by, caught in machines, etc. never cease. In order to further reduce those industrial accidents, it is described that risk assessment should be implemented and risks should be reduced in stages of design, manufacturing and use of machinery to enhance machinery safety in the “Guideline of comprehensive safety standards of machinery”, and persons with sufficient knowledge on methods for researches on hazards related to machinery should prepare notices on hazards of machinery in they are prepared, in the “Guideline for promoting the preparation of notices on hazards of machinery by transferors”

“Design engineers” who belong to a machine manufacturer, a machine engineering company (including a company integrating machines into a system), a transferor of machines (including a distribution company) or a company involved in machine design and modification and a user as well, and “Manufacturing technology managers” who belong to machine user company play important roles in implementing analysis on hazards. Therefore, the aim is to further prevent industrial accident caused by machinery through vesting the knowledge on promoting machinery safety to enhance machinery safety by providing those persons with education curriculums for safety-and-health education.

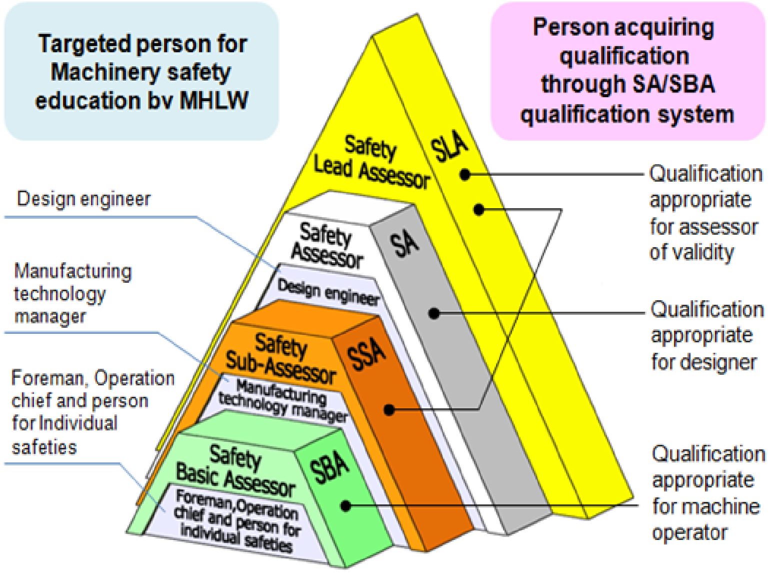
Further, (1) machine manufacturers, corporation users and (2) safety-and-health organizations, trade associations, etc. are specified as performers of the said education, and as requirements of a lecturer, it is pointed out that he or she should have sufficient knowledge and experience on education curriculum.

Further, notifications introduce the operation guide of machinery safety education for design engineers and manufacturing technology managers, and the SA/SBA qualification systems are highly evaluated as beneficial to industries. Further, the SA/SBA qualification systems were picked up as recommended education programs for the development of human resources. There, it was clearly stated that foremen of machine users, operation chiefs and persons in charge of safety is effective for machinery safety education. The content is shown in Table 2. This table shows the comparison of SA/SBA qualifications holders and persons targeted for education in the notification of Ministry of Health, Labour and Welfare. From the table, it is understood that the SLA qualification and the SA qualification is suitable for design engineers and the SBA qualification is suitable for manufacturing technology managers as well as foremen, operation chiefs and persons in charge of safety.

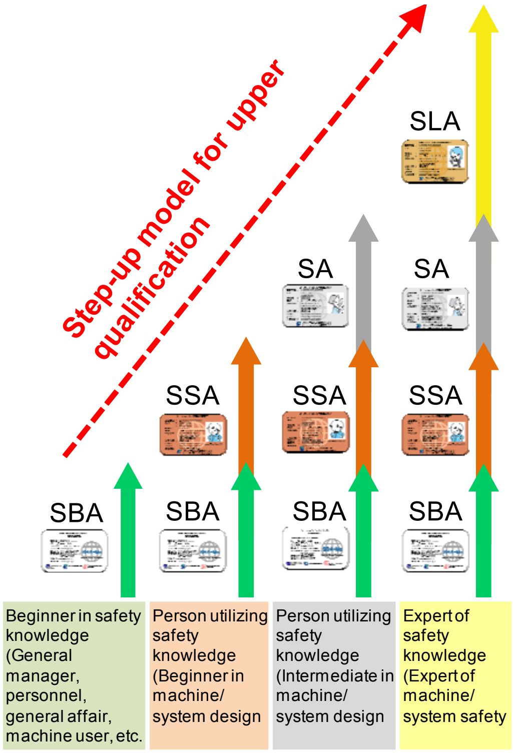
Notifications, require total education time of 15 hours for engineer’s moral, related laws and regulations, machinery safety rules, risk assessment in machine operations and reducton of risks as a machinery safety education curriculum for “Manufacturing technology managers, and 30 hours (40 hours for electric control engineers) for engineer’s moral, related laws and regulations, machinery safety rules, risk assessment in machinery design and manufacturing, reducton of risks and notices on hazards of machinery as a machinery safety education curriculum for “Design engineers”. The

Table 2: Relationships between SA/ SBA systems and targets for curriculum of machinery safety by Ministry of Health, Labour and Welfare

SA/SBA qualified persons		Target for education by MHLW
Safety Lead Assessor		Machine designer
Safety Assessor		
Safety Sub Assessor		Manufacturing technology manager
Safety Basic Assessor	Field of Machine operational safety	Foreman, operation chief and person in for individual safeties
	Field of explosion-proof appliances	


Targeted person for Machinery safety education bv MHLW
Person acquiring qualification through SA/SBA qualification system
Design engineer
Manufacturing technology manager
Foreman, Operation chief and person for Individual safeties
Safety Lead Assessor
SLA
Safety Assessor
SA
Design engineer
Safety Sub-Assessor
SSA
Manufacturing technology manager
Safety Basic Assessor
SBA
Foreman,Operation chief and person for individual safeties
Qualification appropriate for assessor of validity
Qualification appropriate for designer
Qualification appropriate for machine operator

(a) Co-relationship between SA/ SBA systems and targets for curriculum of machinery safety by Ministry of Health, Labour and Welfare


Step-up model for upper qualification
SLA
SA
SA
SSA
SSA
SSA
SBA
SBA
SBA
SBA
Beginner in safety knowledge (General manager, personnel, general affair, machine user, etc.
Person utilizing safety knowledge (Beginner in machine/ system design
Person utilizing safety knowledge (Intermediate in machine/ system design
Expert of safety knowledge (Expert of machine/ system safety

(b) Example of phased skill-up in safety knowledge by targeted person

Figure 10: Relationships between SA/ SBA systems and targets for curriculum of machinery safety by Ministry of Health, Labour and Welfare

fact of SA/ SBA qualification systems having been approved by Ministry of Health, Labour and Welfare as effective qualifications means that the range of examinations and lectures in SA/ SBA qualification systems are fully encompassing that of the knowledge in the education curriculum required by the said notification.

Most troublesome matters for companies to implement machinery safety education in accordance with this notification is difficulties in preparing training materials and exercise programs for machinery safety education in line with curriculums (subjects) of more than 15 hours to 40 hours, which are shown in the notification, and further difficulties in finding lecturers, who have sufficient knowledge and experiences in education curriculums, satisfying the requirements.
Problems for those corporations can be solved by using SBA/SA qualification programs.

For easy understanding of relationships between SA/SBA systems and targeted trainees of Ministry of Health, Labour and Welfare, examples of phased skill-up in safety knowledge by targeted trainee are shown in Fig. 10 (a) and Fig. 10 (b). These figures show that requirements of knowledge and the range of examination and lecture in SA/SBA qualifications fully satisfy education curriculums for design engineers and manufacturing technology managers required by Ministry of Health, Labour and Welfare. Especially, as shown in Fig. 10 (b), it is understood that those four levels of qualifications are effective in upgrading careers. Beginners with small knowledge on safety can begin with acquiring the SBA qualification and systematically step up from the SBA qualification, the SSA qualifications, the SA qualification to the SLA qualification accumulating experiences and learning knowledge.

Example of SA/ SBA Systems Introduced by AGC ASAHI Glass

Next, here introduced the case of introduction by AGC ASAHI Glass Group and the effect, as an example of a company to have introduced SA/SBA qualification systems. The AGC Glour with ASAHI Glass (ASAHI GLASS Co., Ltd.) as a core is a world-leading company in manufacturing of glass [12]. The company is a smokestack facility industry, manufacturing high-quality glass such as for automobiles, televisions and building windows. The AGC Group, global company, which carrys on a business worldwide has been making efforts on machinery safety as common measure for safety management since 2006.

As previously mentioned, in Japan, “Guidelines for the basis of comprehensive safety Standard of Machinery” of Ministry of Health, Labour and Welfare came into force in 2001, and risk assessments came to be often implemented by machine users because of the promotion of obligation to use best efforts on risk assessment in response to the enforcement of the revised Industrial Safety and Health Act in 2006. However, the risk assessment in stages of designing and manufacturing, which are most important, was not activated so much. It is because that risk assessment of existing facilities requires the validation of safety designs at the stage of design drawing based on international safety standards.

Since the AGC Group is not involved in manufacturing machinery, it was further difficult measures to make not

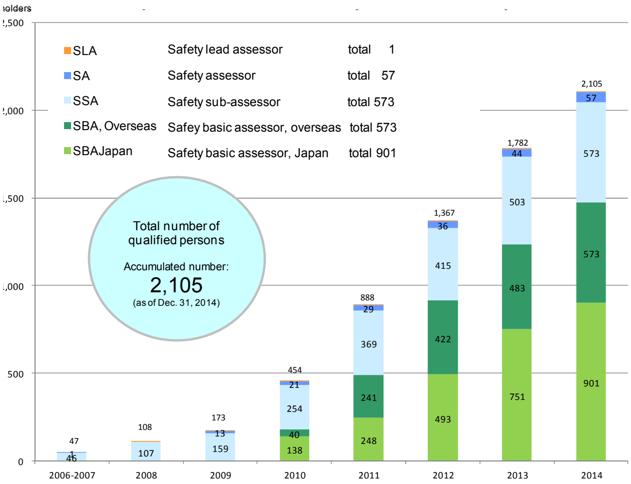


Figure 11: Change in the accumulated number of person acquiring SA/ SBA qualifications in the AGC group and partner companies

only in-house personnel but outside partner companies have competence for risk assessment

Therefore, SA/ SBA qualification systems were introduced into the whole AGC Group in 2006 as an effective measure for enhancing safety, and in-house lectures have been held for departments of machine facility design, machine facility maintenance, environmental safety, and outside partner companies to promote acquisition of qualification. The group has been involved in enrooting safety concept based on international safety standards as well as trying hard to keep the concept of "No production without safety" and disseminating international safety standards. The number of qualification holders, as shown in Fig.11, has been satisfactorily increasing to 1 person for Safety Lead Assessor, 57 persons for Safety Assessor, 573 persons for Safety-sub Assessor and 1,474 persons for Safety Basic Assessor as of the end of December, 2014. If engineers of group companies and partner companies are included, the total number represents 2,105 persons.

As the AGC group is a global company and has a principle to introduce facilities conforming to international standards into all domestic and overseas plants, it introduced SBA qualification systems for Asian affiliated companies in 2011 since it is necessary for those companies, behind Japan in concept of machinery safety, to have machinery safety education. So far, 40%, 573 persons, of 1,474 qualification holders has come to be occupied by six Asian countries. As the important point for machinery safety is risk assessment in designing phase and identifying of hazards and measures conforming to international safety standards are essential, it is heard that the company plans to establish the system where designers should acquire SSA (Bronze) or highher and the approval of risk assessment should be conducted by persons with SA (Silver).

Further, a point worthy of special mention is that sharing knowledge on machinery safety has been advanced, and declared in April, 2014 that "Machine facilities without design risk assessment cannot be accepted" diffusing this policy over inside and outside people, i.e. not only employees but outside contractors. As of the end of December 2014, the number of its qualification holders came to be 135 persons representing 1/5 of total domestic SA/SSA qualification holers of 630 persons. It is said that contractors of facility manufacturing are currently actively acquiring qualifications though initially they had a strong resistance against acquisition of qualifications, and it has become competitiveness in receiving an order to be "superior in machinery safety knowledge".

Meanwhile, for acquiring competency in basic machinery safety which machine designers should have, it is recommended to acquire the qualification of "Safety Sub-Assessor" to every machine and electric designer. The number of holders of "Safety Assessor" which requires a high level of competency in machinery safety, is 57 persons, still a small number. However, it is planned to guarantee machinery safety by using them as approvers of risk assessment in the stage of designing in the future.

The change in the number of accidents by pinching and being caught in machines in AGC ASAHI Glass is shown in Fig. 12, as an index of the effect from the introduction of SA/SBA. Although all of them cannot be said to be caused by machines, it shows that accidents by pinching and being caught in machines, which occur at the average rate of 30% in manufacturing industries, has been decreasing over the years. Glass manufacturing facilities often use high-power motors and actuators. However, it is recognized that accidents caused by machines significantly decreased by using guards and interlocks conforming to international standards.

Meanwhile, there are always worries for a low productivity through those safety measures. However, the graph of the number of plate glasses manufactured drasticlly gets close to the target, as shown in Fig. 13, by reduction of short-time breakdown rate. Those facilities were additional production lines for certain products which were equipped with latest guards and interlocks. In those days, short-time breakdown after operation often occurred, and operators manually response to those stops at their own will. However the

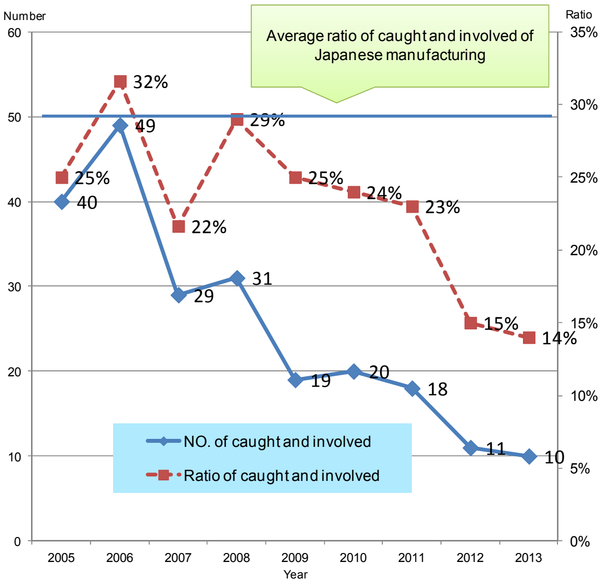


Figure 12 : Trend of accidents of caught and involved in AGC Japan and Asia

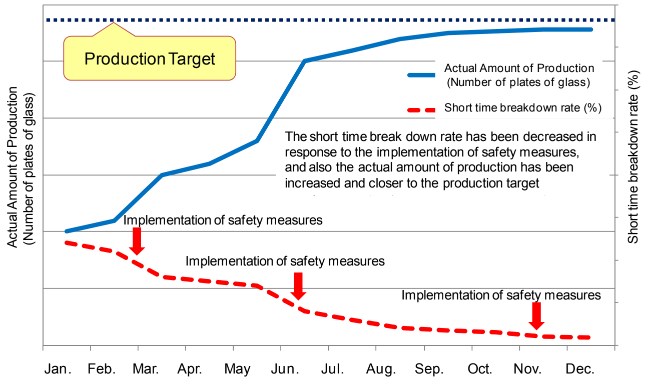


Figure 13: Improvement of Productivity by Implementation of Safety measures at Production line

operation was not available without opening the safety door, and every time the machine made emergency stop. Therefore, the productivity was entirely poor in initial situations. Therefore, initially, the manufacturing department strongly insisted on removal of safety fences. However, as the result of the drastic analysis on measures for short-time breakdown with the attendance of persons in charge of facility, short-time breakdown were reduced and the number of plate glasses manufactured was drastically getting close to the target. Further, isolation of operators from hazards by safety fences allowed doubled conveyance speed to realize much more larger processing capacity than on designing. It is said that , through this experience, the common recognition of “Machinery safety is consistent with productivity” has become the culture of AGC ASAHI Glass.

The above mentioned is the case of SA/ SBA qualification systems introduced by AGC ASAHI Glass, which is highly evaluated by many companies since they realized the safety at manufacturing sites. In addition, what should be especially mentioned, is that many companies not familiar with safety experience the effect of introduction of the system and they widely introduce them.

Development of SA/ SBA qualification systems in Asia and the world

With domestic penetration of SA/ SBA qualification systems, companies which desire to develop those systems at overseas bases began to appear. For example, first,Taiwanese and Korean local managers good at communicating in Japanese language come to Japan for examinations. Or lecturers are dispatched from Japan to overseas bases to implement lectures and examinations for local engineers. As shown in figures 4 and 5, overseas development has been expanded in East Asia and East-South Asia since 2010, and there are SBA qualified persons presently in Asian countries such as China, Korea, Taiwan, the Philippines, Indonesia and Thailand, other than Japan, as shown in Fig. 14.

In short, there are various EN safety standards in Europe and IEC and ISO safety standards were developed based on EN standards. However, Asian region is less familiar with those international standards, in terms of safety, compared to regions with many advanced countries. Therefore, it is very important for the region to understand SA/ SBA qualification systems. Consequently, we are promoting the ODA’s (Official Development Assistance) “Project for building safety management qualification at manufacturing sites”, supported by Ministry of Economy, Trade and Industry of Japanese government, aiming at social contribution by disseminating SA/SBA qualifications in the global society.   This is the scheme that Thailand-Japan Technology Promotion Association (TPA) of Thailand operates those systems in this country. In October, 2015 it plans to launch with the SBA system, beginner’s version, and start operation of the SSA and the SA systems in stages from the next fiscal year.

In the vicinitiy of Bangkok of Thailand, automobile-related machine production is active. Consequently, unemployment rate is inclined to be low and labour costs tends to increase. Companies have come to think that ecxellent labourers are their assets and became to put efforts into taking measures for preventing industrial accidents and injuries at manufacturing sites. Ministry of Labour of thailand promulgated the Occupational Safety, Health and Environment Act in 2011 to legislate the enhancement of management of Industrial   and Health. The government is promoting dissemination of the management of Industrial Safety and Health based on Thai industrial sandard, TIS 18001(OSHAS 18001). Thus, signboards of “Safety First” are hung out in plants in Thailand, and safety measures are promoted in cooperation between labour and management.

However, it is impossible to nip actual risks of machinery only from the viewpoint of safety management. It is the status quo that manufacturing facilities conformig to internationall standards including ISO12100 and engineering aproaches for safety design and measures are not penetrated in societies and local sites as they are not all conforming to TIS standards. Since TPA has been managing a safety manager course for companies, they recognized the neccesity of engineers with safety knowledge. However, it is not easy to develop practical training curriculums from huge number of machinery safety standards.

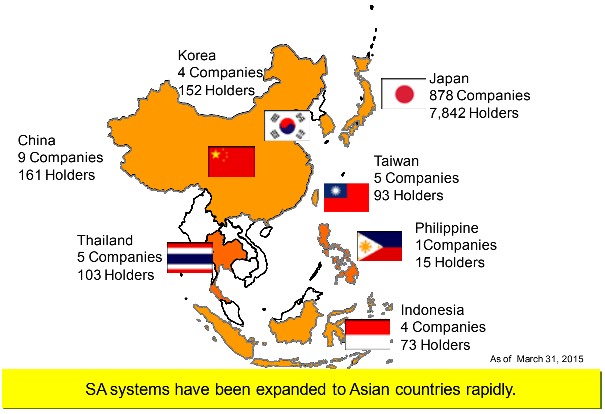


Figure 14: Global development of Safety Assessor and Safety Basic Assessor Certification System

Figure 15: Technical Seminar of Safety Basic Assessor Certification System in Thai

Therefore, taking notice to safety assessor and safety basic assessor systems with more than ten years of achievement in Japan for developing safety engineers with engineering approaches based on international safety standards, TPA decided to transfer the SA system to Thailand in cooperation with NECA and The Overseas Human Resources and Industry Development Association (HIDA).

In February, 2015, NECA and TPA held a seminar on the SA system for companies in Bangkok (Fig.15). When details were illustratively shown for easy understanding of the then situation, there was a question on the difference between Safety Officer to promote industrial safety and health and SA qualified persons. In SA, technologies to design and supply safe machines are learned, while in Safety Officer, management methods to safely use machines are learned. On that occasion, many of participants were satisfied with the answer that the combination of SA and SO brings safety in manufacturing sites. According to the questionnaire for attendees, 84% of participants, in fact, answered that they wanted to take the examination of the SA system.

Considering from above situations, it is also important, in Thailand, to provide guidance on methods for risk assessmant, position for safe guards and their size, concept of interlock, etc. Various standards and systematic knowledge on technologies including methods for selecting safety switches and devices are indispensable for practical safety measures. Under the support of the ODA project by the Japanese government, we are implementing trainings for Thai lecturers involved in lecturing the SA system. They did not only take lectures based on the text for SA, but also visit local Thai plant, practiced risk assessment of machine facilities and also visited National Institute of Occupational Safety and Health, Japan (JNIOSH) and Japanese safety control equipment manufacturers, to acquire enough experience and knowledge. With regard to the text and the curriculum, it is planned to use them with the content edited by them for Thailand. And it is planned to launch operations of SSA and SA respectively in the summer of 2016 and in 2017, to continue and enhance trainings for TPA lecturers.

Also in Thailand, if the SA system is developed and disseminated, safety in Thai plants and local sites will be safe, leading to the decrease in industrial accidents. We hope the system will strengthen Thai companies and it will make workers happy.

Conclusion

In Europe and U. S., especially in Europe, EN 292, the base of ISO 12100, was developed, and safe machinery is distributed under the EC machinery directives where efforts were made on consistency of various safety standards and rules. Therefore, the concept of machinery safety will have already been disseminated and the education system will be established. In Japan, the importance of machinery safety was recognized, and SA/SBA systems, systematic educational qualification system based on international standards, were also recognized. They, as programs recommended in notifications of Ministry of Health, Labour and Welfare, have been infiltrated into not only major companies but especially medium-and-small companies meeting their needs in the education for machinery safety .

Looked down on flow in the future, it is essential to realize safety in the field of manufacturing as developing countries will increasingly promote industrialization. Namely, from the perspective of safety in approximately 3.4 billion laborers out of the global poputation of 7 billion peoples in the aspect of demography, particularly manufacturing sites in Asian developing countries, it is very important to secure the education of machinery safety and the development of human resources in this field as in SA/ SBA systems espacially important since only productivities are focused on and safety is ignored at local sites.

In order to appropriately implement risk assessment and develop human resources who can build safety based on international standards, we plan to actively work on further dissemination and development of SA/SBA systems and promote activities for dissemination of safety through those systems in the future.

Acknowledgements

We owe our deepest gratitude to Information and Communication Electronics Division, Commerce and Information Policy Bureau and Trade and Industry, Technical Cooperation Division, Trade and Economic Cooperation Bureau of Ministry of Economy, Trade and Industry, Technology Promotion Association Thailand-Japan (TPA) and The Overseas Human Resources and Industry Development Association (HIDA) for great guidance and support. Our heartfelt appreciation goes to Professor Emeritus, Dr.Masao Mukaidono of Meiji University, Professor, Dr. Mamoru Ozawa of Kansai University, Professor, Dr. Takafumi Fukuda of Nagaoka University of Technology and Ministry of Health, Labour and Welfare, Industrial Accident Prevention Association, National Institute of Occupational Safety and Health, Mr. Masatoshi Suzuki of the Society of Safety Technology and Application, Japan and many other people for cooperation and support. In addition, we would like to express the deepest appreciation to Mr. Friedrich. H. Harless, Chairman of ACOS, Mr. R. Heidel, Chairman of IEC/TC65 and many other people of IEC, research institutes and certification bodies for positive and useful advices.

References

[1] ISO 12100 *Safety of machinery -- General principles for design - Risk assessment and risk reduction*, International Organization for Standardization, 2010

[2] Masao Mukaidono: *ISO "Machinery safety" International standards*, Japan Machinery Federation, Nikkan Kogyo Shinbun (1999)

[3] Masao Mukaidono: *Trend of machinery safety standards and European standards, standardization and quality control*, 157 (11), Japanese Standards Association，p.30-34 (2004)

[4] NECA 0901 Criteria for certification of Safety Assessor Qualification, Nippon Electric Control Equipment Industries Association, 2007

[5] NECA 0902 Criteria for certification of Safety Basic Assessor Qualification, Nippon Electric Control Equipment Industries Association, 2009

[6] Y. Ishida, T. Yamamoto, Y. Matsueda, R. Maeda, M. Mukaidono T. Fujita.: The creation of a safety assessor accreditation system in Japan; 4th International Conference SIAS 2005, Chicago, USA, Sep. 26-28 (2005)

[7] Ikuo Kumazaki, R.Maeda, T.Arai, Y.Ishida, M.Mukaidono: Safety Assessor Program Assessment; 5th International Conference SIAS 2007, Japan, Nov. 12-13, p.103-110 (2007)

[8] M.Tochio, K. Nakayama, S. Nonaka, M. Shiomi, H. Kanamaru, H. Kojima, H. Toyama, T. Fujita, H. Kasai, M. Mukaidono: The implementation of Safety Basic Assessor System to expand the awareness of safety complied with international standards for engineers and non-engineers in Japan and Asian Countries; 6th International Conference SIAS 2010, Finland, Jun. 14-15 (2010)

[9]http://www.japan-certification.com/certifying-examination/qualification_transition/

[10] http://www.neca.or.jp/assessor/tsutatsu-20140415/

[11] Safety Guide Book-the safety measures of machinery in the workplace-, NECA (2015)

[12] Hiroyuki Takaoka: The day when Japan realizes the safest work places in the world, collection of award-winning work in notes of centennial anniversary of industrial safety campaign project, secretariat of executive committee for centennial anniversary of industrial safety campaign project, p.4-14 (2011)

Corresponding address

Toshihiro Fujita, Ph.D.,
Nippon Electric Control Equipment Industries Association,
2-1-17 Hamamatsu-cho, Minato-ku, Tokyo, 105-0013, Japan

SIAS 2015

8th INTERNATIONAL CONFERENCE
ON THE SAFETY OF INDUSTRIAL
AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

Poster session

Isolation of energies: Establishing Safe Working Conditions

Jean-Christophe BLAISE, Sandrine HARDY

Institut National de Recherche et de Sécurité

Abstract

Work on a machine or a manufacturing process subjects operators to many risks mostly due to presence of multiple sources of energy (electrical, mechanical, hydraulic, pneumatic, etc.). The paper entitled "Operating on machinery out of production modes: principles and accidentology" presented at the 2010 SIAS conference highlighted recurrent issues affecting lockout procedures, isolation and operating live (i.e. under energy). Ensuring safe energised working conditions requires us to consider not only technical but also organisational and operational factors. A first approach to the technical aspects of isolation involving electrical, mechanical and fluid energies has been provided in a dedicated booklet. This paper introduces this document, which describes and explains both lockout devices and an exhaustive operation lockout-to-restoration procedure. The paper subsequently addresses isolation application and applicability based on operator knowledge and risk perception. These aspects have been considered in relation to electrical power, leading to establishment of task organisation and worker training principles. The situation is quite different for other forms of energy and common practices have not yet been adopted in this respect. Finally, we present fresh research involving indirect observation of isolation procedures by means of a questionnaire and interviews; this work may prompt publication of a series of good practices.

Keywords:

Maintenance; Isolation; Energies

Introduction

Accident statistics [1] reflect a permanency of isolation-related causes. Accidents occur because either no isolation has been ensured prior to performing an operation or isolation has been improperly performed. Work equipment, which is stopped during operations, is therefore at the origin of occupational accidents often with serious consequences. These accidents may be due to one or more employees coming into contact with bare parts under electrical voltage, pressurised fluids (hydraulic, steam, hazardous chemicals, etc.) or unforeseen movement of mechanical parts. In most cases, the victim believed he or she was safe, but isolation proved to be incomplete.

Yet, there are technical solutions for intervening safely on work equipment. In this paper, we demonstrate that isolation is one of these solutions and that, in addition to its technical aspects, it involves organisational and human components. For this purpose, we introduce a document intended for companies, which highlights all these issues and offers illustrative examples [2].

The first part of this paper is dedicated to describing the challenges, complexity and limits of machinery isolation and release. The second part addresses best practices in terms of isolation: those relating to the specific case of electrical energy and those relating to other energies through a description of our current investigations.

Operations on Equipment and Isolation

Types of stop

Operating on work equipment is never hazard-free and requires preparation. The following general procedure should be applied before performing or having an operation performed on work equipment:

- Define type of operation to be performed
- Assess risks associated with operation
- Take most suitable measures to operate in safety
- Identify resources needed for successfully completing operation
- Allocate operation to specifically trained personnel with necessary capabilities.

When opting for the measure to be taken to ensure safe operation, there is often confusion between making safe and stopping the work equipment. However, these two notions are totally different and an apparently immobile state is not a guarantee of safety. Thinking on safety, when stopping machinery [3], has revealed that, among the types of stoppage surveyed, only two allow the operator to intervene based on a clearly defined level of safety. These are the "safe stop", which is usually more appropriate for short-term operations and the "sustained safe stop", which guarantees no unexpected start. The "safe stop" state is achieved by involvement of safety device and therefore depends on the equipment control system. The "sustained safe stop" is achieved by implementing one or more technical and/or organisational measures, for example isolation.

Isolation procedure

Isolation, which itself combines technical and organisational measures, is a way of achieving this sustained safe stop and it thereby permits operations to be performed in safety. However, working conditions after isolation can only be safe, if the isolation procedure has been correctly followed, and it must fall within the pre-operation assessment procedure referred to above. Major risk factors emerging from research into accidents, which have occurred during operations on work equipment [4], include imperfect, incomplete or unsuitable isolation application (Figure 1 taken from [2]). Despite the strong technical component it embraces, the very nature of this method means that it remains in effect an instruction and it therefore requires compliance with organisational measures and operating procedures.

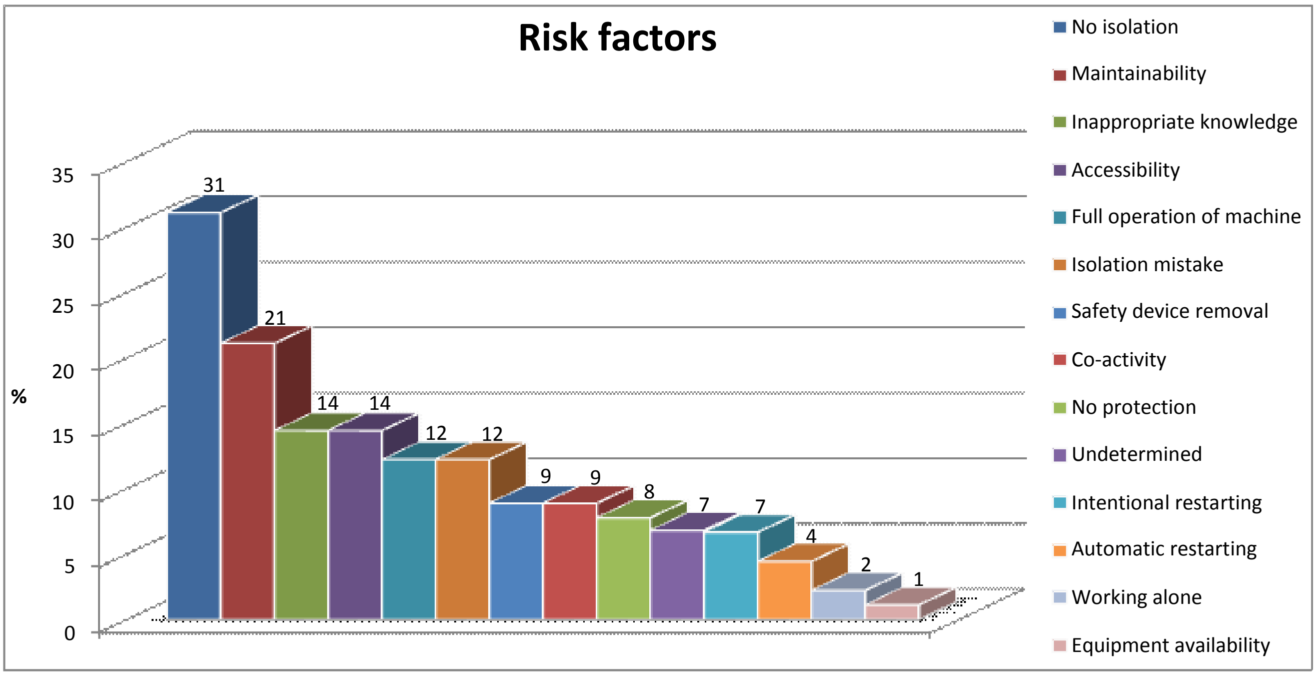


Figure 1 - Distribution of accidents outside production based on risk factors

Isolation: a complex procedure

Work equipment isolation therefore associates technical features, organisational measures and operating procedures. Isolation can be said to be a complex procedure in this sense. It takes into account the different energies present and implements specific procedures, which may be interlinked. Isolation requires adequate training of the operators performing it.

Following a brief description of isolation based on its technical and organisational aspects and with respect to training, we introduce the document entitled "Consignations et déconsignations" [isolation and release operations] [2] as well as the aims and issues it embraces. Isolation limits are also explained.

Technical aspects

For a given energy, the isolation procedure usually comprises the following steps:

1. Disconnection
2. Securing against reconnection
3. Dissipation or retention/containment
4. Checking and identification.

These four steps are generic. They must be adapted to the energy used (e.g. in electricity, checking voltage absence is performed before dissipation of accumulated energy – earthing and short-circuiting [5]) and the combined presence of different energies (e.g. electrical isolation of fan motor prior to mechanical isolation of fan blades). Similarly, equipment and protective equipment to be used during isolation must be suited to each operation.

The order and performance of these steps may be modified following risk assessment based on the specific characteristics of the case under consideration. Disconnection involves acting on one or several devices that separate the equipment from its energy source(s). This requires prior identification of the energy sources including any secondary and emergency sources. After disconnection, securing against reconnection is an operation, which involves guaranteeing sustained disconnection; it requires locking by a specific hardware device that is difficult to neutralise and is tagged. Dissipation involves eliminating all potential and residual energies or evacuating hazardous substances. Energy retention or containment may be resorted to, when elimination is impossible. Finally, checking involves ensuring the effective absence of energy or fluid including hazardous residual energy. Checking must be considered an energised operation; it involves implementation of safety measures and use of suitable equipment.

Performance of an operation on an equipment unit is only possible once all these steps have been fulfilled. After the operation, the different energies must be restored to the equipment unit: this is called release for return to service. Release includes all the measures enabling previously locked out work equipment unit to be restored to its operating condition, while ensuring the safety of personnel and equipment. It requires the same care as isolation in terms of selecting and sequencing its stages. It does not systematically involve performing isolation operations in reverse, but must always result from risk assessment and the need to test the implemented modifications or not.

Organisational and training aspects

The variety of situations makes it impossible to propose a model standard procedure and isolation cannot be reduced to just the four stages previously described. This is why it is important to combine technical measures with other measures affecting work organisation and operator training.

The employer is in charge of work organisation and must therefore lay down the procedure to be respected for each operation requiring isolation. The procedure must be confirmed by practical implementation preferably by qualified personnel, who have not taken part in its preparation. The following basic points must be considered:

- Delimitation of operation zones supervised by a single person in charge of coordinating operations in progress
- Systematic informing of equipment operators of planned operations
- Appointment of isolation supervisor and of company internal and external maintenance operators
- Coordination of isolation and release monitoring, when there is a shift changeover (e.g. work performed by successive teams or work over several days)
- Consideration of installation environment during isolation (e.g. steam pipework crossing locked out installation).

When drafting operating procedures, it should be remembered that risk prevention is not limited to just the isolation procedure. Additional procedures or permits (fire, excavation, access permits, warning lights and signs, etc.) may possibly need to be implemented.

Adequate training and information must be given to the different maintenance operators to enable organisational measures to be applied and isolation stages to be safely fulfilled. The purpose of this training is to ensure the capacity to perform safely operations on work equipment, in particular:

- To know how to assess risks and implement necessary measures
- To control relevant work equipment in relation to the type of operation
- To know how to use correctly protective equipment in relation to the hazard involved and any specific instructions
- To know how to assess the limits of the operations to be performed.

Training must integrate theoretical content illustrated by practical cases to facilitate skills acquisition. Additionally, practical work enables acquisition of know-how. This training provides knowledge of risk prevention as well as isolation and release procedures; it must not replace training allowing acquisition of technical skills for the operator's job.

Brochure ED 6109

Accidentology has prompted us to note that isolation procedure complexity is sometimes misunderstood by companies. This is why, a number of years ago, INRS published a brochure [2] to assist in drawing up an isolation procedure adapted to the situation under consideration, while nevertheless recalling that there are other methods of making operation safe.

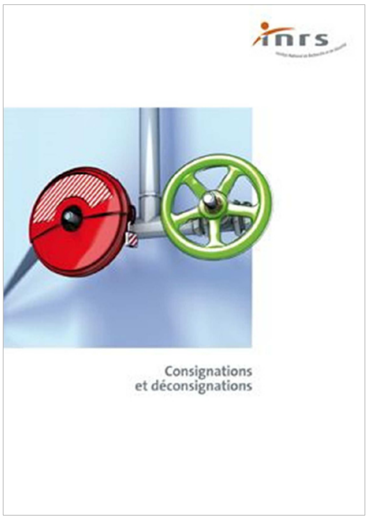


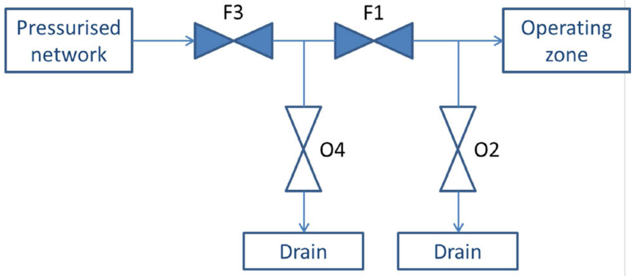
Figure 2 - Brochure ED 6109 (INRS, 2014)

The purpose of this guide is to show end-users that establishment of an isolation procedure is the result of global thinking on conditions governing work equipment intervention. This document is primarily intended for use by operators, but may also be advantageously used by designers. Its objective is also to introduce and describe disconnecting and lockout devices that can be used for isolation purposes. Isolation performance will be severely compromised, if these devices are not provided for in the equipment design (as indeed required by European Directive 2006/42/EC [6]).

This brochure illustrated in Figure 2 deals with both isolation and release operations. Following an explanation of the overall approach to be applied during operations on work equipment, the different technical, organisational and training aspects of isolation and release operations are duly detailed. Special attention is given to taking into account the different energies present: the risks inherent to electrical, fluid and mechanical energies are described and the procedures associated with each of these energies are detailed and illustrated. Taking fluids as an example, we present the procedure for separating these energies by additional isolation, enabling valve leaktightness to be checked. This appears in the brochure in the form of:

- Illustrations representing potentially usable valves
- A diagram reproduced in Figure 3, which describes the procedure to be followed
- An explanation concerning usage (*"This procedure is especially suitable, when the operation location is far away from shut-off devices"*)

Based on examples such as this and reminders of the overall approach to operating on an equipment unit, the anticipated outcome of this guide is better understanding of the equipment intervention procedure by companies and hence better prepared and safer operations.



It is imperative that the following chronology be adhered to:

1. Close isolation valve F1
2. Open drain valve O2
   - ➢ Check operation of drain O2 and that flow has ceased
3. Close isolation valve F3
4. Open drain valve O4
   - ➢ Check operation of drain O4 and that flow has ceased

Figure 3 . Example of separation by additional isolation to check valve leaktightness [2]

Greater understanding of this procedure also enables us to appreciate better isolation limits and to only apply the procedure, when it is entirely suitable.

Isolation limits

The great majority of accidents [1] occurring outside production feature a risk factor related to an organisational issue (therefore involving isolation procedures). Isolation clearly has its limits and, while it allows a "sustained safe stop", it is not necessarily suitable for all equipment operations.

Equipment isolation is very often projected as the panacea, for which there are no alternatives. Machine manufacturer instruction manuals recommend general machine isolation for all operations without considering actual operating conditions and related constraints. Most often, this type of instruction will not be applied because it is viewed as a procedure that is onerous to implement, especially due to the operation time/isolation time ratio or, simply because the operation requires full or partial energy conservation. Even the "Machinery" directive includes an exemption from isolation [6, p. 1.6.3] to allow, for example, part maintenance, data back-up, lighting of internal parts, etc.

Could the accidents referred to above have been avoided, if the machine had been deprived of its energy supplies, i.e. isolated? The most relevant question is: could isolation have been performed? Some interventions - diagnosis, testing, setting, etc. - indeed cannot be performed without energy. The operator will probably not be working in safety, if isolation is the only prevention measure implemented for these operations. Unsuitability of prevention measures is unsurprisingly one of the recorded causes of unsafe operations [3].

Rather than systematically recommending equipment isolation, the following actions should be implemented:

- Machine manufacturers should opt for a design that curtails maintenance operations and integrates maintainability
- Manufacturers should design operating procedures that allow operations under the required energies for machine usage, while guaranteeing safe stoppage of relevant parts
- Users should analyse actual operator interventions and adapt operating procedures.

Good Isolation Practices

As explained in the first part of this paper, isolation is a way of ensuring safe operations on equipment as long as it falls within a global approach to ensuring intervention safety and that it is correctly performed. Within the scope of current research, INRS would like to extend its work on the issue of isolation beyond the content of the brochure already published [2]. Based on experience feedback and a number of specific regulations, work has therefore been started on listing actual practices involving isolation of energy sources and deriving therefrom a guide listing best practices in relation to preventing occupational risks in this area.

Specific case of electrical energy

Isolation absence is the primary risk factor affecting intervention on work equipment. This same statement can be made in relation to the isolation problem, when studying accidents of electrical origin. The main difference between electrical and other energies (mechanical, pneumatic, hydraulic, etc.) is that the area of electrical hazard has been more documented and standardised.

Operation of electrical installations forms the subject of a European standard, namely EN 50110-1 [7]; this lays down requirements for all operations of and work activity on or near electrical installations. The standard covers not only basic safety principles and work procedures, but also work organisation and training of personnel. With regard to isolation, the section of the standard entitled "Dead working" recalls the five basic safety rules for ensuring that the working area is dead (absence of electrical energy) and safe.

These five requirements are as follows (taken from Standard EN 50110-1 [7]):

- Disconnect completely
- Secure against reconnection
- Verify absence of operating voltage
- Perform earthing and short-circuiting
- Provide protection against adjacent live parts.

We therefore go through the isolation steps described above in the isolation "Technical aspects" section with the addition of providing protection against adjacent live parts, thereby ensuring protection from the environment. This step could, moreover, apply to all energies.

In addition to the general requirements laid down therein, the European standard also refers to possible national requirements, which may exist in the area of electrical installation operation. This is indeed the case in France, where there are very stringent regulations in this area.

In France, electrical energy has for many years formed the subject of research aimed at establishing organisation and worker training regulations imposed to ensure safer interventions. The most recent publication is French Standard NF C 18-510 of January 2012 [5];

this fixes conditions for performing operations on electrical installations (organisation of operations, qualification and training of workers). This standard is quoted as a reference document by existing regulations. Furthermore, qualification of personnel performing these operations is compulsory under the French Labour Code. It requires the employer to provide theoretical and practical training of workers on electricity-related risks and measures to be taken for safely intervening, when performing the operations with which they are entrusted.

Standard NF C18-510 can be considered as the counterpart of previously quoted European Standard EN 50110-1 but it goes further in terms of work organisation, training and worker qualification. INRS has published a complementary document [8], which deals with the place of qualification in preventing electrical risks and the qualification procedure, including the role of different players and training.

Thus, with regard to electrical energy, the principle of worker qualification has been retained in France and intervention conditions are strictly regulated. But, what is the situation with regard to other energies? Existing regulations impose no specific method. As a result, we receive questions from companies regarding the existence of reference frames, other than those applicable to electrical energy, and of possible mechanical qualification in particular.

Case of other energies

Observation

No reference frame has been drawn up to date with regard to energies other than electricity. However, it has been reported that some companies, especially large industrial groups, implement their own internal reference frames in the face of this need. In this connection, possible good practices are neither known nor circulated; INRS has therefore decided to draw up a list thereof based on identification of company needs and expectations. To do this, we propose drawing up a qualitative survey of organisational practices and measures already in place as well as of training courses provided and their possible formalisation (recognition of prevention skills). This initial data survey will enable us to assess the relevance, to prevention, of a constraining reference frame dedicated to energies other than electrical. The criteria to be considered will be determined prior to the survey, but we can already cite company expectations, real motivations for setting up this type of reference frame, results obtained in terms of prevention (accidentology, advancing of a prevention culture, etc.), existence of alternative solutions and ease of implementing measures.

The action aimed at surveying good practices for isolating all energies can be broken down into two stages:

1. Select companies, which have installed good practices, based on answers to a questionnaire
2. Visit and interview selected companies.

Action in progress

The questionnaire has been sent directly to companies identified by French regional health insurance funds during the second quarter of 2015. This survey has no quantitative aim and hence includes no search for representativeness. The questionnaire has also been administered via a mailing targeting subscribers to the INRS and AFIM (Association Française des Ingénieurs et responsables de Maintenance) newsletters. The purpose of the questionnaire is to identify the energies present at the company and to address isolation-related practices for each of these energies: Who decides on isolation? Who performs isolation? What specific training courses are there? Are isolation procedures available? Are they drawn up based on a reference document? Where does this come from (if it exists)? A section of the questionnaire is dedicated to the needs and expectations of the companies surveyed; this part focuses on technical, organisational and training aspects. Finally, the questionnaire suggests that companies so wishing leave their contact details in view of a possible meeting.

Interpretation of the replies to this questionnaire will allow selection of relevant companies and more in-depth questioning during visits. Based on an interview guide, the aim will be to check whether their practices indeed enable prevention to progress and whether they can be shared. On completion of this survey and depending on the results, research may be directed towards editing a guide to good practices including a model organisation, training reference document (knowledge, know-how), skills recognition methods and assistance in operator risk assessment. This action is planned for the second six months of 2015 and the first six months of 2016.

Conclusion

Could the accidents referred to in the introduction to this paper have been avoided, if the machine had been deprived of its energy supplies, i.e. locked out? Why was this isolation not performed or improperly performed? This paper shows us that technical solutions do exist. With regard to electrical energy, a reference document defining organisation and training methods is even implemented in France. Other investigations have been started to assess the relevance to prevention of establishing a reference frame dedicated to energies other than electrical to provide good practices for isolation. But is energy isolation always feasible? Some interventions - diagnosis, testing, setting, etc. - indeed cannot be performed without energy.

On a wider scale than isolation, a practical procedure for controlling all energies should be drawn up and implemented. The Association Française des Ingénieurs et responsables de Maintenance (AFIM) and INRS have prepared the Sécurafim guide with this in mind. This guide proposes a procedure to facilitate and make safe maintenance operations on work equipment based on the principles inherent to energy control. Using a model, this procedure enables one to produce a reference record of energy disconnection points for each machine and installation of suitable tags. Maintenance operations are therefore considered from the standpoint of their energy status (energies isolated or operations performed with all or some energies present). It should be remembered that energies can be residual or be used for power or control systems.

This work is currently being directed towards French standardisation, in which a draft standard is now being drafted. Once tested, these French contributions can be promoted at European and even international level. Finally, it should be recalled that isolation is only part of the overall maintenance operation process [9], which just like isolation itself, must be mastered to ensure safer maintenance activities [10].

References

[1] Blaise&Wélitz, Operating on machinery out of production modes : principles and accidentology" in 6th Int. Conf. Safety of Industrial Automated System (SIAS), Tampere, Finland, 2010.

[2] INRS, Consignations et déconsignations, ED 6109, 2014.

[3] INRS, Intervention sur un équipement de travail - Réflexions pour la sécurité lors des arrêts, ED 6038, 2008.

[4] INRS, Sécurité des machines - Modes de fonctionnement protections neutralisées, ED 6127, 2012.

[5] *NF C 18-510 :* Opérations sur les ouvrages et installations électriques et dans un environnement électrique - Prévention du risque électrique, AFNOR, 2012.

[6] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery" in Official Journal of The European Union, 2006, pp. L157, pp. 24-86.

[7] EN 50110-1, Operation of electrical installations - Part 1 : general requirements, CENELEC, 2013.

[8] INRS, L'habilitation électrique, ED 6127, 2015.

[9] NF X60-027 : Maintenance - Processus maintenance et indicateurs associés, AFNOR, 2014.

[10] Blaise, Levrat and Iung - Process approach-based methodology for safe maintenance operation: from concepts to SPRIMI software prototype - Safety Science, 2014, Vol. 70, pp. 99-113.

Corresponding address

Jean-Christophe Blaise, jean-christophe.blaise@inrs.fr

INRS Centre de Lorraine

Rue du Morvan - CS 60027 - 54519 Vandœuvre Cedex - France

Tel. +33 3 83 50 20 00

Start up Safety Assessor Qualification to Educate Safety Engineers in Thailand

Patiphon Koompai*, Hiroo Kanamaru**

**Technology Promotion Association (Thailand-Japan) (TPA)*
*** Nippon Electric Control Equipment Industries Association (NECA)*

Abstract

To reduce occupational accidents in Thailand, NECA, HIDA and TPA have entrusted Safety Assessor Qualification which has operated more than 10 years in Japan. From Oct. 2015, the entry course of SAQ is started in Thailand.

Keywords:

Safety Assessor; Occupational Safety and Health, Thailand

Introduction

In Thailand, the injured labors are decreasing in every year, but the death persons are not (Figure1). To reduce victims in factories, we need not only a safety manager but also a safety engineer who learned IEC /ISO safety standards and techniques.

Methods

Safety Assessor Qualification (SAQ) system[1] has been operated over 10 years in Japan, and it has contributed to reduce occupational accidents. NECA/HIDA decided to entrust TPA with SAQ to educate safety engineers in Thailand.

From 2013, we have studied an adequate curriculum and raised SA instructors of TPA. In Oct. 2015, the Safety Basic Assessor (SBA)[2] qualification system is started in Thailand.

Results

Before starting SBA operation, TPA asked his customers whether they would be interested in SBA. 84% of customers were interested n SBA. The answers requested to the lecture of safety techniques of for machineries. Now, there are 100 candidates to SBA lecture with a capacity of 40. We will held SBA lectures in every 2-3 months in Thailand.

Discussion

SBA is the entry course of SAQ system. Many machinery engineers would step-up to the next SSA and SA qualification. We will start the rest upper course near the future.

And how to collaborate with the safety officer who has responsibility to safety management is the next problem in Thailand.

Conclusion

SAQ which had established in Japan was entrusted to Thailand. It shall contribute to reduce occupational accidents of machines in Thailand.

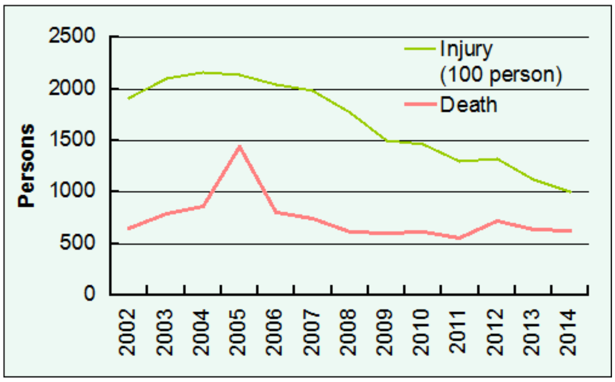


Figure 1: Trend of Occupational Accidents in Thailand [3]

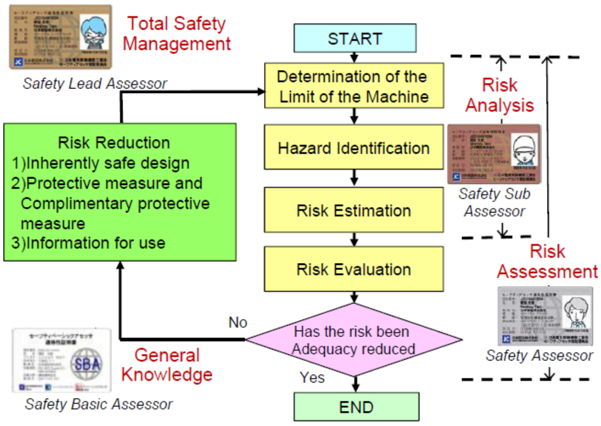


Figure 2: Safety Assessor Qualification in the risk assessment flow-chart

References

[1] M.Tochio, The Improvement of Industrial Safety achieved by the Introduction of Safety Assessor/ Safety Basic Assessor Qualification System and its International Operations, Proc.of SIAS 2012 Montreal, CA, Oct. 2012

[2] NECA standards 0902:2011 Standard for certification of safety basic assessor.

[3] National Profile on Occupational Safety and Health of Thailand 2015. Ministry of Labor Thailand

Special Thanks

This work was accomplished by support of METI (Ministry of Economy, Trade and Industry) Japan.

*HIDA: The Overseas Human Resources and Industry Development Association

Corresponding address

Soi Patthanakan 18, Suangluang, Bangkok 1025
patiphon@tpa.or.th

Camera-Monitor-Systems in Excavators – Using Eye-Tracking to Assess Utilization and Design

Markus Koppenborg, Birgit Naber, Andy Lungfiel, Michael Huelke

Institute for Occupational Safety and Health (IFA)

Abstract

The structure of excavators obstructs direct view from the cab to the rear and right side of the machine. For this reason, cameras on the tail and flank of the machine are intended to provide operators with information about the surrounding area. However, it is unclear how operators actually use such systems. This article describes field studies in which eye-movements of excavator operators were recorded. It further describes how this data can be used to evaluate the design of such systems and to formulate improvements.

Keywords: excavator; camera-monitor-systems; eye-tracking; Situation Awareness;

Introduction

Construction sites are highly dynamic workplaces where a changing number of persons and machines interact in an ever changing physical environment. Excavators add to the dynamic by their high movement variability. As with other dynamic systems, safe operation requires achieving and maintaining operator Situation Awareness, i.e. the system shall inform the operator about the elements in the environment, their meaning and their status in the near future [1]. More specifically, the design of the system has to be in a way that facilitates the flow of information from the different technical elements to the operator and support his understanding of the situation [2,3]

However, the structure and form of excavators may prevent operators from attaining Situation Awareness. Direct sight from the cab to the areas behind and on the right side is obstructed by the counterweight and the boom. Mirrors compensate this only insufficiently. This setup can make reversing and swiveling potentially dangerous movements. Correspondingly, statistics show a clustering of accidents in these parts of the machine [4].

To overcome this modern excavators are equipped with cameras on the right flank and/or the tail and their images are presented on a monitor in the cabin. However, the design of these systems differs widely across manufacturers, models and retrofit solutions. It remains unclear how operators use these systems and how these should be designed to optimally support the operator achieving and maintaining Situation Awareness.

To shed light on this issue the Institute for Occupational Safety and Health (IFA) is conducting field studies on behalf of the German Social Accident Insurance Institution for the construction industry (BG BAU). As a first step the aim is to examine the information needs of operators during potentially dangerous maneuvers (i.e. reversing and swiveling), to assess the occurance of such maneuvres, and to understand how excavator operators use monitors and mirrors during and shortly before these maneuvers by using eye-tracking. In a second step, design recommendations shall be formulated. After project closure results will be made available (in German; summary in English) on http://www.dguv.de/ifa/Forschung/Projektverzeichnis/IFA5126.jsp.

Methods and preliminary results

Apparatus

To understand, which information about the surroundings are needed during reversing and swiveling, preliminary interviews and conversations were conducted with experienced operators, teachers and apprentices. These revealed five different areas around the machine which the opertor needs to monitor in order to prevent collisions (Table 1).

Table 1: Maneuvres and areas of potential collision

Maneuvre	Areas of potential collision
Reversing - while lifting object - with boundary	Rear area - Lifted object - Distance between wheels/track and boundary
Swiveling	Side area of excavator (in direction of movement) Area next to tail (opposite to direction of movement)

Further, tasks and maneuvers were observed and coded in 8 construction sites by using a previously developed coding scheme and a tablet computer (Koppenborg et al., 2015). Two video cameras were used to record excavator operations and use the footage for subsequent correction of observational data.

Eye-tracking was chosen as a method to quantify operator utilization of mirrors and monitors. A head-mounted eye-tracker “Ergoneers Dikablis” was employed, which allowed operators to move their head and body during recording and also exit the cab when necessary.

Additionally, operators were interviewed for approximately 15 minutes about their use of mirrors and monitors and the conversation was recorded with a voice recorder.

Sample and Procedure

To achieve natural operator behavior all data were recorded on typical construction sites with experienced operators during a typical work shift. The sample only comprised operations with regular tools (i.e. buckets and grabs) so as to represent prototypical tasks. Both mobile and crawler excavators were part of the sample, and were equipped with different camera-monitor-systems (Table 2).

Table 2: Sample description: Excavators and operators

No.	Excavator	Cameras	Operator age and years of experience
1	Volvo EC 300 NL crawler	Rear & Side	47 (6)
2	Liebherr A 916 mobile	Rear	38 (3)
3	CAT 325 B LN crawler	None	46 (17)
4	Hitachi 140 N mobile	Rear	56 (25)
5	CAT 329 E LN crawler	Rear	38 (12)
6	Hitachi Zaxis 225 crawler	Rear	51 (27)
7	Liebherr A 924 mobile	Rear & Side	58 (25)
8	Volvo EC 250D NL crawler	Rear & Side	26 (11)

Each measurement consisted of eye-movement recording, while task observation and video recording was conducted simultaneously. Interviews were conducted at the end of the work shift. One measurement lasted between 3 and 5.5 hours and was preceded by a trial measurement on the day before. This was to ensure the operator could get accustomed to the eye-tracker.

Table 3: Description of measurements and reversing movements

		Reversing movements		
No.	Measure-ment duration (h)	Total number	Average duration (s.f)	Total duration (s)
1	4	62	4.5	280
2	5	42	4.9	205
3	5.5	39	3.9	154
4	5	34	6.6	225
5	3.75	114	3.2	368
6	3	60	5.5	327
7	5	59	9.5	559
8	3	30	5.0	151

Variables and Analysis

Table 3 shows durations of each measurement and the amount and average duration of reversing maneuvers. In a next step, these values will also be calculated for swiveling movements. Importantly, for further analysis time intervals will be calculated that consist of the time each maneuver takes plus a time window of four seconds preceding that maneuver. As a central part of the analysis, gaze data will then be analyzed for each interval.

Discussion and further steps

For safe operation systems need to enable operators to achieve and maintain Situation Awareness in an adequate manner [3]. In the case of excavator operations, this applies especially shortly before and during reversing and swiveling movements, because it is during these that many collisions between the machine and humans occur. By means of interviews five different areas of potential collision could be identified, which have to be monitored before or during maneuvers. As camera-monitor-systems have the purpose to support operators' Situation Awareness it is important to assess how their design helps to achieve this.

Results from the current study can be used as a step towards this goal. Glances on the monitor(s) that consistently occur shortly before or during reversing or swiveling can be used as indicators for attaining Situation Awareness. However, maneuvers that are carried out without glances on the monitor(s) require further analysis: How come information on the surrounding is presented, but not regarded? Are there design deficits that discourage operators form using the monitor? Such instances of neglect are expected to provide cues on shortcomings of the system's design. Here, further (qualitative) data from interviews or focus groups may be helpful to find a system design that effectively provides the operator with the needed information.

References

[1] Endsley, M. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors, 37 (1), 32–64.

[2] Salmon, P.M., Walker, G.H., & Stanton, N.A. (2015). Broken components versus broken systems: why it is systems not people that lose situation awareness. Cognition, Technology & Work, 17, 179–183.

[3] Stanton, N.A. … (2006). Distributed situation awareness in dynamic systems: theoretical development and application of an ergonomics methodology. Ergonomics, 49, 1288–1311.

[4] Leisering, H. (2011). Rückfahrkameras an Erdbaumaschinen. BauPortal, 1, 7–13.

[5] Koppenborg, M., Lungfiel, A., Naber, B., Nickel, P., & Huelke, M. (2015). Ein flexibles Gerät zur Tätigkeitskodierung per Beobachtung – Anforderungen und Ergebnisse einer Erprobung. 61. Kongress der Gesellschaft für Arbeitswissenschaft, 25.-27. Februar 2015. GfA-Press: Dortmund.

Corresponding address

Institute for Occupational Safety and Health of the
German Social Accident Insurance (IFA)
Unit New Technologies – Man & Technology
Alte Heerstrasse 111
53757 Sankt Augustin
Germany

A Study of a Special Safety-Confirmation Type Washer That Can Detect the Looseness of Tightened Bolts by Way of Leverage-Exerted Displacement Enlargement

Masanobu CHIBA[*1] **Mizuho NAKAMURA**[*2] **Hiroyuki SASAGAWA**[*3] **Tetuo SUJINO**[*4] **Noboru SUGIMOTO**[*5]

**1,2*,3* Regular member, Polytechnic University (2-32-1, Ogawanishi-machi, Kodaira, Tokyo 187-0035),*
E-mail m-chiba@uitec.ac.jp
**4Regular membe, School of Science and Engineering, Meiji University,*
**5 Regular member, Fellow, School of Science and Engineering, Meiji University,*
(1-1-1, Higashimita, Tama-ku, Kawasaki, Kanagawa, 214-8571)

Abstract

Bolt tightening is widely applied to the fastening of mechanical and structural elements. However, as various external forces act on machines and structures, fastened elements are displaced mutually and relatively, which loosens tightened bolts as the time passes. Prior occurrences indicate that bolt looseness like this has often incurred serious accidents. To counter the problem, the authors have experimentally made a special washer that enlarges the displacement caused by a minimal looseness of tightened bolts by applying the principle of leverage to such an extent that the displacement can be visualized. The special washer, which displaces in accordance with the law of gravity as the looseness occurs, can construct the definite safety confirmation type

.***Keywords:***

Bolt loosening , Special washer, Detection

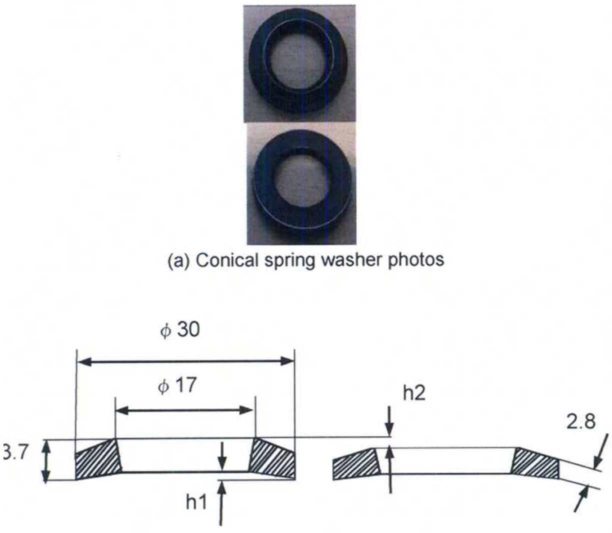
1. Introduction

Screws for fastening are used as a machine element for machine equipment, products and structures of all sizes. Bolts, representing screws, are widely used because of their capability of ensuring strong fastening force and low cost. However, with the action of various external forces on them as the time passes, fastened elements are displaced mutually and relatively, and tightened bolts are loosened. Such bolt looseness has often incurred serious accidents as understood from past cases 1). In order for the elements fastened by means of bolt tightening to be in the stable state, the axial force applied to the bolts in the tensile direction and the compression force applied to the fastened elements should be maintained in the mutually balanced state. However, it is known that "setting" is caused to the bolts due to nut reversing, the secular displacement of the fastened elements and other factors derived from operation and vibration, and the axial force decreases2). This results in the "looseness" of bolts. In terms of safety, the bolt looseness may cause serious faults and hazards to bolt-applied machines and systems. For this reason, in order to maintain the good condition of fastening by means of bolt tightening, human checkup work is absolutely indispensable. Although it is important to adequately educate all workers to make daily checkup complete, it is extremely difficult to check up every one of bolts during operations that are increasingly going complex. When the transition of fastening by means of bolt tightening is observed through time, because there is no bolt that does not become worn or broken indefinitely, the bolt tightening requires periodic maintenance. In fact, however, once bolts are tightened, they are not subjected to maintenance unless some disorder is caused to the equipment or systems they are used. The bolt tightening force and its service life are dependent on empirically-designed value to some extent. However, at the fastened portions placed under various, complex conditions, the bolt looseness or bolt tightening service life may end up in being a dangerous fault when its designed value is exhausted. Also for this reason, periodic checkup is significant.

For on-site bolt looseness checkup work, there is a simple method, i.e., a mark is put on bolts and nuts and the mark displacement is checked for to determine the rotational looseness, or a hammering method, i.e., bolts are struck with a hammer to detect abnormal noise that suggests looseness. However, these methods are not easy because they require skills and 100% checkup. Generally, a direct retightening method by using an open-end wrench is adopted, but this method takes vast amounts of time if a large number of bolts are used for the subject machine equipment. This is where a simpler, more reliable checkup method has been looked for.

With the above in the background and focusing attention on the promotion of the efficiency of daily checkup work, the authors propose a "system for visualizing and monitoring bolt looseness based on the safety-confirmation type3)." This study is conducted under contract with a business enterprise. To be specific, the disc spring washer and bolt shown in Fig. 1 are used for fastening. The axial force on bolts is too small to be estimated directly3). Proposed in this study is a washer unit in which, as an indirect method, the axial force is replaced by the displacement of the disc spring water where the displacement is further enlarged by using the "principle of leverage" ("special washer"). As the important features of the disc spring washer, because the spring reaction force is strong and the hysteresis difference is also large, the difference between the displacement by tightening and the displacement by loosening is large.

The disc spring washer is used in the closely-attached state, and not permitted to be reused because it is designed to be used only once. In this study, the authors receive prototype special washers from the partner business enterprise, and study the possibility of visualization of bolt looseness through the special washers and the effectiveness of a looseness monitoring system for safety-confirmation type bolts configured with a reflection type optical beam sensor. As the conditions of using the special washers in the study, they are placed on a level surface as a rule, and the bolts in use are M16 in nominal size and 4.8 in bolt strength grade. As a tightening method, the torque method using a generally used torque wrench is employed.


(a) Conical spring washer photos

(b) Conical spring washer dimensions

Fig. 1 Body dimensions of disc spring washer (M16)

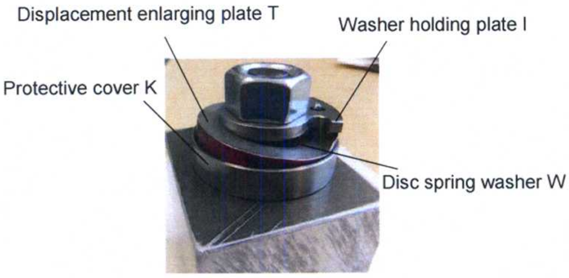


Fig. 2 Special washer

2. Composition of the Special Washer

Fig. 2 shows the fastened state using the special washer, and Fig. 3 is an enlarged view of Fig. 2. The special washer is composed of a washer holding plate I, a disc spring washer W, a displacement enlarging plate T, and a protective cover K. The displacement enlarging plate T has a color-coded graduated scale on the side. When this graduated scale is referred to when the torque wrench is used, the relation between the axial force and the displacement can be recognized. A magnet M built in the displacement enlarging plate T always acts on the protective cover K as an attractive force, and in case of looseness occurrence, detects the looseness together with gravity. As a functional structure, the displacement enlarging plate T is set in the protective cover K, and the disc spring washer W and the washer holding plate I are disposed on the displacement enlarging plate T. The washer holding plate I and the displacement enlarging plate T are in contact at a contact point A. When fastening is made, the contact point A is pushed down. In case of looseness occurrence, the contact point A is released in no time by the restoring force of the disc spring washer W, and the displacement enlarging plate T is displaced downward by the action of the gravity and magnet M on the displacement enlarging plate T. Fig. 4 shows an enlarged view of this function. It is understood from this view that the displacement enlarging plate T plays an important role of conveying the information of fastening and looseness. Here, the washer holding plate I playing an important role of conveying the information of fastening and looseness has adequate stiffness enough not to be deformed.

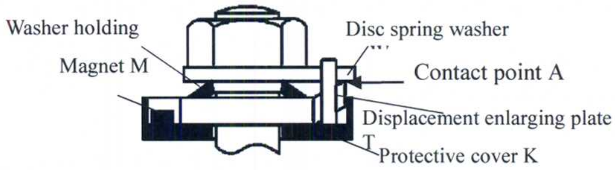


Fig. 3 Enlarged view of the special washer

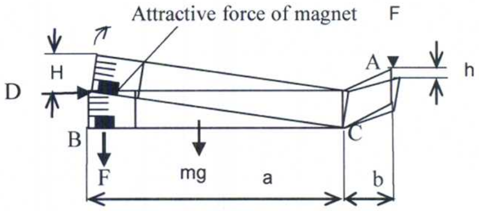


Fig. 4 Displacement enlarging plate T

3. Fastening Displacement and Looseness Displacement

The axial force of the tightened bolt, which cannot be read directly, is generally grasped indirectly by using a torque wrench. In this study, the special washer, the micro-elongation of which is enlarged double by way of leverage, is experimentally evaluated and the effectiveness of the special washer is verified. Fig. 5 shows the experimental data of the axial force and displacement of the special washer furnished by the partner business enterprise to the experiment. Ffmax is the maximum axial force point when the disc spring washer W is closely attached to the fastened element. Ffmin is the minimum axial force point, below which the looseness is not permitted. Hmax is the maximum tightening displacement point in response to the axial force, and Hmin is the looseness boundary displacement point. The axial force Ffk is an axial force deficiency alarm point, which is in response to the looseness alarm displacement point Hk. Ffk, being positioned before the looseness boundary displacement point Hmin, plays a role of preventive maintenance by issuing an alarm.

Therefore, the period between Hk and Hmin is the maintenance respite period Hm, which requires maintenance to eliminate looseness between the time when the alarm is issued to the time when the looseness boundary point is reached.

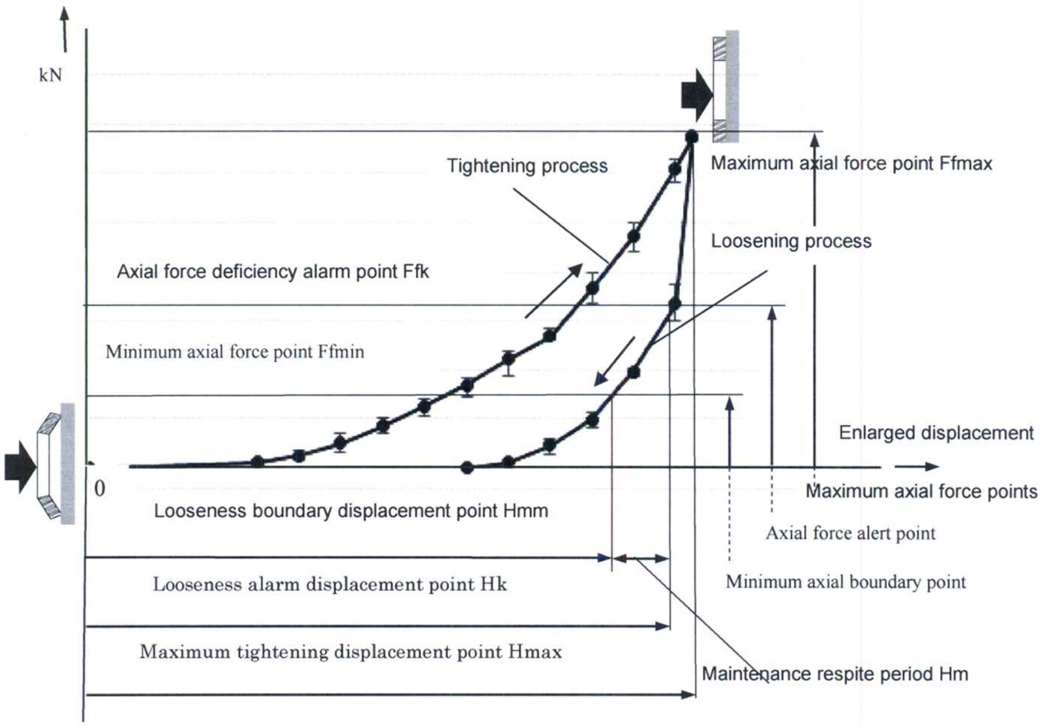


Fig. 5 Experimental data of the axial force and displacement of the furnished special washer

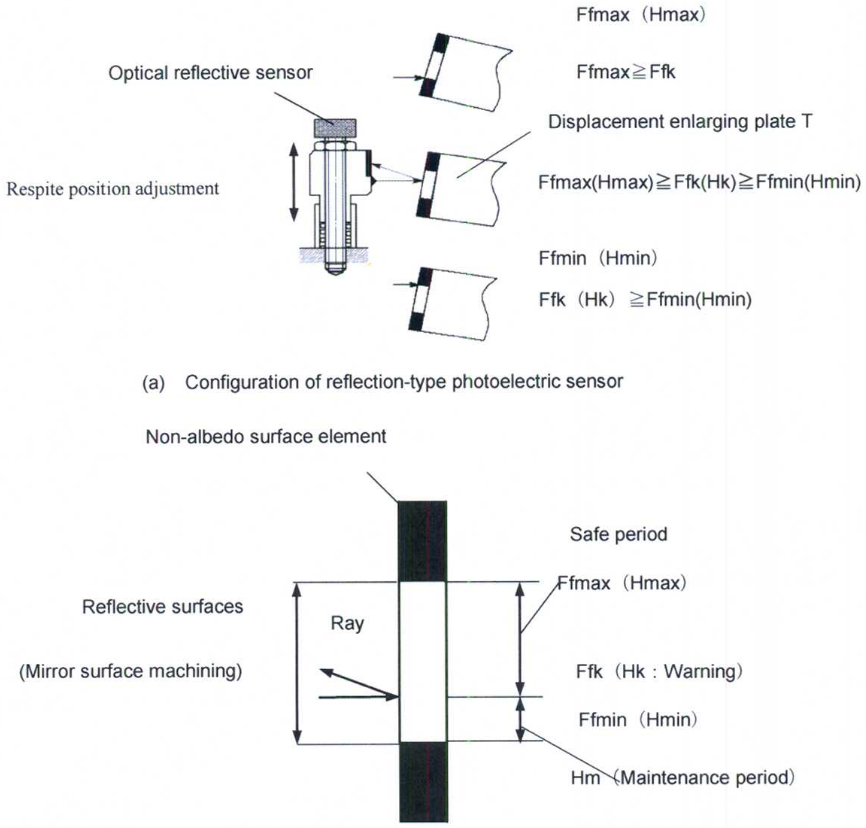
4. Configuration of Safety-Confirmation Type to Realize Fail-Safe

Among the important elements for realizing fail-safe are safety-confirmation type and non-symmetric failure[4]. The safety-confirmation type "permits a dangerous act only when safety information is notified." In the case of the special washer, only when the displacement enlarging plate T is protruded upward and the tightening axial force is within the allowable range, the safety information is continuously notified. The downward displacement means looseness, which further means danger due to the lowering of the axial force, and the downward displacement below the looseness boundary displacement point Hmin is not permitted. On the other hand, the non-symmetric failure is represented by the use of physical phenomenon, such as infallible gravity. It is a type of failure that certainly falls into one side. Since the displacement enlarging plate T of the special washer always acts downward due to the gravity acting on the tension spring and the displacement enlarging plate T, the special washer failure notifies the safe failure. In this case, the safety information is no longer notified, which is judged as "having loosened," and the fastened element should be maintained immediately.

As described above, the bolt looseness is configured to be a failure on one side of non-symmetric failure, i.e., safety side. In order to realize the non-symmetric failure of the special washer, safety-indicating energy should be maintained on a high level but should pass out of existence upon the looseness occurrence. Article 4.5 of ISO 12100-2, international basic standards for safety, defines the "positive mechanical fastening" as the "fastening that acts on other mechanical component when mechanical components contact directly each other or via some synthetic element." The special washer proposed in this study conforms with this standard.

5. Considerations of Looseness Detection by Using an Optical Beam Sensor

Supposing that bolts are tightened by human labor, a method of using an optical beam sensor for looseness detection is considered. Fig. 6 shows a configuration using a reflective sensor, and also the layout on the reflective-plate side of the displacement enlarging plate T. Ffmax (Hmax), Ffk (Hk) and Ffmin (Hmin) show the relation between the axial force and the displacement. The bolt is tightened at the Ffmax (Hmax) point. In case of looseness occurrence due to various factors as the time passes, the bolt looseness exceeds the designed value range at the Ffmin (Hmin) point into the dangerous state. To prevent this, Ffk (Hk) is positioned above the Ffmin (Hmin) point to have a role of alarm and notification. Maintenance is requested before Ffk (Hk) reaches Ffmin (Hmin).


Ffmax（Hmax）
Optical reflective sensor
Ffmax≧Ffk
Displacement enlarging plate T
Respite position adjustment
Ffmax(Hmax)≧Ffk(Hk)≧Ffmin(Hmin)
Ffmin（Hmin）
Ffk（Hk）≧Ffmin(Hmin)
Non-albedo surface element
Safe period
Ffmax（Hmax）
Reflective surfaces
Ray
(Mirror surface machining)
Ffk（Hk：Warning）
Ffmin（Hmin）
Hm（Maintenance period）

(a) Configuration of reflection-type photoelectric sensor

(b) Displacement enlarging plate T

Fig.6 Configuration of reflection-type photoelectric sensor

6. Conclusion

Focusing on the maintainability of looseness in bolt fastening, the authors have studied a special washer that can detect the bolt looseness by using a "mechanism for enlarging displacement by applying the principle of leverage." The axial force is change in the internal stress, which cannot be read directly on the site of bolt tightening. In this study, the authors tried the special washer that enlarged the displacement of the disc spring washer by applying the principle of leverage. This method enables determination whether the visual judgment of bolt looseness is "safe (S = 1)" or "dangerous (S = 0)." However, because "dangerous (S = 0)" means that the axial force is already zero and the fastened state contains a risk, it requests immediate maintenance. In the elements fastened by bolt tightening, there is no choice but to resort to electric signal to detect the micro-period of transition from "safety (S = 1)" to "danger (S = 0)." In this study, detection was tried by using a reflection type photoelectric sensor. Since the detection of bolt looseness depends on the restoring force of the disc spring washer, the displacement amount under load is important. From the experiment results, though the displacement amount is minute, when the principle of leverage is applied to the enlargement of the displacement amount, the minute displacement can be confirmed. The primary use of the special washer is not for the holding of the axial force but as maintenance signal in case of bolt looseness occurrence. If the alert of bolt looseness is issued, immediate maintenance is required. The disc spring washer used for this study is so small in displacement amount, it is inevitable that the special washer body should be upsized to raise the enlargement factor. The authors believe that if this problem is solved, more precise visual judgment can be expected, which will lead to higher efficiency.

References

1)"Twenty-four Wheel Dropout Accidents of Large-sized Vehicles due to Wheel Cover or Bolt Break in 2012," MLIT News Report ; "Bolt Drops from Play Equipment, Causing Light Injury," Asahi Shimbun, morning edition, Apr. 30, 2012; "Bolt Drops from Coaster," Asahi Shimbun, morning edition, Dec. 6, 2010

2) Akira Yamamoto: Principle and Design of Fastening," Yokendo , 1996

3) Isamu Yoshimoto (Editor): Points of Design of Thread Tightening," JIS, 1992

4) Masao Mukaidono: Safety Technology in the Future, JISHA, 2000

Setting-up a Virtual Reality Simulation for Improving OSH in Standardisation of River Locks

Peter Nickel[a], Rolf Kergel[b], Thilo Wachholz[c], Eugen Pröger[d], Andy Lungfiel[a]

[a] Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), Sankt Augustin
[b] German Social Accident Insurance Institution of the Federal Government and for the Railway Services (UVB), Münster
[c] Federal Waterways and Shipping Administration (ASt Mitte), Hannover
[d] Federal Waterways and Shipping Administration (FVT), Koblenz

Abstract

The German network of waterways of some 7400 km with about 450 lock sites requires continuous attention and activities while ensuring high level of operational availability and occupational safety and health (OSH). With consideration of best practice standards for river locks of the future it should be possible to improve the quality of the network, to draw upon spare capacity for increasing freight transport volumes and to reduce costs across the life cycle. Standardisation in river lock design has been established referring to several lock components (e.g., gates, inspection safety closings, bollards). A project has been launched to strengthen the impact of OSH in the standardisation of river locks in their future contexts of use; referring to European Directives on machinery safety and on safety and health of workers at work.

A virtual reality (VR) simulation model based on plans for a new river lock site will be used for assessing risks and for providing measures to reduce risks compatible with component standardisation and OSH requirements. The procedure of setting-up a VR model will be guided along (1) purposes for setting up a VR model, (2) the context of use, (3) scenarios, (4) relevant information and its sources, (5) model components (6) means to enable human-system interaction, (7) merging of model elements into a VR master model, (8) usability of the VR model, and (9) virtual river lock support for risk assessment. The procedure presented is specific, as it will result in a VR model for a standardised river lock in Germany; however, it is also generic as it can easily be adapted for model development of any other machinery or work system.

Keywords:

Modelling and Simulation, Risk Assessment, Machinery Safety, Usability, Safety Through Design

Introduction

The German network of waterways of some 7400 km with about 450 lock sites requires continuous maintenance, development and services while ensuring high levels of operational availability and occupational safety and health (OSH) [1]. Future river locks should consider best practice standards to improve the quality of the network, to draw upon spare capacity for increasing freight transport volumes and to reduce costs across the life cycle. Standardisation in the given context has given high priority and refers to several lock components such as gates, inspection safety closings, and bollards [16], to name but a few; being selected based on best practice, experience and expertise in river lock construction for inland waterway transportation.

Risk assessments for river locks are mandatory with regard to the Machinery Directive (2006/42/EC) [18]. They are also required for operational acitivites according to the OSH Framework Directive (89/391/EEC) [24]. Although both types of risk assessments refer to design requirements and address risks with regard to human interaction with machinery, the first focusses on designing safe machinery and the latter focusses on machinery operation in the context of use. Integration of risk assessment in a process of component standardisation for river locks may therefore not only improve OSH but also has additional advantages. This is because re-design due to safety issues would be highly resource-demanding, if not impossible, when river lock construction has already been completed. As digital technologies become widely used in machinery design and in construction [Zhou et al. 2012], tools and processes for digital models are developed and improved to support collaborative activities in OSH such as risk assessments.

The German Social Accident Insurance Institution of the Federal Government and for the Railway Services (UVB) launched a project to strengthen the impact of OSH on the standardisation of river lock components in their future context of use. The aim of the research is to perform risk assessments of river locks of the future, including standardised components and referring to European Directives on machinery safety and on safety and health at work (see also IFA5135 at www.dguv.de/ifa/sutave). The research issues presented here is to inform about the development of a dynamic virtual reality (VR) model of a future river lock with standardised components as a highly crucial step with serious consequences for the support of risk assessment and for recommendations on OSH design improvements in early stages of design.

Development of a simulation model

Risk assessments in practice often benefit from considering on-site operations and from accessing functional knowledge, experience with similar technology, mental simulation and imagination in order to compensate for incomplete predictions of machinery in future contexts of use [31]. Increasingly, this is supported by model based animation and simulation methods for machinery components (e.g. 3D CAD), for whole machinery (e.g. mock-ups), in dynamic operations (e.g. operational states) and contexts of use (e.g. work system) [4, 14]. VR modelling and simulation has been considered an initial step for conducting risk assessments of a standardised river lock within specified future contexts of use and in line with [9]. This calls for an iterative multi-step procedure in model set up referring to systematic approaches and recommendations available from studies in similar contexts [11, 2, 14, 17, 19, 22]; as developed, agreed upon and presented in the following subchapters:

1. Clarify and specify purposes for setting up a VR model
2. Understand and describe the context of use
3. Define and select scenarios
4. Select all relevant information and identify the source of information
5. Design model components and specify level of detail
6. Specify and develop procedures/ means for human-system interaction within scenarios
7. Merge model components, environments, dynamics and interactions into a VR master model
8. Evaluate the usability of the VR model
9. Apply the VR model for risk assessment support

Clarify and specify purposes for setting up a VR model

VR models are used for different purposes such as visualisation of past, present or future design solutions or as interactive environments for testing, studying and controlling system design components or as training facility [13]. Unfortunately, it is not always possible to use one VR model for different purposes (i.e. testing and training). In the given research the VR model should primarily allow for risk assessment support based on the Machinery Directive (2006/42/EC) [18] as well as on the OSH Framework Directive (89/391/EEC) [24]. Performing the risk assessments should also be similar to real life situations with a range of different scenarios available for on-site inspections at the virtual river lock. The VR model is intended to assist and to support risk assessments by inspectors experienced in OSH assessments and in operational concepts of river locks.

Understand and describe the context of use

It is important to know how the overall system should work and what may happen during operation as well as who is involved and is doing what and when with technical system components. This is best specified in terms of the context of use [8], describing the users, tasks, equipment, and the physical and social environment in which a product is used [7]. Methodological support for task or activity analyses is provided by [6] and [10, see also 12].

In the given research, potentially relevant users of river locks could be seen as personnel working at the river lock for inspection, maintenance and control as well as others, such as personnel of river barges, crews of private boats and emergency services. All tasks, activities and potential incidents at a river lock should briefly be described, including normal operations (e.g. locking barges, maintenance of lock gates, transportation of floating debris) and abnormal operations (e.g. collision of barge with lock components, failures of technical system components). Since the given project refers to OSH assessments, it may even be relevant to identify contexts of use over the machinery life cycle from putting into operation, operation, maintenance, until demolition or recycling (see Figure 1). At this section no restrictions are required for context of use descriptions. Reasonable explanations for reductions should be given, however, when selecting and describing use cases and scenarios.

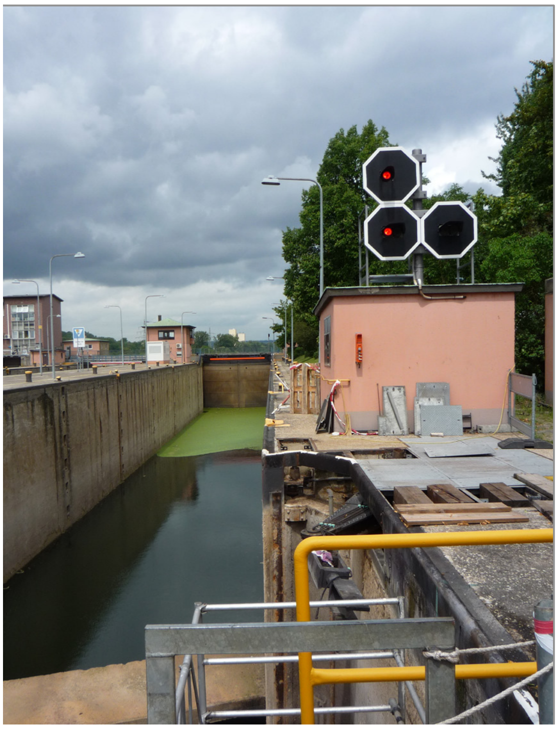


Figure 1: River lock chamber during maintenance work [Foto: Nickel/IFA]

Define and select scenarios

Scenarios are seen as procedures of tasks or activities at work that should specifically be addressed during application of the VR model. Descriptions usually refer to all individual components and how they are related in static and dynamic situations. They include storyboards on documentation of sequences of events.

In the given research this refers to scenarios relevant for OSH risk assessments at the virtual river lock using standardised components. Scenario specification and selection is required since not all variations in contexts of use will be represented in individual scenarios. VR modelling, however, allows for more different and flexible switching between scenarios than usually available at a time in reality. OSH assessments may require referring to systems design both before putting into operation and during normal and maintenance operations under various conditions. Unforeseen situations, however, as occurring in real life, cannot properly be modelled and simulated for lack of information about the sequence of events.

Once the VR model is available for application, it may require some additional resources to include new scenarios due to lack of system components or functionality or interactivity.Therefore, a discussion about criteria for scenario selection is seen helpful to avoid disappointments about limitations of the VR model for risk assessment support. Relevant criteria could be (a) typical tasks, (b) accident prone situations or (c) core hazardous situations, (d) common tasks, (e) situations involving many operators, (f) situations that refer to many components or the whole system, (g) situations that refer to specific components of the machinery, (h) operational concepts, to name but a few.

For risk assessment support of river locks a mixture of several criteria should be taken into account. As the most typical and common task, scenarios for upstream as well as downstream locking of ships will be included. In addition, draining dry of a river lock for maintenance work at lock gates should be available, since it is accident prone, includes many hazards, involves many operators and requires additional equipment at the worksite. Finally, several other scenarios will more specifically address standardised components during locking of barges and during maintenance procedures (see Figure 2). The VR model should therefore also comprise specific functionality and interactivity.

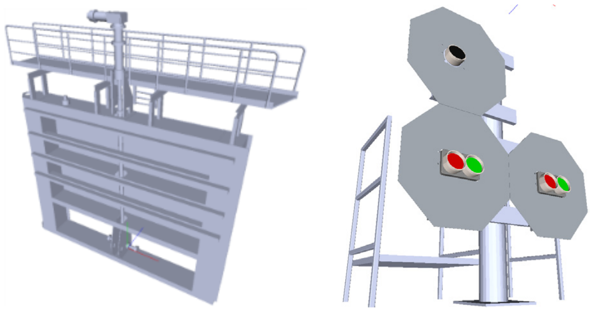


Figure 2: River lock components.

Select all relevant information and identify the source of information

For modelling and simulation, virtual scenarios require digital data in a quality not always at hand in reality. Data required for a specific scenario will not be readily available for use; however, some data for components may. Identification of potential sources of relevant digital information therefore supports scenario composition and development. Since planning and construction of technical equipment nowadays often is processed in software, scenario components may be available from manufacturers or from vendors providing 3D CAD formats and solids. Scenarios can therefore be created based on 3D model components, complemented with components manually prepared using 3D CAD software.

This is similar in the given project. The first river lock including several standardised components is still under planning. As far as accessable, 3D model components from the waterways and shipping administration would be suitable, however, for planning processes most often 2D and electronic or paper drawings are seen sufficient. Besides, river locks in general consist of several components related to mechanical engineering (e.g. hydraulic jacks) or others related to construction engineering (e.g. pier or steel piling). Across domains, software programmes and data formats often are different. When engineering offices get a tender for developing planning information, they often internally work with 3D, but provide specific 2D format as required by administration. Model components not available or not suitable due to formatting therefore require redesign. 3D CAD will then be used for development based on paper drawings or other information available from the waterways and shipping administration.

Design model components and specify level of detail

All model components need some editing before they can be integrated in a VR master model [30]. This refers to models in 3D CAD format and decisions about the level of detail required for VR application. It also refers to a VR software toolkit and decisions about functionality for animation and control to be integrated.

A high quality data set with design components representing real planning data has been rated important in the given project. Therefore, all VR model components will initially be made available in 3D CAD (Solid Works, USA) format. This format is used for editing and redesigning components. Editing is required for adaptations of last minute changes with regard to the planning state, but it is also related to simplifying components and making them more suitable for the given VR applications. VR model components should require low processing resources and contain as few as possible polygons; i.e. CAD solids without inside information, if possible. In case movement of parts is required, some details need still be available to demonstrate mechanisms and movements (e.g. sliding panel in lock gate).

The project refers to three sources for model components. The main source will potentially be 3D CAD already available. CAD files are divided into individual components and edited to get CAD solids. Another source is related to additional or environmental components (e.g. barges, cranes, trees, and buildings) that can be purchased and integrated from 3D model vendors or from former VR applications. The most labour-intensive components are those not yet available in 3D CAD format. Design and redesign of components based on 2D planning information available is required. All model components will be made available in Virtual Reality Modeling Language (vrml) format for import into the Vizard Virtual Reality Toolkit (WorldViz LLC, USA).

Specify and develop procedures/ means for human-system interaction within scenarios

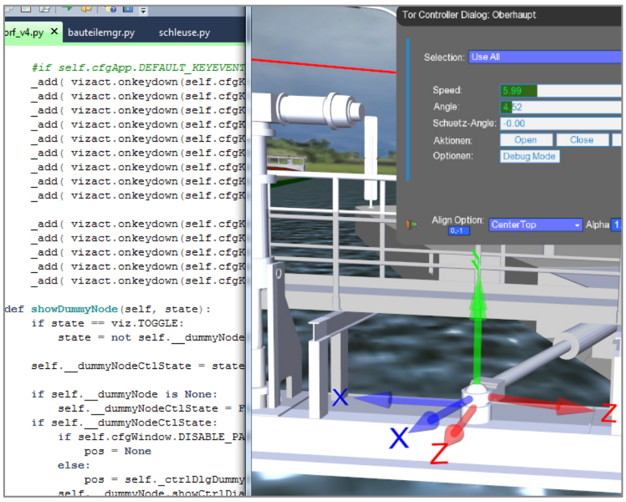
Another important issue in the development of a dynamic VR model is the specification of sequences of events and dynamics within scenarios and how to control them [27]. It is fundamental since it addresses requirements for appropriately performing risk assessments associated with machinery involved in work tasks and activities. Information about actions and processes are provided by the context of use analysis, scenario descriptions and storyboards. VR programming also refers to physical processes (e.g. systems for moving or changing) and allows interactive simulation. Dynamics will be implemented into VR model components. Integration of controllers in terms of graphical user interfaces enable input and trigger events.

Among the most complex scenarios is the locking of barges, because it includes the machinery as a whole and requires movements and changes of several components of the river lock (e.g. gates, bollards, signalling) as well as the environment (e.g. barges, sound, water). Variations of natural speed of movements would be helpful to support realisms while at the same time benefit from simulation systems. Options like speeding up or replaying sequences have been shown advantageous for effectively performing risk assessment [25]. They are considered a specific requirement for assessing risks associated with moving parts of machinery.

Several tools in terms of preferably graphical user interfaces are required in VR to support risk assessments according to requirements. They should serve purposes such as

- switching between points of view, changing inspection places and walking fast (e.g. predefined bird view, on the pier or under water, potentially hazardous areas),
- triggering predefined movements of various moving parts of the river lock within a context of use (e.g. opening gate),
- triggering procedures according to storyboards (e.g. do not switch to green signalling before gate is clear),
- reviewing crane access on the river lock (e.g. space requirements for crane and material loaded),
- viewing design alternatives (e.g. downstream gate collision protection by cable or bar),
- taking pictures or videos for documentation (e.g. of identified hazard),
- controlling wheather conditions at the river lock (e.g. sunshine, artificial lightning), and
- taking 3D tape and other measures in the virtual environment (e.g. height of guardrails, width of emergency exits).

In the present research, Python (Python Software Foundation, USA) and the Vizard Virtual Reality Toolkit are used for the development of procedures and means for human-system interaction including tools required to support interactions (see Figure 3). The software also implements kinetics and animations for moving parts of machinery (e.g. lock gates, water level). As a result all model components should be available in appropriate format and size to build a master model in VR.



```
    #if self.cfgApp.DEFAULT_KEYEVENT
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK

    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK
    _add( vizact.onkeydown(self.cfgK

def showDummyNode(self, state):
    if state == viz.TOGGLE:
        state = not self.__dummyNode

    self.__dummyNodeCtlState = state

    if self.__dummyNode is None:
        self.__dummyNodeCtlState = F
    if self.__dummyNodeCtlState:
        if self.cfgWindow.DISABLE_PA
            pos = None
        else:
            pos = self._ctrlDlgDummy
        self.__dummyNode.showCtrlDia
```

Tor Controller Dialog: Oberhaupt

Selection: Use All

Speed: 5.99

Angle: 4.52

Schuetz-Angle: -0.00

Aktionen: Open Close

Optionen: Debug Mode

Align Option: 0,-1 CenterTop Alpha 1

Figure 3: Modelling systems and including control for dynamics of the virtual river lock.

Merge model components, environments, dynamics and interactions into a VR master model

The VR master model will be close to the virtual environment for conducting risk assessments of river locks with standardised objects. All model components available will be fed into a database with information about file name and location, coordinates and orientation within the virtual environment and settings for presentation and scenario control. Some of the components are available in different versions (e.g. downstream gate collision protection by cable or bar), some have different options for visualisation (e.g. caverns covered or not) and others are available with the VR toolkit needing adaptation and specification (e.g. environmental models for water, sky, lightning, sound, gravity).

VR applications available also require coding for moving and navigating in the environment (e.g. walk on river lock, switch points of view), for taking 3D measurements at the virtual river lock (e.g. flexible tape measure), and for virtually manipulating and controlling components and scenarios (e.g. user interface for locking of barges). In addition, some functionality for documenting activities in the VR laboratory during OSH assessments has also seen useful (e.g. taking pictures and screen shots, videotaping sessions and logging of activities).

Evaluate the usability of the VR model

In general, design efforts in human system interaction including the concept of usability have undergone a shift from being computer-oriented and programme-oriented to being more focused on the actual context of use [3, 29]. VR applications can suffer from severe usability problems such as disorientation and lack of manipulation functionality resulting in low external validity [28]. Therefore, a dynamic VR model including all options and tools (see Figure 4) should undergo a usability evaluation before conducting a risk assessment by a team of inspectors.

Inspection methods such as cognitive walkthrough and heuristics have already successfully been used for evaluations of VR models [28, 15] and refer to analytical techniques in formative evaluations for improving ergonomics design quality and human-system interaction [20]. In addition, design recommendations for conducting risk assessments in VR should be taken into account during model development [25, 22, 5, 26]. Ideally the evaluation should also consider the location for conducting the assessment (e.g. VR lab; see www.dguv.de/ifa/sutave).The evalution should be embedded in a design review for integrating VR functionalities and procedures in the design and verification process for model development.

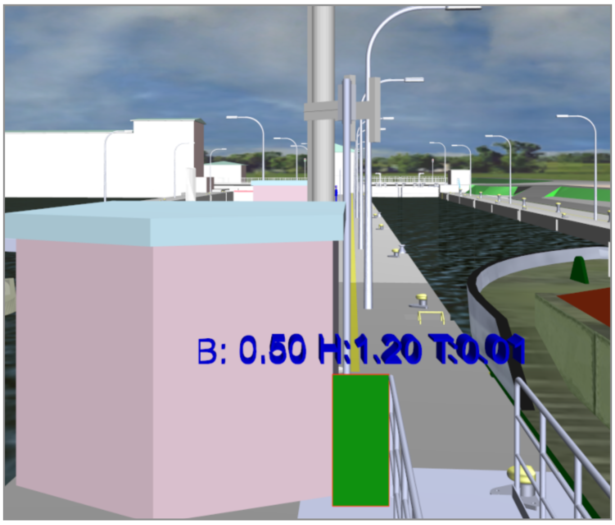


Figure 4: Taking 3D tape measures (green box) at the virtual river lock.

Apply the VR model for risk assessment support

After having successfully conducted a usability evaluation the VR model is available for application. In addition to decisions about media to choose for applications (e.g. computer monitor, VR lab, head mounted display) preparations are also required for conducting the risk assessment. Relevant issues are questions about what, who, why, when, how addressing among others scenarios, interactions, number of inspectors, basis for decision making, decision making process, tools required, time frame, and documentation.

Discussion

A procedure for setting up a VR master model to support risk assessments has successfully been developed and agreed upon. With regard to the project on OSH improvements for standardised river locks in early stages of design it has already been possible to initiate the process. The main purpose of the VR model has been specified as application for risk assessment support. The context of use within the given project is restricted to new constructions of river locks for inland waterway transportation that takes into account recently standardised components.

Though there are potentially many scenarios relevant for risk assessments, the number of scenarios has been limited. It was important to provide scenarios to investigate requirements related to both the Machinery Directive and the OSH Framework Directive. As a rather generic scenario upstream and downstream locking of barges has been selected. With a view to Machinery Directive it was seen important to start with aft and head of the river lock and to concentrate on both the mechanical and construction engineering part of the machinery and their interactions. With a view to the OSH Framework Directive it was seen important to focus on maintenance operations with several operators involved (e.g. draining of river lock and gate maintenance) and on safety issues with regard to the lock superstructure (e.g. guard railing, maintenance for lightning and camera systems). With an emphasis on prevention through OSH design at river locks it is important to take a complement approach with regard to risk assessments and design requirements from both Directives.

Further steps will build on experiences from former projects [23, 25] and from above mentioned sources. Some clear advantages of the presented approach have already been demonstrated. The procedure presented is specific, as it will result in a VR model for a future river lock with standardised components in Germany; however, it is also generic as it can easily be adapted for model development of any other machinery or work system.

References

[1] BMVI (2014). *Verkehrsinvestitionsbericht für das Berichtsjahr 2012* [Report on traffic investments for 2012]. Deutscher Bundestag, Drucksache 18/580, 18/02/2014

[2] Bouchlaghem D., Shang H., Whyte J., Ganah A. (2005). Visualisation in architecture, engineering and construction (ACE). *Automation in Construction 14*(3), 287-295

[3] Bowman D.A., Gabbard J.L., Hix D. (2002). A survey of usability evaluation in virtual environments: Classification and comparison of methods. *Presence 11*(4), 404-424

[4] Ciccotelli J., Marsot J. (2005). Réalite virtuelle et prévention. Apports et tendances. *Hygiènes et sécurité du travail 199*(2), 99-111

[5] Dźwiarek M., Grabowski A., Jankowski J., Strawinski T. (2013). *Analysis of usability of the VR technology for risk assessment in machinery design*. In Proceedings of EMET 2013 (146-153), Sep 28-30, Venice, Italy

[6] EN 614-2:2000. *Safety of machinery - Ergonomic design principles - Part 2: Interactions between the design of machinery and work tasks*. Brussels, CEN

[7] EN ISO 6385:2004. *Ergonomic principles in the design of work systems*. Brussels, CEN

[8] EN ISO 9241-210:2010. *Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems*. Brussels, CEN

[9] EN ISO 12100:2010, *Safety of machinery – General principles for design – Risk assessment and risk reduction*. Brussels, CEN

[10] EN 16710:2014. *A methodology for work analysis to support design (draft).* Brussels: CEN

[11] EN 61160:2005, *Design review.* Brussels, CEN

[12] Fadier E. (2015). *Ergonomics – A methodology for work analysis to support design (prEN 16710:2015).* Presentation on the 8th International

Conference on Safety of Industrial Automated Systems (SIAS 2015), Nov 18-20, Königswinter

[13] Hale K.S., Stanney K.M. (Eds.) (2015). *Handbook of virtual environments: Design, implementation, and applications.* Boca Raton, CRC Press

[14] Helin K., Evilä T., Viitaniemi J. et al. (2007). *HumanICT. New Human-Centred Design Method and Virtual Environments in the Design of Vehicular Working Machine Interfaces*. Tampere, VTT

[15] Jacko J.A. (Ed.) (2012). *The human-computer interaction handbook: Fundamentals, evolving technologies and emerging applications*. Boca Raton, CRC Press

[16] Jander A. (2012). *Aktuelle Situation der Standardisierung von Schleusen.* In Bericht des Kolloquiums Innovation mit Tradition: Hydraulischer Entwurf und Betrieb von Wasserbauwerken (33-38), July 4-5. Karlsruhe, Bundesanstalt für Wasserbau (BAW)

[17] Määttä T.J. (2007). Virtual environments in machinery safety analysis and participatory ergonomics. *Human Factors and Ergonomics in Manufacturing 17*(5), 435-443

[18] Machinery Directive 2006/42/EC of the European Parliament and the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast), *Official Journal of the European Union L 157*, 09/07/2006, 24-86

[19] Marc J., Belkacem N., Marsot J. (2007). Virtual reality: A design tool for enhanced consideration of usability 'validation elements'. *Safety Science 45*, 589-601

[20] Nickel P., Nachreiner F. (2010). *Evaluation arbeitspsychologischer Interventionsmaßnahmen* [Evaluation of interventions in work psychology], In U. Kleinbeck, K. Schmidt (Eds.), Arbeitspsychologie (Enzyklopädie der Psychologie, D, III, 1) (1003-1038). Göttingen, Hogrefe

[21] Nickel P., Lungfiel A., Huelke M., Pröger E., Kergel R. (2012). *Prevention through design in occupational safety and health by risk assessment of virtual river locks.* In Proc. SIAS 2012 (35-40), Oct 11-12, IRSST, Montréal, Canada

[22] Nickel P., Pröger E., Kergel R., Lungfiel A. (2014). *Development of a VR planning model of a river lock for risk assessment in the construction and machinery industry.* In G. Zachmann, J. Perret, A. Amditis (Eds.), Conference and Exhibition of the European Association of Virtual and Augmented Reality. Geneve, The Eurographics Association

[23] Nickel P., Pröger E., Lungfiel A., Kergel R. (2015). *Flexible, dynamic VR simulation of a future river lock facilitates prevention through design in occupational safety and health,* In Proc. IEEE VR 2015 (385-386), Annual International Symposium on Virtual Reality, Mar 25-27, Arles, France

[24] OSH Framework Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work. *Official Journal of the European Union L 183*, 29/06/1989, 1-8

[25] Pröger E., Nickel P., Lungfiel A. (2015). Risikobeurteilung nach Maschinenrichtlinie an einer virtuellen Neckarschleuse [Risk assessment of a virtual lock at River Neckar according to Machinery Directive], *Der Ingenieur 54*(2), 9-13

[26] Santos I.J.A., Grecco C.H.S., Mol A.C., Carvalho P.V.R. (2009). The use of questionnaire and virtual reality in the verification of the human factors issues in the design of nuclear control desk. *International Journal of Industrial Ergonomics 39*, 159-166

[27] Stanney K.M., Mollaghasemi M., Reeves L., Breaux R., Graeber D.A. (2003). Usability engineering of virtual environments (VEs): Identifying multiple criteria that drive effective VE design. *International Journal of Human-Computer Studies 58*, 447-481

[28] Sutcliffe A.G., Deoul Kaur K. (2000). *Evaluating the usability of virtual reality user interfaces*. Behaviour & Information Technology 19(6), 415-426

[29] Westerdahl B., Suneson K., Wernemyr C., Roupé M., Johansson M., Allwood C.M. (2006). Users' evaluation of virtual reality architectural model compared with the experience of the completed building. *Automation in Construction 15*(2), 150-165

[30] Whyte J., Bouchlaghem N., Thorpe A., McCaffer R. (2000). From CAD to virtual reality: Modelling approaches, data exchange and interactive 3D building design tools. *Automation in Construction 10*(1), 43-55

[31] Williams M.J. (2000). *Application of virtual reality for risk assessment and training in the minerals industry* (Doctoral thesis), University of Nottingham

[32] Zhou W., Whyte J., Sacks R. (2012). Construction safety and digital design: A review. *Automation in Construction 22*, 102-111

Corresponding address

Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA),
Alte Heerstraße 111, D-53757 Sankt Augustin, Germany,
Email peter.nickel@dguv.de, Tel. +49 (0)2241 2312832

A Study of Safeguarding Based on Human Body Communication Technology

Kohei OKABE[a]

[a] *JNIOSH (National Institute of Occupational Safety and Health, Japan)*

Abstract

A way to utilize radio sensors communicating via human body is discussed to ensure the safety of human-machine cooperative working. Radio sensors can be one of useful safeguards as well as trip-sensors in such environment where a physical contact between humans and machinery may result in severe injury. They can contribute to safety monitoring to prevent such hazardous contacts, for instance, by giving warnings to humans. Such warnings reduce the possibility of injuries whereas contact detections by touch-sensitive sensors decrease severity of injuries.

Keywords:

Human body communication; Hazardous contact; Contactless communication

Introduction

Ordinary radio sensors have difficulties to reproduce reliable responses. Unstable responses easily affect both safety and usability. Technique to satisfy both of them is principal subject of utilizing radio sensors as safeguards. Long distance communication is sensitive to noises. Radio sensors interfere each other in the communication. Short distance communication performed by physical property in nature is applicable. Human body communication [1] in which human body works as a radio antenna is a kind of near filed communication. A measure based on the communication to support safe working is proposed in this study.

Method

Good example of human body communication is keyless entry to open vehicle doors. It allows drivers to unlock doors by just touching with a finger. This example implies that human body communication can provide contact sensing. General human body communication systems transmit signal by inducing current in human body. They require electrical contact to do communication.

In terms of safeguarding against hazardous contact such as shearing or compression, contactless presence (precontact) sensing is more adequate measure. Contactless human body communication can contribute to reduce risk as well as pre-crash control system for vehicle safety. It can also contribute to reduce unnecessary outbreak of emergency stop. Key point for successful safeguarding is to ensure stability of contactless communication.

Devices

To realize the contactless communication, a radio sensor system generating electric field was experimentally implemented. Portability of the system is not considered. The system has a transmitter unit and a receiver unit as shown in Fig. 1. Each unit is equiped with a wired antenna. The configuration of the antennas are same. Simple cooper-plates are embedded in plastic cases. The size of the plate is 50x80 mm.

The transmitter generates impulsive waves in 30kHz. The power of transmission output is set to around 100W at DC 24V drive. The receiver drives on DC 9V and indicates received field strength.

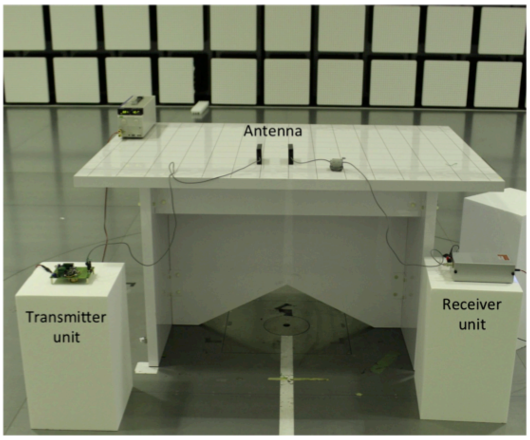


Figure 1: Developed radio sensor system

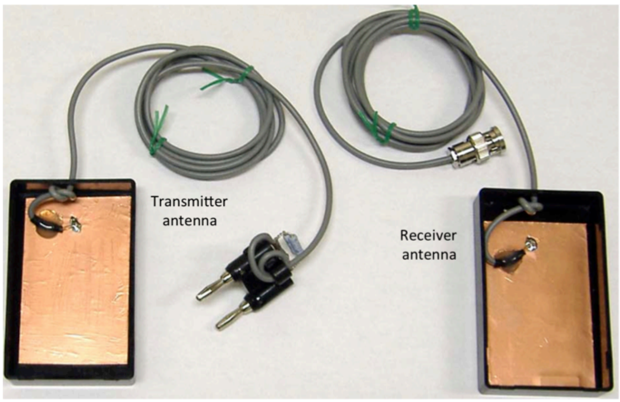


Figure 2: Antenna configuration

Experiments

Following 4 kinds of experimental communications (XMSNs) were conducted in anechoic chamber.

1. Contactless direct XMSN
2. Contact XMSN via mimic skin
3. Quasi-contactless XMSN via mimic skin
4. Quasi-contactless XMSN via human body

Experiment 1

Experiment 1 is performed to examine capability of contactless communication. Main aim of this test is to know the potential ability of electric field communication to realize contactless human body communication. Antennas are faced each other as shown in Fig. 4. Sensor signals are directly transmitted from the transmitter to the reciver. Received field strengths according to distances between the transmitter and the receiver are measured.

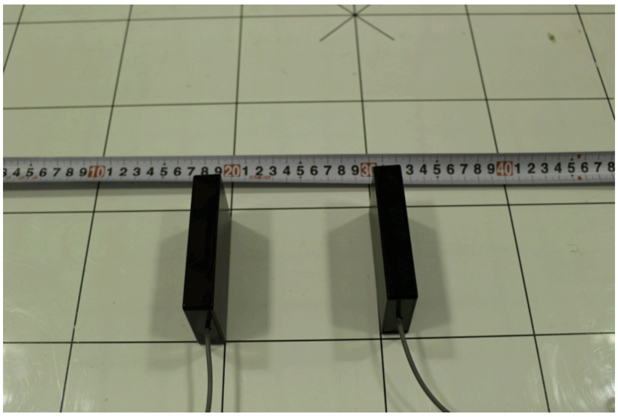


Figure 4: Initial setting of contactless direct communication

Experiment 2

Experiment 2 is capability test of contact communication via human body. Fundamental ability of electric field communication to perform human body communication is examined. Originally developed mimic skins substitute for human body. The artificial skins are made of silicone gum to reproduce permittivity of human body. Antennas are put on the mimic skin. The transmitter sends signals to the receiver through the skin as shown in Fig. 5.

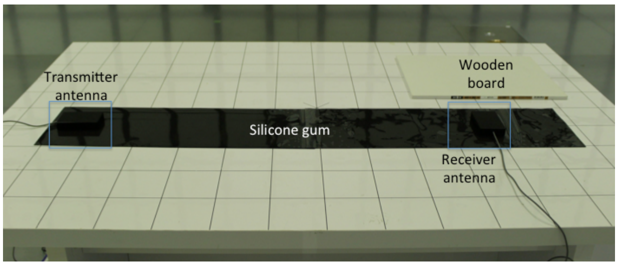


Figure 5: Setup of contact communication via mimic skin

Experiment 3

Experiment 3 is capability test of contactless communication via human body. Feasibility of electric field communication to perform contactless human body communication is confirmed. Wooden board lies between the mimic skin and the receiver as shown in Fig. 6 in order to ensure reproducibility of contactless communication. Thickness of the board is 9 mm.

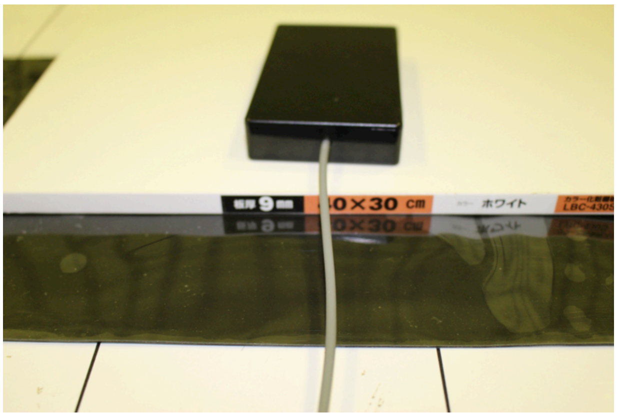


Figure 6: Setup of quasi-contactless communication via mimic skin

Experiment 4

Experiment 4 is verification of contactless communication via human body. Performance of contactless human body communication is verified. The wooden board lies between human hand and the receiver as shown in Fig. 7. Thickness of the board is 9 mm.

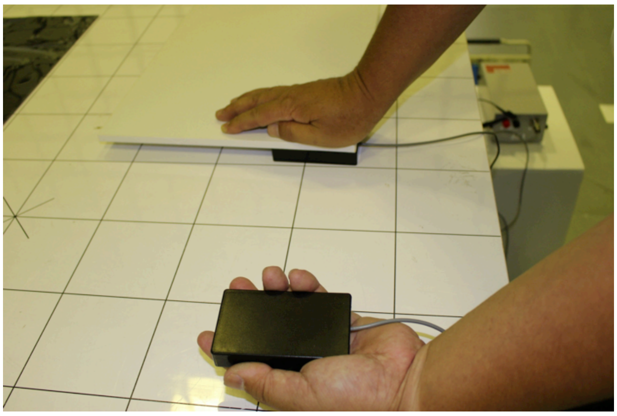


Figure 7: Setup of quasi-contactless communication via human body

Results

As a result of 4 kinds of experiments, a list of received field strengths were established as shown in Table 1. The strength 4.88V is maximum value that the receiver can indicate.

Table 1: Received field strengths of experiments

Experiment number	Condition	Intermediate	Distance	Strength
No. 1	face to face	open air	10 cm	580mV
		open air	5 cm	3.04V
		open air	3 cm	4.88V
No. 2	via mimic skin	-	-	4.88V
No. 3	via mimic skin	wooden board	9 mm	3.08V
No. 4	via human body	wooden board	9 mm	1.88V

Discussion

Experiment 1 showed sufficient potential of electric field communication to realize contactless communication. As shown in table 1, received field strength varied in accordance with the distance between the transmitter and the receiver. The variation of field strength reflects general feature of electric field communication.

Experiment 2 indicated capability of electric field communication via human body. Maximum strength was always measured anywhere on the mimic skin.

The wooden board used in the experiments 3 and 4 contributed to confirm the reproducibility of contactless communication. The monitored strengths with wooden board were stable, while the monitored strengths without wooden board were unstable. The values shown in talbe 1 is a result of the experiments under the conditoin that the receiver got signals in contact with the wooden board. The permittivity of general wood is larger than that of air. The order of wood permittivity is same level of air. Strictly speaking, the communication described in the experiments is not perfect contactless but quasi-contactless. We need to note that actual received strength of perfect contactless will be smaller than that of quasi-contactless. It means that responece area of sensors becomes narrow.

Conclusion

Contactless human body communication has a potential to behave as a barrier to protect hazardous contact. The developed radio sensor system effectively revealed the capabilities of electric field communication to realize such protective device based on human body communication technology. Main future work is portability of the system. Portable radio sensor system is going to be newly developed.

References

[1] T. G. Zimmerman. Personal Area Networks: Near-field intrabody communication. IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996

Corresponding address

okabe@s.jniosh.go.jp

Risk reduction effect of a supporting protective system for an integrated manufacturing system

Shoken Shimizu[1], Shigeo Umezaki[1]

[1] National Institute of Occupational Safety and Health,Japan

Abstract

In an integrated manufacturing system characterized by compositely combined machines, residual risks arise during severe occupational accidents.
Some machine users adopt risk reduction measures that considerably depend on worker attentiveness as a means of appropriately eliminating or reducing these risks.
However, the risk reduction effects of these measures are largely affected by uncertainty and sometimes widely differ from the results of risk assessment because of human errors and intentionally unsafe worker behaviors.
This study proposes a “supporting protective system” that serves as a counteraction to anticipated human errors and deliberately perilous acts. The system is designed to effectively prevent the errors (slips or slips in conduct) that occur during operations through the appropriate use of an information and communication technology (ICT) instrument or a combination of ICT instruments in resolving the residual risks that originate from the risk assessment performed by machine manufacturers.

Keywords:

Supporting protective system, Integrated manufacturing sysytem

Introduction

In safety standards, such as the International Standardization Organization (ISO) 12100/Japanese Industrial Standards (JIS) B 9700 (Safety of Machinery: General Principles for Design), the risk of accidents is reduced by adopting a method of basically eliminating or reducing risks, a method of separating the workers’ operation areas from a machine’s dangerous moving parts, a method of keeping workers away from dangerous regions when such parts are in motion, and a method of stopping the parts when workers enter dangerous regions.

However, in actual facilities with machines, hazardous points near operations (operations in which workers need to approach a machine’s dangerous moving parts while the parts are in motion to facilitate checking, adjustment, processing, troubleshooting, maintenance, inspections, repairs, cleaning, or removal) exist, so the risk of accidents may not be reduced appropriately by only adopting the above methods. In the integrated manufacturing system, in which multiple machines are cooperatively controlled, new risks are generated by combining facilities and machines.

Some risk reduction measures performed by machine users at work sites are strongly dependent on worker attentiveness. Such risk reduction measures are largely affected by uncertainty. When a worker makes a human error, the expected risk reduction effects cannot be exerted, and consequently, a severe accident occurs.

To increase the certainty of risk reduction measures performed by machine users at work sites, the present study proposes a supportive protection system using appropriate information and communication technology instruments, compares the system’s risk reduction effects with those of measures with risk assessment performed by machine users at work sites, and verifies the system’s risk reduction effects by performing a demonstration experiment.

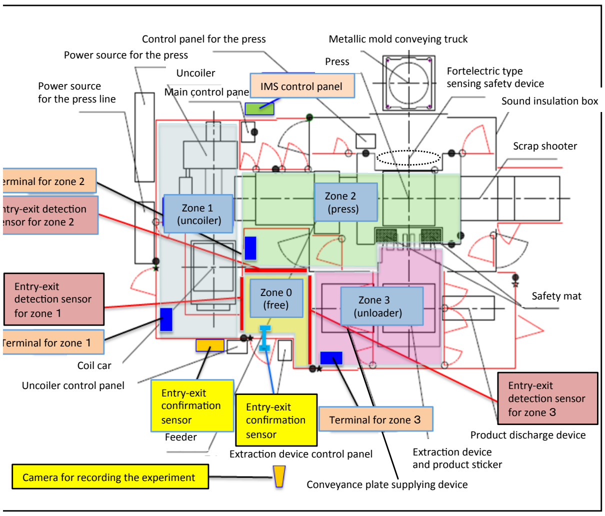
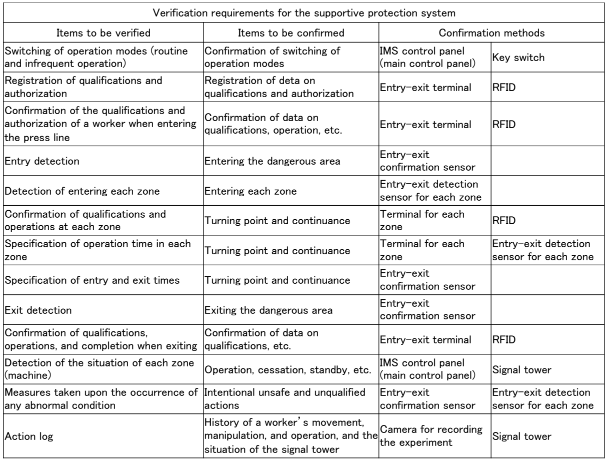

Control panel for the press
Metallic mold conveying truck
Power source for the press
Press
Uncoiler
Fortelectric type sensing safety device
Power source for the press line
Main control pane
IMS control panel
Sound insulation box
Scrap shooter
erminal for zone 2
ntry-exit detection nsor for zone 2
Zone 1 (uncoiler)
Zone 2 (press)
Entry-exit detection sensor for zone 1
Zone 0 (free)
Zone 3 (unloader)
Safety mat
Terminal for zone 1
Coil car
Uncoiler control panel
Entry-exit confirmation sensor
Entry-exit confirmation sensor
Terminal for zone 3
Entry-exit detection sensor for zone 3
Feeder
Product discharge device
Extraction device control panel
Extraction device and product sticker
Camera for recording the experiment
Conveyance plate supplying device

Figure 1 Schematic diagram of company A’s press line and the layout of experimental

Table 1 Verification requirements for the demonstration experiment



Verification requirements for the supportive protection system			
Items to be verified	Items to be confirmed	Confirmation methods	
Switching of operation modes (routine and infrequent operation)	Confirmation of switching of operation modes	IMS control panel (main control panel)	Key switch
Registration of qualifications and authorization	Registration of deta on qualifications and authorization	Entry–exit terminal	RFID
Confirmation of the qualifications and authorization of a worker when entering the press line	Confirmation of data on qualifications, operation, etc.	Entry–exit terminal	RFID
Entry detection	Entering the dangerous area	Entry–exit confirmation sensor	
Detection of entering each zone	Entering each zone	Entry–exit detection sensor for each zone	
Confirmation of qualifications and operations at each zone	Turning point and continuance	Terminal for each zone	RFID
Specification of operation time in each zone	Turning point and continuance	Terminal for each zone	Entry–exit detection sensor for each zone
Specification of entry and exit times	Turning point and continuance	Entry–exit confirmation sensor	
Exit detection	Exiting the dangerous area	Entry–exit confirmation sensor	
Confirmation of qualifications, operations, and completion when exiting	Confirmation of data on qualifications, etc.	Entry–exit terminal	RFID
Detection of the situation of each zone (machine)	Operation, cessation, standby, etc.	IMS control panel (main control panel)	Signal tower
Measures taken upon the occurrence of any abnormal condition	Intentional unsafe and unqualified actions	Entry–exit confirmation sensor	Entry–exit detection sensor for each zone
Action log	History of a worker’s movement, manipulation, and operation, and the situation of the signal tower	Camera for recording the experiment	Signal tower

Demonstration Experiment

Figure 1 shows a schematic diagram of company A’s press line and the layout of experimental devices used in the demonstration experiment.

In the press line, one press machine was placed; a zone of supplying coil-shaped materials (an uncoiler) was located before the press machine, and a zone of discharging pressed products (an unloader) was located after the press machine.

Table 1 shows the verification requirements for the demonstration experiment.

1 Experimental devices

1-1 Entry-exit terminal

The entry-exit terminal (Photograph 1) compares information about workers’ qualifications and authorization that already been registered in the terminal with data in a radio-frequency identification (RF) tag possessed by workers when they enter and exit the press line, and judges whether operation items declared by the workers are allowed based on their qualifications and authorization. Their qualifications and authorization have already been stored in a memory in the terminal as matrix-shaped data.

The entry-exit terminal is equipped with a radio frequency identification (RFID) reader/writer, which can read and write information in an RF tag possessed by a worker, a touch panel, by which a worker registers the start and end of an operation, an operation key, and a signal tower, by which the line situation can be monitored. The operation key prevents third parties from operating the terminal and allows workers possessing qualifications and authorization to perform operations in the zones.

1-2 RF tags

Four types of RF tags (A–D) were used to confirm workers’ qualifications and authorization by entry-exit and zone terminals. In the demonstration experiment, information to identify workers was input into a memory in each type of RF tag, and information about their qualifications and authorization and about zones where they are allowed to operate were input in the entry-exit terminal. Table 2 shows the relationships among the four types of RF tags and information on a worker’s qualifications and authorization and information on zones where a worker is allowed to operate.

1-3 Entry-exit confirmation sensor

An entry-exit confirmation sensor is a type of image sensor and was installed at the entry-exit door (gate) section to confirm the number of workers and their directions. The sensor adopted the time of flight system. The sensor measures the distance between the door section and a worker by projecting a near-infrared ray (850 nm) and receiving the reflected ray by the worker using a specific image sensor; thus, the entry-exit confirmation sensor is hardly affected by ambient light. Photograph 2 shows the appearance of an entry-exit confirmation sensor installed at the work site using exclusive jigs.

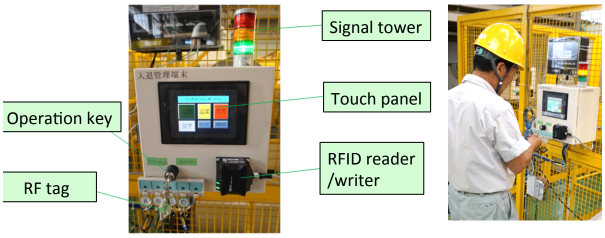


Photo 1 Appearance of the entry-exit terminal

Table 2 Relationships among RF tags and information on a worker’s qualifications
and authorization and information on zones where a worker is allowed to operate

Types of RF tags	Information on a worker’s qualifications	Information on a worker’s authorization									Information on zones where a worker is allowed to operate		
		Instructions on the press	Change of press die	Set up of the press	Adjustment of the press	Set up of conveyance	Adjustment of conveyance	Production	Repairs	Cleaning	1(UC)	2(P)	3(UL)
A	Administrator	○	○	○	○	○	○	○		○	○	○	○
B	Administrator of the press	○	○	○	○			○	○			○	
C	Administrator of the conveying machines								○		○		○
D	Cleaning person									○	○	○	○

Photo 2 Appearance of the entry-exit confirmation sensor

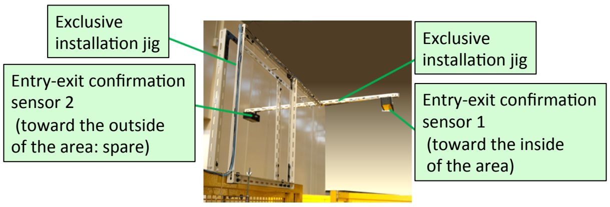
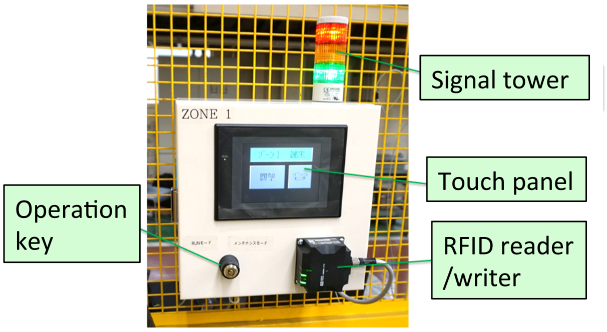

Exclusive installation jig
Entry-exit confirmation sensor 2
(toward the outside of the area: spare)
Exclusive installation jig
Entry-exit confirmation sensor 1
(toward the inside of the area)

Photo 3 Entry-exit detection sensors for zones

Photo 4 Zone terminal



1-4 Entry-exit detection sensors for zones

As an entry-exit detection sensor, a transmission-type (photoelectronic) safety sensor was installed at each of the admission ports of zones 1−3. Photograph 3 shows the entry-exit detection sensors installed for the zones (left photograph: entry-exit detection sensor for zone 3, right photograph: entry-exit detection sensors for zones 2 and 3).

1-5 Zone terminals

A zone terminal was installed for each of zones 1−3 (Photograph 4).

After entering a zone, when a worker inserts the operation key in the key hole on the zone terminal and turns on the terminal, the worker's registration is completed. Following the instructions displayed on the touch panel, the worker performs his/her identification by holding the RF tag over the RFID reader/writer and selects an operation, which has already been registered on the entry-exit operation terminal; consequently, the worker is allowed to begin the operation.

Verification of the Demonstration Experiment

Table 3 shows the dates of experiments, the number of operations, the contents of operations, the number of workers without RF tags, and the total number of experiments in the demonstration experiment. In this table, the number of workers without RF tags was determined by counting the number of workers entering the press line not holding RF tags by comparing the facilities' operations, data obtained by processing the operation detection, and data obtained by processing the entry-exit confirmation sensors. The total number of workers entering the press line over the four days of the demonstration experiment was 308 (a total of 15 h and 30 min). A total of 112 workers entered the press line holding RF tags.

Results of the Demonstration Experiment and Discussion

The aim of the demonstration experiment was to verify the risk reduction effects of the supportive protection system during non-routine operations in company A's press line (production line) compared with those of an existing system.

The results of each item in the demonstration experiment are described below.

1-1 Risk reduction effects when a worker possessing qualifications and authorization performs non-target operations

In an existing system, when a worker enters a dangerous area, he/she is allowed to perform any operation of any machine. Therefore, it is up to the worker to perform only appropriate operations.

When a worker performs an unauthorized operation, the risk of an occupational accident is high because of his/her insufficient technical skills.

In the supportive protection system, a worker is not allowed to perform an operation that has not already been registered. The demonstration experiment confirmed that the supportive protection system did not allow a worker to perform non-target operations.

1-2 Risk reduction effects when a worker not possessing qualifications and authorization performs operations

In an existing system, a door is installed at an entry-exit gate, and entry-exit management is performed using safety plugs. However, any worker can pull out the safety plug and enter the operation area. Therefore, a worker not possessing qualifications and authorization can access any machine and facility.

When a worker performs an unauthorized operation, the risk of occupational accidents, such as being caught in a press or being entangled in a conveyor, is high because of his/her insufficient technical skills.

It was confirmed that in the supportive protection system, when a worker's qualifications and authorization did not agree with those that had already been input into the worker's RF tag, the worker could not operate the target machine.

1-3 Risk reduction effects when a third party restarts the machine while a worker with qualifications and authorization performs an operation

In an existing system, a door is installed at an entry-exit gate, and entry-exit management is performed using safety plugs. The risk that a third party restarts the machine while a worker with qualifications and authorization performs an operation is reduced by placing safety mats on the floors of blind spots to detect that a worker is within the fence. However, practically speaking, it is difficult to place safety mats on the floors of all blind spots. When dangerous failures, such as wire breaking and poor contact of a safety mat, are considered, it is necessary to employ a safety mat equipped with a wire breaking detector. Moreover, it is assumed that a third party can confirm workers at places other than blind spots. Therefore, when a third party cannot find a worker in an operation area due to the third party's carelessness, the risk that the third party restarts the machine is high. It was confirmed that in the supportive protection system, a worker entering an operation area confirmed his/her exit by him/herself, and when the number of workers entering an operation area did not agree with that existing the operation area, the third party could not restart the machine.

Table 3 Dates and results of experiments

Dates of experiments	Number of operations	Contents of operations									Number of workers without RF tags	Total number of experiments
		Instructions on the press	Change of press die	Set up of the press	Adjustment of the press	Repairs	Cleaning	Production	Schedule of conveyance	Adjustment of conveyance		
28-Oct	31	1	1	1	2	3	5	3	10	5	38	69
29-Oct	29	2	2	1	0	4	8	3	11	0	60	89
30-Oct	37	2	2	3	1	3	10	5	11	2	73	110
31-Oct	15	1	1	0	0	0	7	1	5	1	25	40
Total number	112	6	0	5	3	10	30	12	37	8	196	308

Evolution of SIAS Conferences from 1999 to 2012

Denis Turcot[1], Yuvin Chinniah[2]

[1] Scientific Division, Institut de recherche Robert-Sauvé en santé et sécurité du travail,Montreal, Canada
[2]Mathematics and Industrial Engineering Department,Polytechnique Montreal,Université de Montréal, Montreal, Canada

Abstract

This is the eighth International Conference on the Safety of Industrial Automated Systems (SIAS). Since the first one was held in Montreal in 1999, the conference has attracted researchers from different countries who share a common interest in machine safety. SIAS is the only international conference that focuses solely on the safety of machinery. Over the years, it has evolved in terms of organization, the scientific committee and participants. The papers presented at SIAS, which take the form of oral presentations and posters, have also evolved. We present an overview of the evolution of the SIAS conferences by classifying (i) the number and changes in topics in the program, (ii) the number of papers on each topic, (iii) information about the lead authors of the papers (country of origin and institutional affiliation) and (iv) the content of the papers. Since over 300 papers (oral presentations and posters) have been published in the SIAS proceedings, we have classified the content of their abstracts only.

Keywords:

Machine safety; Conferences overview

Introduction

The SIAS international conferences on the safety of industrial automated systems [1-7], which are now in their eighth year, have provided a forum for machinery researchers, designers and integrators, as well as for industry specialists interested in machine safety. In this paper we take a look back at the first seven conferences, focusing on their organization and the material (oral presentations and poster sessions) published in their proceedings. We present an overview of the evolution of the SIAS conferences by classifying (i) the number and changes in topics in the program, (ii) the number of papers on each topic, (iii) information about the lead authors of the papers (country of origin and institutional affiliation) and (iv) the content of the papers. Since 355 papers (oral presentations and posters) have been published in the SIAS proceedings, we have classified the content of their abstracts only. The breakdown of oral presentations and posters by conference is shown in Table 1.

Methods

Papers were classified by topic on the basis of their abstracts. As a total of 355 oral presentations and posters, ranging in length from 4 to 10 pages, have been published at the seven SIAS conferences, it was decided that the abstracts would be used for analysis purposes. The abstracts are taken from the SIAS conference proceedings and represent both oral presentations and posters. For SIAS conferences, all contributing authors must submit a paper (for oral presentations as well as for posters), which is then published in the conference proceedings. The abstracts vary in length from a few lines to half a page. Opening remarks made at the conferences were not considered.

Table 1: Breakdown of oral presentations and posters at SIAS conferences

SIAS year	Oral presentations	Posters	Total
1999 – Montreal (Canada)	37	7	44
2001 – Bonn (Germany)	40	9	49
2003 – Nancy (France)	34	16	50
2005 – Chicago (USA)	34	8	42
2007 – Tokyo (Japan)	36	32	68
2010 – Tampere (Finland)	33	19	52
2012 – Montreal (Canada)	25	25	50
TOTAL	239	116	355

A database (Microsoft Access) was set up to facilitate the analysis. The database entry on each paper contains the following information: conference it was presented at, identification of first author (surname, given name, country and affiliation), session it was given at, title of the presentation or poster, one to three keywords indicating the subject of the paper and an optional note. Keywords are grouped under eight main topics: (i) risk assessment, (ii) risk reduction, (iii) safe work organization, (iv) standards, rules and regulations, (v) protective devices, (vi) equipment, (vii) risk factors and (viii) other risks. These topics are then further divided into two or three additional levels to specify the subject in question. For example, the topic “safety devices” is divided into 13 categories, including guards, presence sensing devices, control systems and automated system reliability. Most of these categories are then broken down into further subcategories (11 subcategories or third-level keywords for control systems, for instance).
The list of keywords is based on a search of terms used in machine safety, risk assessment training [8], the classification formerly used by the ILO (International Labour

Organization) and international standards. This list was reviewed by more than five machine safety professionals or researchers and was used on three occasions in studies to characterize machine safety research projects carried out by occupational health and safety research centres. The list is regularly updated to reflect new developments in the field.
A list of 173 keywords was used to characterize the papers surveyed.
Finally, we should note that the classification of the papers using keywords was not checked by another person, which means that the coding was not validated and that the margin of error could not be quantified.

Results

As mentioned earlier, the results of this analysis concern the different topics examined at past conferences and the number of papers associated with them, the lead authors (country, affiliation) and the content of the papers.

Topics

As a general rule, for each conference, seven or eight topics are proposed to potential contributors, and these topics have varied somewhat from one conference to the next. Table 2 shows that two topics have been featured at every conference: risk assessment and training (including knowledge transfer and education).

Table 2: Number of papers presented at SIAS Conferences, by topic

		SIAS							
id	**Generic Session Title**	**Montreal 1999**	**Bonn 2001**	**Nancy 2003**	**Chicago 2005**	**Tokyo 2007**	**Tampere 2010**	**Montreal 2012**	**Total number of papers per topic**
1	Risk Assessment	4	5	5	6	7	12	3	42
2	Training, Knowledge Transfer and Education	2	3	4	6	4	6	7	32
3	Machine Safety: Ergonomic and human factor	7	8	11	—	8	—	5	39
4	Control System Design	5	8	—	—	13	—	9	35
5	Standards	8	—	—	—	—	—	—	8
6	Protective devices and systems	3	6	4	6	—	11	10	40
7	Case Studies	11	8	7	5	7	—	5	43
8	Fieldbus Safety	4	7	6	—	—	—	—	17
9	Safe Software / Software Tools	—	4	—	4	—	3	—	11
10	Functional safety	—	—	13	5	12	12	—	42
11	Robots	—	—	—	5	12	8	11	36
12	Vision / ID	—	—	—	—	5	—	—	5
13	Innovation and the future	—	—	—	5	—	—	—	5
	TOTAL	44	49	50	42	68	52	50	355

Other frequently proposed topics are protective devices and systems (6 out of 7 conferences), case studies (6/7) and machine safety: ergonomic and human factors (5/7). At around half of the conferences, authors could choose from among the following topics: control system design (4/7), functional safety (4/7), robots (4/7), fieldbus safety (3/7) and safe software/software tools (3/7). Three topics have been featured only once at SIAS conferences: standards, vision/ID systems, and innovation and the future.

Although standards were proposed as a specific topic only at the first SIAS, the subject was still examined at other conferences, but from the perspective of other topics. The database contains over 40 entries for papers referring to one or more standards in their abstracts. To take an example, it can be seen that standard ISO 13849 was mentioned in the titles of 13 papers at the last four SIAS conferences alone. The keywords “control systems” or “system reliability” were assigned to nine of these papers. Even if the topic of functional safety has not featured at all the conferences, aspects of this topic certainly have.

And while the topic of robots was first proposed at the fourth SIAS conference (Chicago, 2005), papers related to robotics have been published in the proceedings of all the conferences. (For all conferences, the word “robot” appears in the titles of 40 papers.) The descriptor “robot” associated with papers is referenced 42 times using keywords (from one to three keywords assigned per paper, without repetition among them). This leads to the subject of collaborative robots. The first session describing this specific aspect of robot use was presented in Japan (Tokyo, 2007) under the title: “Robots – Human-cooperative features.” But the very first papers on the topic were presented at the third SIAS conference (Nancy, 2003). The use of keywords makes it possible to specify a subject that a search for a descriptor in a title would not turn up. Thus, for collaborative robots, the titles of some papers do not contain the descriptor "collaborative," but do include "cooperative" or "coactivity." Papers that describe measuring the impact force or pain threshold of a worker who is hit by a collaborative robot (such as "Risk Assessment and Investigation of Change from Pressure Feeling to Pain") would not be found if the keyword "collaborative robot" were not used.

A last example concerns vision/ID systems. The first time a session was held on this topic was at the fifth SIAS conference. However, the database indicates that papers on the subject were presented for the first time at the third conference (Nancy, 2003) and then at others that followed.

Authors

Authors from eight countries have accounted for the bulk of SIAS contributions so far (342 papers), with contributors from another seven countries providing the remaining 13 papers at the seven conferences. The breakdown of contributions by country of each paper's first author is shown in Table 3. Authors from Germany have presented almost 28% of all papers, followed by Japan (23%), France (15%), Canada (12%), Finland (8%), the United States (8%), the United Kingdom (4%) and Poland (2%).

Table 3: Number of papers per country, based on country of first author – all SIAS conferences

	Montreal 1999	Bonn 2001	Nancy 2003	Chicago 2005	Tokyo 2007	Tampere 2010	Montreal 2012	ALL SIAS
Canada	13	6	6	4	3	3	9	44
France	12	7	11	7	5	3	7	52
Germany	6	23	16	12	17	12	14	100
Japan	1	3	6	10	32	13	15	80
Finland	2	2	3	2	3	12	4	28
USA	3	3	1	4	3	1	2	17
UK	2	3	4	2		3		14
Poland	1	1	3	1		1		7

The breakdown of first authors by type of institutional affiliation is shown in Table 4. Three institutional categories were used: occupational health and safety research centres, all universities in a given country and an "Other" category that takes in representatives of safety device manufacturers, companies and industry associations, industrial research centres, professional associations, experts in various fields, etc.

In the "Other" category, Germany and Japan stand out from the other countries by their high number of papers, chiefly by authors employed in industry (manufacturers, integrators and consultants): over 25 of the 53 from Germany and 14 of the 61 from Japan.

.

Table 4: Papers published in the proceedings of all SIAS conferences from 1999 to 2012

	Canada	Finland	France	Germany	Japan	Poland	UK	USA
Research Center (OHS)	22 (IRSST)	24 (VTT)	39 (INRS)	39 (IFA)	10 (JNIOSH)	5 (CIOP)	8 (HSE)	5
Universities	13	3		8	9			
Other	9	1	13	53	61	2	5	12

Content of papers

As mentioned earlier, papers were classified using up to three keywords, with each of these able to have up to two subcategories. The classification obtained for the SIAS conference topics associated with the first-level keywords (see Table 5) shows that the topic "protective devices" was assigned to close to half (48%) of the abstracts. Note, however, that this topic accounts for over a third of the keywords, i.e., 37% of all the keywords used (60/173) in the classification scheme developed for this analysis.

Table 5: Number of papers published by topic, where topic is first keyword used

	Montreal 1999	Bonn 2001	Nancy 2003	Chicago 2005	Tokyo 2007	Tampere 2010	Montreal 2012
Risk Assessment	4	4	2	8	5	4	5
Risk Reduction	8	2	7	2	6	7	8
Safe work organization	2	4	5	5	6	6	3
Standards, Rules and Regulations	5	1	3	—	3	1	2
Protective Devices	23	30	24	20	32	25	15
Equipment	—	1	4	3	10	5	17
Risk Factors	—	3	4	1	5	—	—
Risks - Others	—	—	—	1	1	—	—

The other categories are also represented across all SIAS conferences, with the exception of risk factors and other types of risks. These last two categories were used to classify subjects examined only occasionally. Table 6 presents a detailed breakdown of the topics most frequently addressed at the conferences, based on the first keyword associated with each abstract.

Table 6: Number of abstracts described by their first keyword and indexed up to a second level

Topics Keywords level 1	Keywords – level 2	Total, All SIAS
Risk Assessment	Grouping : General, Hazard identification, Risk Estimation Tools	33
Risk Reduction	Grouping : General, Safety design, Process improvement, Development of safety or protective devices	17
	Maintenance, Lockout	15
	Safety and ergonomics	8
Safe work organization	Training	17
	Statistics on machine accidents	7
Standards, Rules and Regulations		17
Protective Devices	Guards	9
	Safety distance	8
	Interlocking devices	3
	Presence sensing devices	29
	Safety controllers	10
	Control systems	75
	Reliability (of automated systems)	27
	Tampering	3
Equipment	Stationary machines - Robots	26

To make the table 6 easier to lay out and read, a more detailed breakdown based on a selection of second-level keywords has been provided, representing 85% of all the papers classified.
Finally, an analysis of the most common second-level category, "control systems," and its subcategories (third-level keywords) reveals a fairly balanced breakdown between the various topics, with the exception of hydraulics in control circuits (Table 7).

Table 7: Number of abstracts indexed with control system-related keywords

	All SIAS
Control Systems (general)	12
PLCs (programmable Logic Controllers) or Programmable safety systems	13
Control system components	6
Performance levels	17
Safety critical software	6
Hydraulics (in control circuits)	1
Fieldbus safety	13
External control (Internet, wireless, etc.)	7
TOTAL	75

Conclusion

The analysis of the abstracts of papers presented at the SIAS conferences has shown how the topics addressed have changed over the years, as well as the number of papers on each topic, provided an overview of the institutional affiliation and country of the first author of each paper and, finally, offered a breakdown of the papers by topic based on keywords assigned to them. While space limitations make it impossible to show all the analytical tables created, a detailed example of the classification generated for control systems illustrates the database's flexibility and the type of information that can be retrieved. This paper has taken a look back at past SIAS conferences and could be used to help structure future meetings.

References

[1] Proceedings, International Conference on the Safety of Industrial Automated Systems, October 5 to 7, 1999, Montreal, Canada

[2] Proceedings, 2nd International Conference on the Safety of Industrial Automated Systems, November 13 – 15, 2001, Bonn, Germany

[3] Proceedings, 3rd International Conference on the Safety of Industrial Automated Systems, October 13 – 15, 2003, Nancy, France

[4] Proceedings, 4th International Conference on the Safety of Industrial Automated Systems, September 26 – 28, 2005, Chicago, USA

[5] Proceedings, 5th International Conference on the Safety of Industrial Automated Systems, November 12 – 13, 2007, Tokyo, Japan

[6] Proceedings, 6th International Conference on the Safety of Industrial Automated Systems, June 14 – 15, 2010, Tampere, Finland

[7] Proceedings, 7th International Conference on the Safety of Industrial Automated Systems, October 11 – 12, 2012, Montreal, Canada

[8] Paques, J.-J.,Formation en sécurité des machines: appréciation et réduction du risque*,* IRSST, 2002, Montreal.

Corresponding address

Denis Turcot, ing.

Institut de recherche Robert-Sauvé en santé et sécurité du travail

505, boul. de Maisonneuve Ouest

Montreal (Québec) H3A 3C2

Tel. : +1 514 288 1551 x271

turcot.denis@irsst.qc.ca

Investigation of evaluation method for strength of artificial bones by using Finite Element Analysis

Atsushi YAMAGUCHI[a], Kohei OKABE[a], Hiroyasu IKEDA[a]

[a] *Mechanical & System Safety Research Group, National Institute of Occupational Safety and Health, JAPAN*
Kiyose-shi, Tokyo, Japan

Abstract

Artificial bones made from biomaterial simulated the physical properties of human tissue are developed by several suppliers. It is necessary to obtain the strength of artificial bone by a strength test in order to investigate the reproducibility and validity of the developed artificial bone. However, an evaluation test for strength of artificial bone has not been established.

In this study, an availability of Finite Element Analysis (FEA) on evaluation test for strength of artificial bone is shown by comparing the strength of the artificial bone obtained by experimental. The analytical results agree well with the experimental results, because the difference between the FE result and the average of test results is within 6%. Thus, it is considered that the breaking load of a human ulna and an artificial ulna are able to estimate by using FEA.

Keywords:

Artificial bone; Finite Element Analysis; bending test

Introduction

Cooperative robots, such as care robots, are required to operate in close contact with the elderly. In addition, cooperative robots are required a high power such as supporting the elderly. The technology that satisfies both the required specifications and the adequate safety has not yet been established in the field of cooperative robots. For the establishment of the technology, it is necessary to clarify a relationship between the load caused by cooperative robots and the tolerance of human bone. However, verification using human bone has ethical difficulties. An investigation using artificial bone is nowadays addressed.

Artificial bones made from biomaterial simulated the physical properties of human tissue are developed by several suppliers. It is necessary to obtain the strength of artificial bone by a strength test in order to investigate the reproducibility and validity of the developed artificial bone. However, an evaluation test for strength of artificial bone has not been established.

In this study, an artificial born is tested by a three point bending test in order to investigate an evaluation method for strength of artificial born. And then, a validity of analysis condition is investigated by comparing the test result and analysis result.

Artificial bone

Figure 1 show the appearance of artificial ulna. The artificial ulna is simulated the ulna of a Japanese woman. The length of artificial ulna is approximately 210 mm. The mechanical properties of the artificial ulna are shown Table 1. The Young's modulus, yield strength and tensile strength of an artificial cortical bone, which is constructed of an epoxy resin, are 16,000 MPa, 95 MPa and 106 MPa, respectively. Then, The Young's modulus yield strength and tensile strength of an artificial cancellous bone, which is constructed of a compressive foam, are 155 MPa, 6 MPa and 8 MPa, respectively. Both mechanical properties are obtained by ASTM D 638[1] and ASTM D1621[2], respectively.

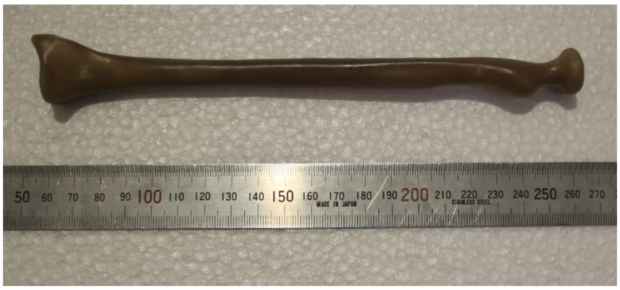


Fig.1 Appearance of artificial ulna

Table 1 Mechanical properties of an artificial ulna

Artificial ulna	Young's modulus (MPa)	Yield strength (MPa)	Tensile strength (MPa)
Cortical bone	16,000	95	106
Cancellous bone	155	6	8

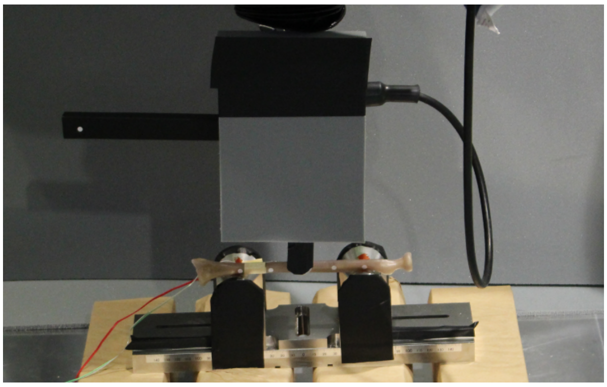
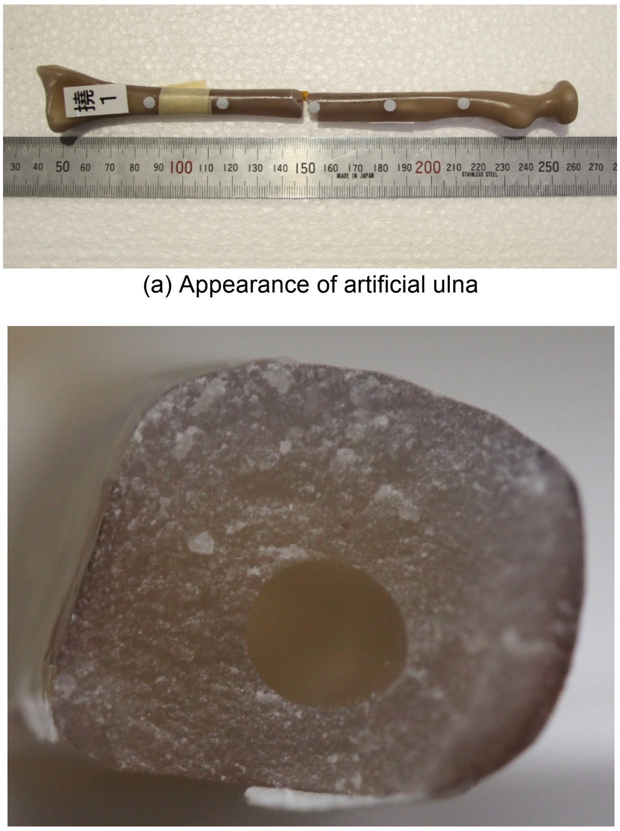


Fig.2 Situation of three point bending test



(a) Appearance of artificial ulna

(b) A failure surface

Fig.3 Artificial ulna after bending test

Bending test for artificial ulna

A three point bending test was carried out in order to obtain the bending strength of ulna of artificial born. The length of both supporting points is 100 mm as shown in Figure 2. Also, curvature radius of loading point and supporting points are 10 mm and 12 mm, respectively.

The result of bending test is shown in Table 2, and the test is carried out 4 times. The maximum breaking load is 503.5 N, and the minimum breaking load is 437 N and the average breaking load is 482.8 N. Figure 3 shows the appearance of artificial ulna after the bending test and failure surface. It is considered that artificial ulna was break due to a brittle failure, because a cracking and a deformation are not observed in artificial ulna after bending test. Generally, it is considered that crack born before break when bone is subjected to static loading. Therefore, it is considered that the toughness of artificial ulna is low compared with that of ulna.

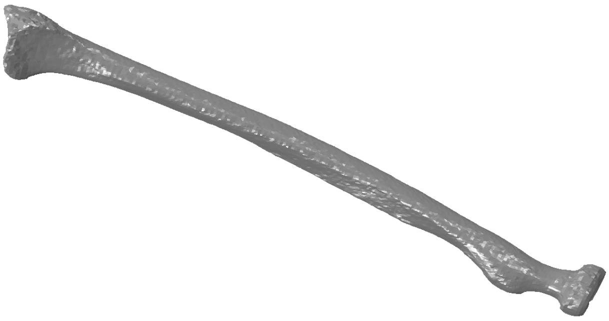


Fig.4 Finite element model of the artificial ulna

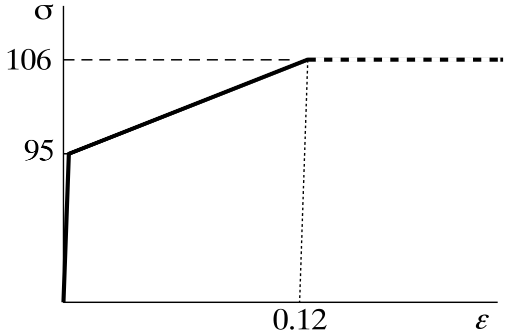


Fig.5 True stress-strain relation using FEA

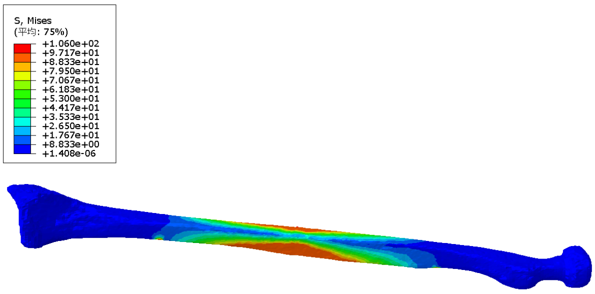


Fig.6 Stress distribution right before break on artificial ulna

Finite Element Analysis

Finite element analysis is carried out in order to calculate the breaking load by three point bending test. Figure 4 shows the FE model of artificial ulna. Finite element analysis is carried out using ABAQUS 6.11. The FE model, which is a full-scale model of the artificial cortical bone, meshes 718,255 elements and 153,480 nodes using three-dimensional elements (C3D4). The Young's modulus and Poisson's ratio of the artificial cortical bone are 16,000 MPa and 0.34, respectively. The true stress-true strain curve using FEA, as shown in Figure 5, was experimentally derived on the assumption that the specimen volume was constant up to the maximum load point. The true stress-strain relation is obtained based on result of ASTM D 638.

And then, the mechanical properties of artificial cancellous bone are lower than that of artificial cortical bone. It is considered that artificial cancellous bone does not contribute the strength of artificial ulna. Thus, the artificial cancellous bone is not included in FE model. Also, Finite element analysis is not able to simulate the break. In the present study, the failure load calculated by using FEA is defined as the load at which the strain does diverge.

Figure 6 shows von Mises stress right before a break of the ulna. A breaking load is calculated by FEA is 512 N. The analytical results agree well with the test results, because the difference between the analytical result and the average of test results is within 6%. Thus, it is considered that the breaking load of a human ulna and an artificial ulna are able to estimate by using FEA.

Conclusion

(1) The analytical results in this study agree well with the test results, because the difference between the analytical results and the test results is within 5%.

(2) In the evaluation of breaking load in artificial born, there is no need to consider the mechanical properties of a cancellous bone.

(3) It is considered that the breaking load of a human ulne and an artificial ulna are able to estimate by using FEA.

References

[1] ASTM D 638

[2] ASTM D1621

Corresponding address

Atsushi YAMAGUCHI, yamaguchi@s.jniosh.go.jp
Kohei OKABE, okabe@s.jniosh.go.jp
Hiroyasu IKEDA, ikeda@s.jniosh.go.jp

SIAS 2015

8th INTERNATIONAL CONFERENCE
ON THE SAFETY OF INDUSTRIAL
AUTOMATED SYSTEMS

Foto: © – jim, Fotolia

Product exhibition

– List of manufacturers –

We would like to express our thanks to the exhibitors for their significant contribution to the sucess of the conference!

CE Design Technical Compliance GmbH
Hauert 14
44227 Dortmund
Germany

E. Dold + Söhne KG
Bregstr. 18
78120 Furtwangen
Germany

ELOKON Polska Sp. z o.o.
Tytoniowa 22
Warsaw 04-228
Poland

EUCHNER GmbH & Co. KG
Kohlhammerstr. 16
70771 Leinfelden-Echterdingen
Germany

IMI Precision Engineering
Bruckstr. 93
46519 Alpen
Germany

Luetkens Automation
Aaraustr. 85
72762 Reutlingen
Germany

ROSS Europa GmbH
Robert-Bosch-Str. 2
63225 Langen
Germany

K.A. Schmersal GmbH & Co. KG
Möddinghofe 30
42279 Wuppertal
Germany

Universal Robots A/S
Energivej 25
5260 Odense
Denmark