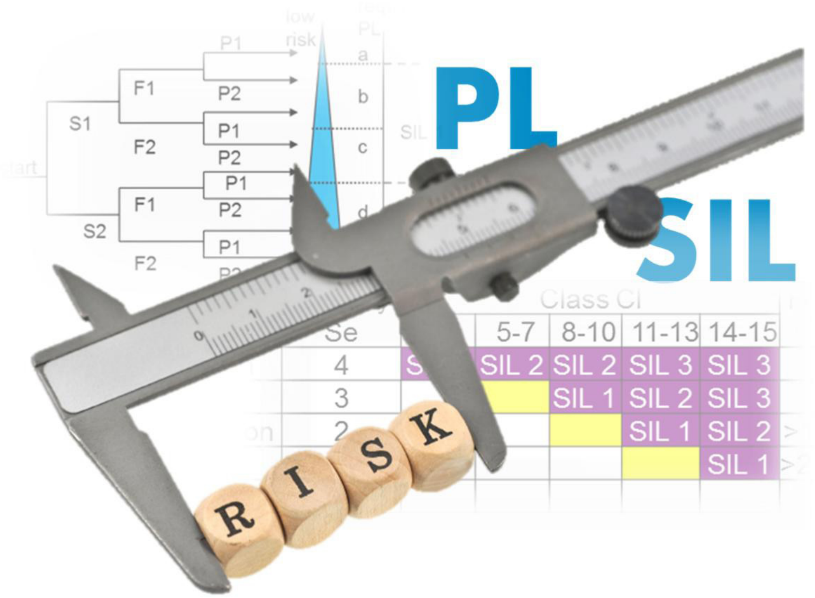
TECHNOLOGY • RESEARCH HIGHLIGHTS • VISIONS • SCIENCE •

241



From risks to requirements

Comparing the assignment of functional safety requirements

Timo Malm | Outi Venho-Ahonen | Marita Hietikko |
Tor Stålhane | Charlotte de Bésche |
Johan Hedberg

VTT TECHNOLOGY 241

From risks to requirements

Comparing the assignment of functional safety requirements

Timo Malm & Outi Venho-Ahonen

VTT Technical Research Centre of Finland Ltd

Marita Hietikko

VTT Expert Services Ltd

Tor Stålhane

Norwegian University of Science and Technology, NTNU

Charlotte de Bésche & Johan Hedberg

SP Technical Research Institute of Sweden

ISBN 978-951-38-8384-3 (URL: http://www.vttresearch.com/impact/publications)

VTT Technology 241

ISSN-L 2242-1211
ISSN 2242-122X (Online)
http://urn.fi/URN:ISBN:978-951-38-8384-3

Copyright © VTT 2015

JULKAISIJA – UTGIVARE – PUBLISHER

Teknologian tutkimuskeskus VTT Oy
PL 1000 (Tekniikantie 4 A, Espoo)
02044 VTT
Puh. 020 722 111, faksi 020 722 7001

Teknologiska forskningscentralen VTT Ab
PB 1000 (Teknikvägen 4 A, Esbo)
FI-02044 VTT
Tfn +358 20 722 111, telefax +358 20 722 7001

VTT Technical Research Centre of Finland Ltd
P.O. Box 1000 (Tekniikantie 4 A, Espoo)
FI-02044 VTT, Finland
Tel. +358 20 722 111, fax +358 20 722 7001

Preface

The project COMPSOFT (Comparing best practices of safety related control system development) was conducted by VTT Technical Research Centre of Finland Ltd (Finland), together with NTNU (Norway) and SP (Sweden). The major part of the funding in Finland was received from the Finnish Work Environment Fund. Each research participant had also their own funding. Many companies from Finland, Norway and Sweden gave their support by answering questions and analysing the test cases. The project team was Timo Malm, Outi Venho-Ahonen (VTT), Marita Hietikko (VTT Expert Services Ltd.), Tor Stålhane (NTNU), Charlotte de Bésche, Johan Hedberg (SP), Matti Sundquist (Sundcon Oy) and Thor Myklebust (Sintef).

Tampere, December 2015, Authors

Contents

Appendices

Terminology

Functional safety: part of the safety of the machine and the machine control system which depends on the correct functioning of the safety-related electrical control system (SRECS), other technology safety-related systems and external risk reduction facilities. [IEC 62061]

Harm: physical injury or damage to health. [ISO 13849-1]

Hazard (from machinery): potential source of physical injury or damage to health. [IEC 62061]

Performance level (PL): discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions. [ISO 13849-1]

Risk: combination of the probability of occurrence of harm and the severity of that harm. [ISO 13849-1]

Risk analysis: combination of the specification of the limits of the machine, hazard identification and risk estimation. [ISO 13849-1]

Risk assessment: overall process comprising risk analysis and risk evaluation. [ISO 13849-1]

Risk evaluation: judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved. [ISO 13849-1]

Required performance level (PL_r): performance level (PL) applied in order to achieve the required risk reduction for each safety function. [ISO 13849-1]

Round robin test: In experimental methodology, a round robin test is an interlaboratory test (measurement, analysis or experiment) performed independently several times. This can involve multiple independent scientists performing the test with the use of the same method in different equipment or a variety of methods and equipment. In reality it is often a combination of the two, for example if a sample is analysed, or one (or more) of its properties is measured by different laboratories using different methods, or even just by different units of equipment of identical construction. [Wikipedia, retrieved 16.9.2015.]

Safety function: function of a machine whose failure can result in an immediate increase in the risk(s). [IEC 62061]

Safety integrity: probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time. [IEC 61508-4]

Safety integrity level (SIL): discrete level (one out of a possible four) corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. [IEC 61508-4]

1. Introduction

1.1 Background

It has been found that 40% of faults contributing to programmable electronic systems-related incidents emerge during the safety requirements specification phase of a system life cycle [Chambers et al. 1999]. In addition, on average, 30% of software-related defects are made in the requirements specification phase, and the share is much higher (60%) for excellent software [Jones 2012]. There is a huge difference in the share of requirements specification faults between good and poor software. It is difficult to say when the requirements specification has no effect on faults except in simple coding error. However, the large number of answers (13500) to the survey (by Capers Jones) and the presented average indicate that the origin of faults is often at the early phases of design [Jones 2012]. It is therefore important to focus on the safety requirements specification and the risk assessment.

When analysts make risk assessments, they typically get different results depending on the background of the analysts. Risk assessments should preferably result in specific PL or SIL requirements in order to set requirements for the control systems. Requirements that are too strict lead to expensive systems and requirements that are too low lead to unsafe systems.

This paper focuses on risk assessment related to the SIL/PL assignment (safety integrity level/performance level). The standards related to functional safety present standard specific methods and, in the risk assessment, methods are referred to by applying relevant standard’s code. In the round robin experiments, the SIL/PL values are treated as risk levels, although the final target would be the SIL/PL assignment associated with the relevant safety function. The required safety functions are not always described for the cases – only the risks. Compared to the functional safety standards, a greater scope of risk assessment for machinery can be found, e.g., from the ISO 12100 standard, which is related to all kinds of safety risks related to machinery.

1.2 Objective

The objective of the project is to improve 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 methods with a good reputation, select a set of best methods and techniques and find ideas to improve or integrate them to better support each other. The impact of the comparative approach of the study is intended to affect performance and safety culture in organizations.

Each participating institute and enterprise has executed a round robin test according to a pre-determined plan. A round robin test includes measurements, analyses or conceptual assessments evaluated by multiple independent experts applying the same methods for case systems (or products) to compare methods and variance of the results (cp. analysis of variance). The objectives of the round robin test are

- to find the best practices for the safety requirements specification and risk assessment
- to find the criteria for the selection of methods and techniques
- to find the strengths and weaknesses of the methods used in the early safety life cycle phases of control system design using a comparative approach
- to find uniform principles, practices and methods used in different institutes.

2. Risk assessment methods for defining requirements

2.1 The dimensions of risk

The risk is typically divided into two parts: severity and probability (see Terminology). Severity describes how severe the consequences of the hazards can be and the probability factor describes the probability of a hazardous or initiating event. All the standards described here (ISO 13849-1, IEC 62061, IEC 61508-5, ISO 26262 etc.) have a severity factor, which may have from 2 to 5 severity levels. Probability is divided into several factors depending on the standard. There are also factors that are mentioned by the standard, but are combined with other factors like 'Probability of avoiding or limiting harm' or 'Probability of occurrence of a hazardous event'. Figure 1 shows the risk factors that can be estimated in a complex system. The list is not comprehensive and some factors can be divided further.

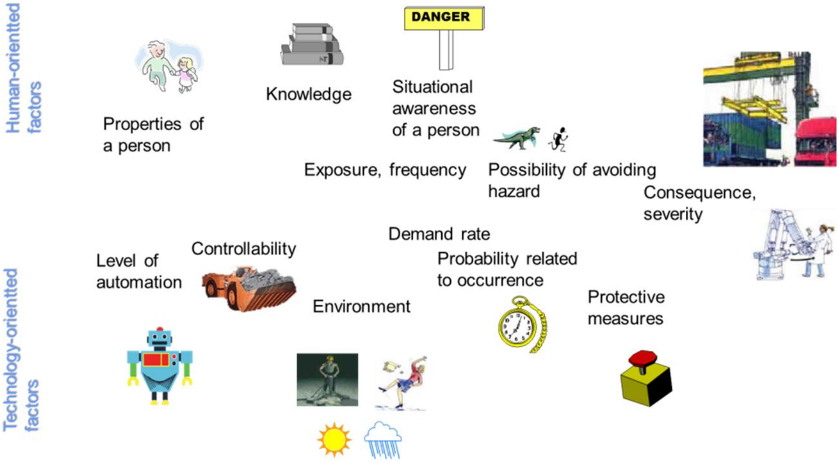


Figure 1. Examples of risk factors.

Figure 2 shows the risk factors in detail according to the IEC 62061 method. All factors should be estimated independently without any effect of other parameters.

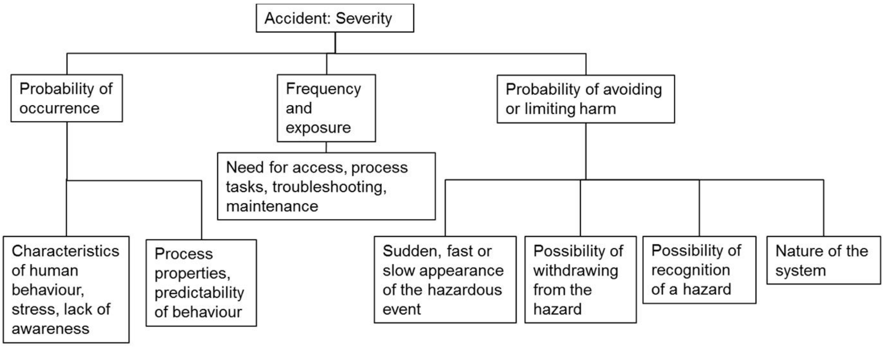

Accident: Severity
Probability of occurrence
Frequency and exposure
Probability of avoiding or limiting harm
Need for access, process tasks, troubleshooting, maintenance
Characteristics of human behaviour, stress, lack of awareness
Process properties, predictability of behaviour
Sudden, fast or slow appearance of the hazardous event
Possibility of withdrawing from the hazard
Possibility of recognition of a hazard
Nature of the system

Figure 2. Risk factors according to the IEC 62061 principles.

2.2 Risk assessment methods of standards

A risk assessment can be carried out for many purposes: to define hazards and their meanings, to compare risks and to define significant risks and related requirements. In this context, the purpose of the risk assessment is to define the risks and the corresponding requirement levels mainly for control systems and safety devices. The idea is that the higher the risk, the higher the requirement level. When the hazard and the related significant risk are found, a requirement must be defined to minimize the identified risk.

Figure 3 shows the phases of design according to IEC 61508-5. The process is designed for control systems and shows when risk assessment is necessary in order to define requirements. There are other needs for risk assessments than the requirements specification, such as verification and selection of subsystems; the risks are then also assessed in later design phase. The principles shown in Figure 3 are the same as in other functional safety standards like ISO 13849-1 and IEC 62061.

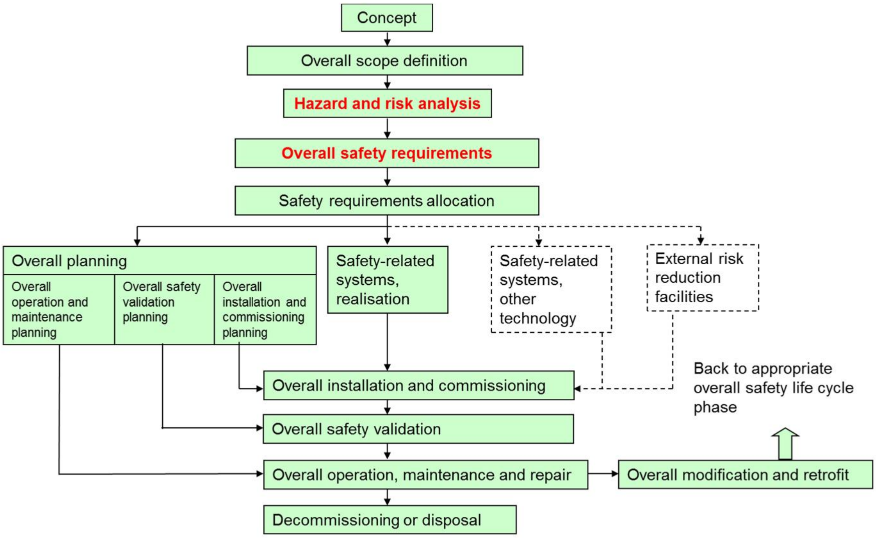

Concept
Overall scope definition
Hazard and risk analysis
Overall safety requirements
Safety requirements allocation
Overall planning
Overall operation and maintenance planning
Overall safety validation planning
Overall installation and commissioning planning
Safety-related systems, realisation
Safety-related systems, other technology
External risk reduction facilities
Overall installation and commissioning
Overall safety validation
Overall operation, maintenance and repair
Overall modification and retrofit
Back to appropriate overall safety life cycle phase
Decommissioning or disposal

Figure 3. Safety life cycle of control systems.

Figure 4 shows how each risk is handled. Each possible hazard is assessed in the risk assessment; there has to be a requirement for each significant risk as well as a design feature and validation procedure. If something is skipped or ignored the risk may not be under control.

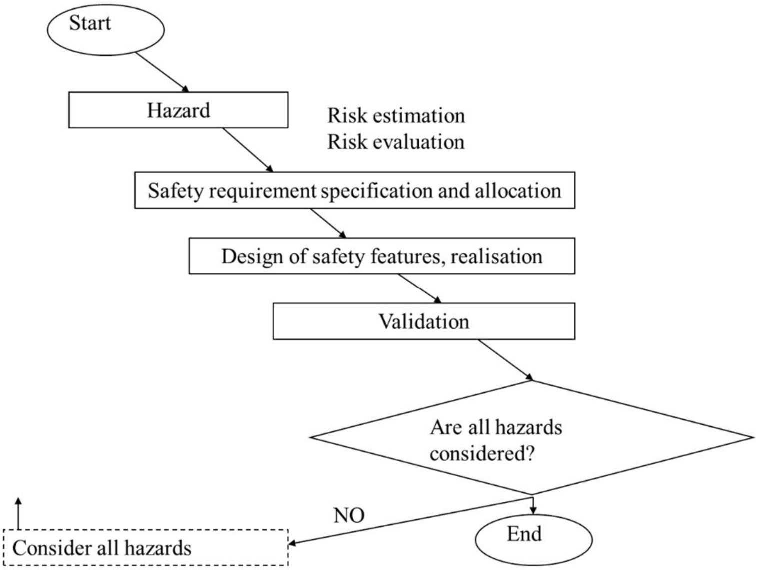

Start
Hazard
Risk estimation
Risk evaluation
Safety requirement specification and allocation
Design of safety features, realisation
Validation
Are all hazards considered?
NO
End
Consider all hazards

Figure 4. The process from hazard to validation.

2.2.1 The process from risk to requirement presented in standards

The methods are usually presented as risk graphs or matrixes with numerical scoring The graph can be a more informative than the matrix when it comes to presenting requirement level assignment according to the risks. If there is no calculation, the arrows do not cross and there are not too many paths to follow. Otherwise a matrix can be clearer than a graph i.e. matrix can present more complex methods.

The following chapters introduce some standards and guidelines that can be used to assign a risk or actual requirement level to a control system. The common functional safety standards, which describe a risk assessment method, are listed below:

- ISO 13849-1: for machinery (see Section 2.2.1.1)
- ISO/TS 15998-2: for earth-moving machinery (see Section 2.2.1.2)
- ISO 25119 family: for agriculture and forestry (see Section 2.2.1.3)
- IEC 62061: for machinery (see Section 2.2.1.4)
- ISO 26262: for the automotive industry (see Section 2.2.1.5)
- MIL-STD 882E: for military applications (see Section 2.2.1.6)
- EN 50126/128/129: for railway applications
- ISO 15998: for earth-moving machinery
- DO 178/254: for aviation
- IEC 61508-5: several methods for generic purposes.

2.2.1.1 The ISO 13849-1 method

ISO 13849-1 uses a decision tree (risk graph) 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 of avoiding the consequences) with the values P1 – possible to avoid under specific conditions and P2 hardly possible. The result of the risk assessment is performance level requirements (PL_r) for the control system safety function. Figure 5 shows the risk graph of ISO 13849-1. Table 1 shows the same risk graph presented in matrix form.

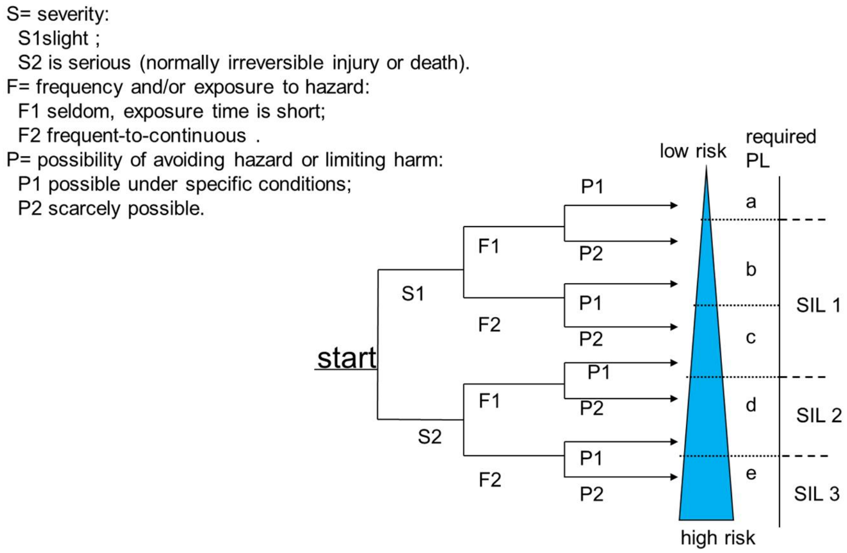

S= severity:
S1slight ;
S2 is serious (normally irreversible injury or death).
F= frequency and/or exposure to hazard:
F1 seldom, exposure time is short;
F2 frequent-to-continuous .
P= possibility of avoiding hazard or limiting harm:
P1 possible under specific conditions;
P2 scarcely possible.
start
S1
S2
F1
F2
F1
F2
P1
P2
P1
P2
P1
P2
P1
P2
low risk
high risk
required PL
a
b
c
d
e
SIL 1
SIL 2
SIL 3

Figure 5. Risk estimation presented in ISO 13849-1.

Table 1. ISO 13849-1 risk graph in matrix form.

Avoid	**P1**		**P2**	
Sev Freq	**F1**	**F2**	**F1**	**F2**
S1	a	b	b	c
S2	c	d	d	e

There will be a new version of ISO 13849-1 in the beginning of 2016. In that version of the standard there will be also a probability parameter, which enables to shift the results one step lower level. However, the minimum level is still PL a.

2.2.1.2 The ISO 15998-2 method

Figure 6 presents the risk graph of ISO 15998-2, which focuses on earth-moving machinery. It resembles the ISO 13849-1 method but has one additional severity level and the required PL results have a value that is one step lower than the ISO 13849 method.

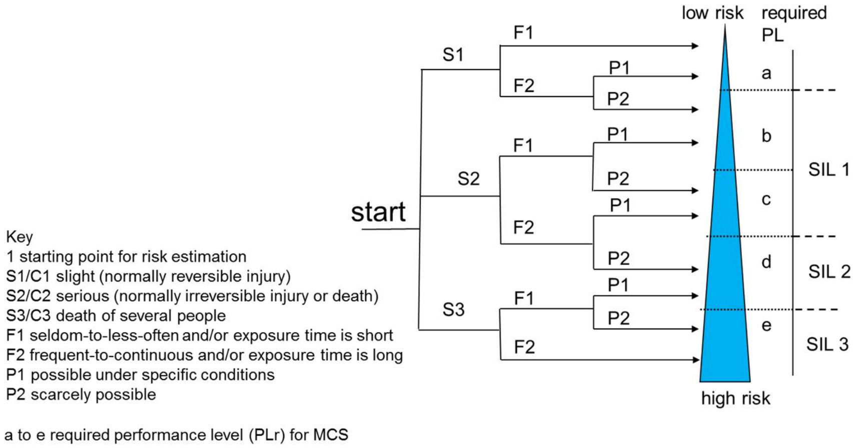

low risk
required PL
start
S1
S2
S3
F1
F2
P1
P2
a
b
c
d
e
SIL 1
SIL 2
SIL 3
high risk
Key
1 starting point for risk estimation
S1/C1 slight (normally reversible injury)
S2/C2 serious (normally irreversible injury or death)
S3/C3 death of several people
F1 seldom-to-less-often and/or exposure time is short
F2 frequent-to-continuous and/or exposure time is long
P1 possible under specific conditions
P2 scarcely possible
a to e required performance level (PLr) for MCS

Figure 6. Risk estimation according to ISO 15998-2.

2.2.1.3 The ISO 25119 method

The ISO 25119 standard family for agriculture and forestry presents a matrix method for risk assessment with the following parameters: severity, exposure and possible avoidance of harm, which is actually related to controllability of the machine. The method is presented in Table 5, Table 2,

Table 3 and Table 4. The letters in Table 5 represent the assigned AgriPL, and ‘QM’ refers to ‘quality management’. Table 5 shows that if the severity or the controllability factor is ‘0’ and the exposure factor is ‘0’ and other factors are not at the highest level, the quality management means are adequate to maintain safety.

Table 2. Severity estimation according to ISO 25119.

S0	**S1**	**S2**	**S3**
No injuries	Light or moderate injuries	Severe (e.g. irreversible injuries) and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Table 3. Exposure estimation according to ISO 25119.

Description	**E0**	**E1**	**E2**	**E3**	**E4**
Definition of frequency	Improbable (but theoretically possible; once during lifetime)	Rare events	Sometimes	Often	Frequently
Definition of duration: <u>(exposure)</u> (average operating) t_{exp}/t_{avg}	<0.01%	0.01% to 0.1%	0.1% to 1%	1% to 10%	> 10%

Table 4. Controllability estimation according to ISO 25119.

C0	**C1**	**C2**	**C3**
Easily controllable The operator or bystander controls the situation with his usual skills.	Controllable (Fewer than 1 in 100 people do not control the situation) The harm is almost always avoided, even for distracted operators or bystanders.	Generally controllable (Fewer than 1 in 10 people do not control the situation) Generally, the average operators or bystanders can avoid the harm.	Non-controllable The average operators or bystanders cannot generally avoid the harm.

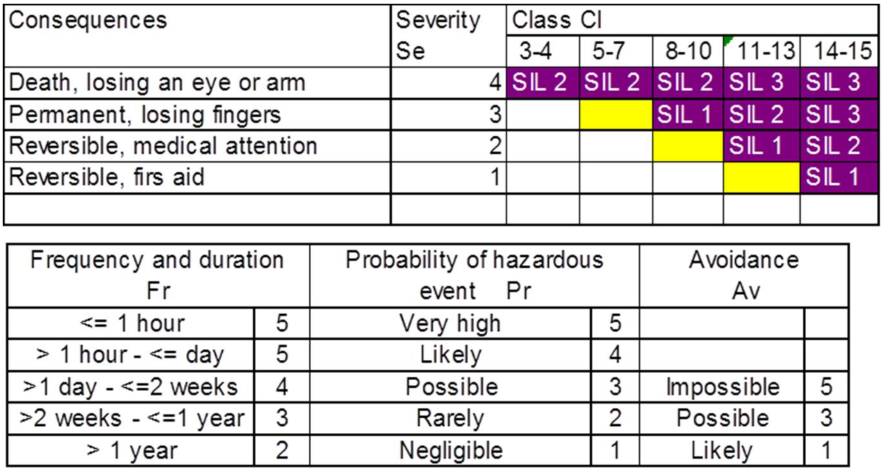
Table 5. AgriPL estimation according to ISO 25119.

		C0	C1	C2	C3
S0		QM			
S1	**E0**	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	a
	E3	QM	QM	a	b
	E4	QM	a	b	c
S2	**E0**	QM	QM	QM	QM
	E1	QM	QM	QM	a
	E2	QM	QM	a	b
	E3	QM	a	b	c
	E4	QM	b	c	d
S3	**E0**	QM	QM	QM	a
	E1	QM	QM	a	b
	E2	QM	a	b	c
	E3	QM	b	c	d
	E4	QM	c	d	e

2.2.1.4 The IEC 62061 method

The risk assessment method has four parameters to estimate: severity (4 levels), frequency (5 levels), probability (5 levels) and possibility of avoiding hazard (3 levels). The result gives the Safety integrity level (SIL 1, SIL2, SIL3 and 0) requirements for the control system safety function.

Table 6. The scoring table of IEC 62061 to estimate SIL.



Consequences	Severity Se	Class Cl				
		3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3		🟨	SIL 1	SIL 2	SIL 3
Reversible, medical attention	2			🟨	SIL 1	SIL 2
Reversible, firs aid	1				🟨	SIL 1

Frequency and duration Fr		Probability of hazardous event Pr		Avoidance Av	
<= 1 hour	5	Very high	5		
> 1 hour - <= 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

2.2.1.5 The ISO 26262 method

In the automotive industry, ASIL is estimated for safety functions. It resembles SIL but includes several factors related to vehicles. The method for estimating ASIL is presented in Table 7, Table 8, Table 9 and Table 10. Table 10 shows that if any factor is ‘0’ the quality management means are adequate to maintain safety.

Table 7. Severity estimation according to ISO 26262.

Class	**S0**	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain, fatal injuries)

Table 8. Probability estimation according to ISO 26262.

Class	**E0**	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Table 9. Controllability estimation according to ISO 26262.

Class	**C0**	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Table 10. ASIL estimation according to ISO 26262.

		C1	**C2**	**C3**
S1	**E1**	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	**E1**	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	**E1**	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

2.2.1.6 The MIL-STD 882E method

MIL-STD 882E focuses on system safety in military applications (USA). It presents the following parameters, which are applied in matrixes:

- severity; four criticality levels
- probability; six probability levels
- control category; five levels: autonomous, semiautonomous, redundant fault-tolerant, influent and no safety impact; the levels also indicate the control between automation and human interaction related to the function
- software criticality index, five levels, which indicate how much effort is required to validate software

2.2.2 Discussion on standard methods

According to the IEC 61508-4 definition, risk is a combination of the probability of occurrence of harm and the severity of that harm. The definition is originally from the ISO/IEC guide 51 and is used in several standards. Severity is presented in all the standards mentioned in Section 2.2 and the probability part can differ from standard to standard.

The method for machinery (ISO 13849-1 and IEC 62061) presents the parameters severity, frequency and exposure, possibility of avoiding hazards (including the possibility of withdrawing from hazard, speed of appearance, recognition, and the nature of the system) and in IEC 62061 also the probability of occurrence (including predictability and human behaviour). Some other standards also present other parameters:

- controllability, which is related to mobile vehicles
- control category, which is related to the role of the safety function, such as the immediate control function, semi-autonomous function and warning function
- demand rate, which enables the risk level to be shifted (IEC 61508-5 Table E2)
- other measures, which enable the risk level to be reduced if other measures are applied to reduce the risk (IEC 61508-5 Section E5)

The first two parameters could be useful for estimating some machines, but for some machines they only complicate the estimation. The accuracy of a risk may improve when there are many parameters and several levels for each parameter, but the input information is almost always uncertain and the accuracy of the result cannot be better than the input information. The nature of a risk is that uncertainty is involved. If a risk is certain then it should be accepted or something done about it. The freedom of parameters should match their uncertainty. Too much freedom in the parameters could lead to a scenario that is far from the practice.

2.3 Survey relating to risk assessment

A questionnaire relating to the risk assessment and safety requirements specification of safety-related control systems and applications was conducted in this project.

2.3.1 Description

In this project, the questionnaire relating to the risk assessment and safety requirements specification of safety-related control system development was conducted using an online computer solution for conducting surveys, gathering data, managing feedback, and reporting data.

The invitation to answer the questionnaire was sent at the end of October 2014 via email to approximately 160 relevant contacts, mainly in the machinery sector in Finland, Sweden and Norway. Recipients were also requested to forward the message to other experts in their organization.

The purpose of this questionnaire was to identify the used risk assessment principles, methods, tools and standards and to find out the main sources of safety requirements, tools and practices to manage safety requirements concerning safety-related control system development.

In the questions, the respondents had to choose one or more suitable options and, in addition, in some cases they could specify the answer more precisely in text format ('please specify' at the end of the question).

The questionnaire was confidential: companies and individuals could not be identified from the results.

2.3.2 Results

This section presents the results of the questionnaire together with some comparisons between the groups. It would have been interesting to draw conclusions about the differences between countries, but it was not feasible due to the small number of answers from some of the target countries.

There were a total of 72 answers: 50 from Finland, 15 from Sweden and 7 from Norway. When studying the questionnaire results, it should be noted that the questions were formulated so that in some cases the respondent could choose one or more options, which led to the sum of the responses in many cases being more than 100%.

Most of the respondents (54.17%) considered themselves safety specialists. The tasks of the respondents in their enterprises are presented in Figure 7. The respondents were generally fairly experienced, with over half (54.17%) of all the respondents having more than 10 years' experience in their task or field. More than 26% of the respondents had 5 to 10 years' experience and fewer than 20% were novices or had less than 5 years' experience of their task.

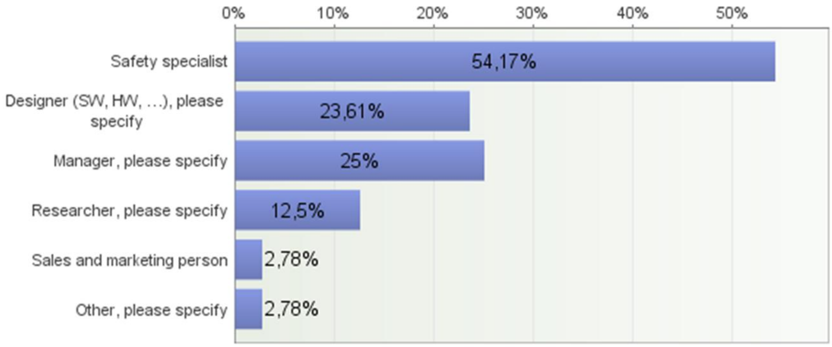


Figure 7. Tasks in the enterprise, number of respondents: 72. Respondents were able to choose one or more options.

Figure 8 presents the field of interest or line of business. The most common line of business among the respondents was 'machinery' (62.5%), the second most common was 'control systems and modules' (50%) and the third 'safety components' (37.5%). As an 'other field', the respondents were mainly researchers or from some institutes or equivalent. Almost 70% of the respondents considered their point of view to be more system oriented than device or component oriented. These figures are a good indication of the groups at which the survey was targeted.

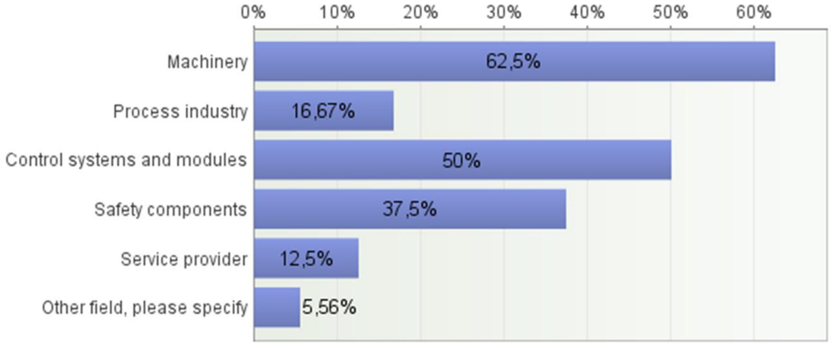


Figure 8. Field of interest or line of business. Number of respondents: 72. Respondent was able to choose one or more options.

The questionnaire asked about the procedure for performing risk assessment for the system or device under consideration.

Figure 9 presents the most common groups making the risk assessment. The safety organization of the company usually conducts the risk assessment together with experts (49.3%), or designers of the company make the risk assessment concurrently with other design personnel (42.25%). In some cases, the risk assessment work is purchased from external specialists (25.35%) or subcontractors make the risk assessment for their products (21.13%).

Figure 10 shows that when comparing the lines of business, the spread is broadly similar in terms of the fields of machinery, safety components and control systems and modules but, for example, in the process industry, designers or experts seldom participate in risk assessment. However, a positive observation is that only in a few cases did the safety organization of the company conduct risk assessment on its own; instead it utilized the expertise of designers and other specialists.

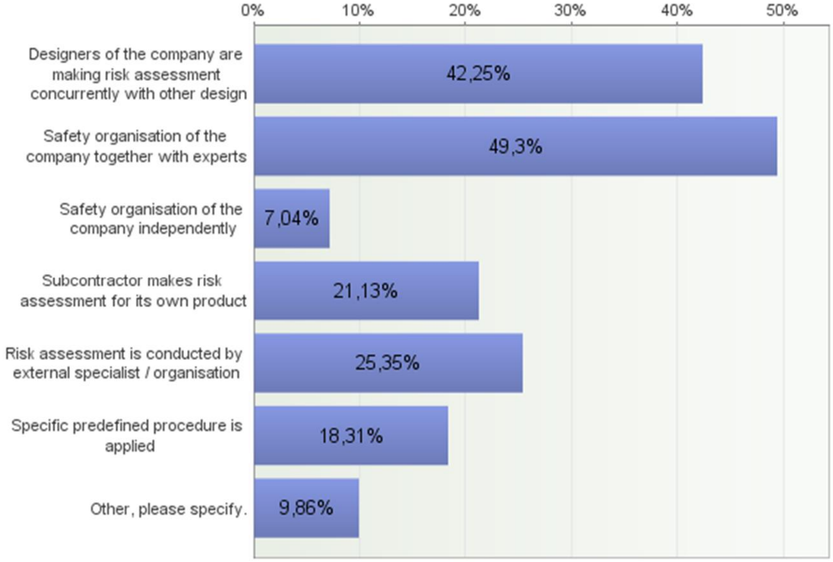


Figure 9. Procedures for making a risk assessment for a system. Number of respondents: 71. Respondents were able to choose one or more options.

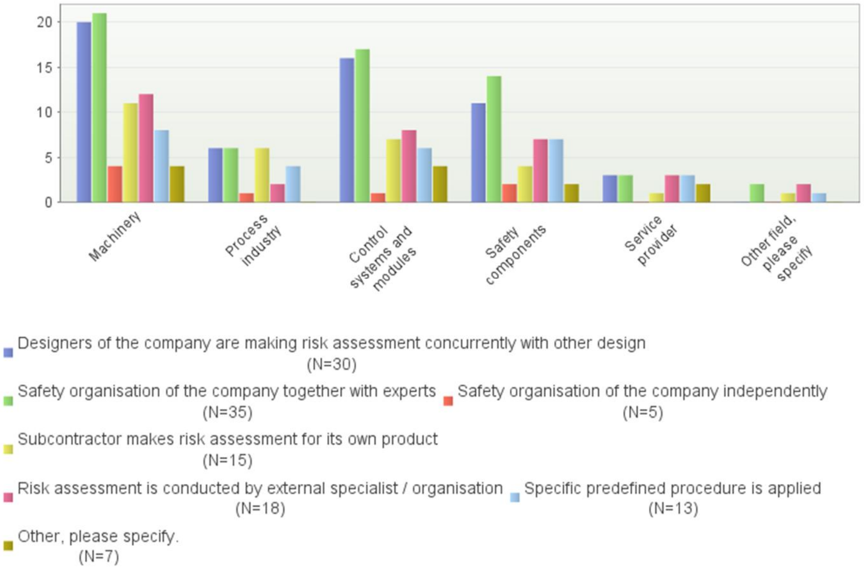


Figure 10. Comparison of procedures in different businesses for making risk assessment for a system. Number of respondents: 71. Respondents were able to choose one or more options.

One of the aims of this questionnaire was to identify standards and methods applied in risk assessment and functional safety SIL/PL assignment processes (see Figure 11). It turned out that the ISO 13849-1 method is the most commonly used (68.57%) and that the IEC 62061 method is also applied quite a lot (27.14%). Other commonly applied methods were ISO 12100, which gives general principles for risk assessment and risk reduction in machinery, and IEC 61508, titled Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. In addition, the old EN 954-1 was still in use according to more than 11% of the respondents.

When considering different lines of business, there were no significant differences in the use of the standards except for process industry and service providers for which the distribution was more even between the standards and methods in question. However, the number of respondents in these groups was low.

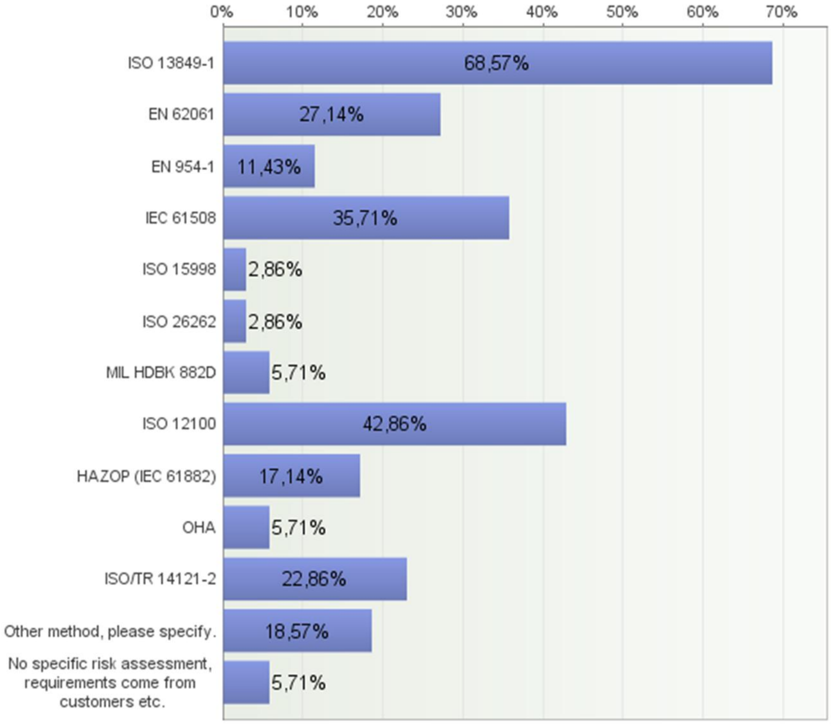


Figure 11. Distribution of standards and related methods used in risk assessment. Number of respondents: 70. Respondents were able to choose one or more options.

Most of the respondents use MS Office Excel (over 30%) or MS Office Word (over 80%) as a tool for conducting risk assessments. Only approximately 30% apply some specific risk assessment tool. More than one-fourth of those using specific risk assessment tool use some company-specific tool while the rest use some commercial application; the most common (appr. 33% of users of commercial tools) was SISTEMA Software PL Calculation Tool.

Figure 12 shows that safety requirements used as a design basis are gathered from different sources, mainly standards and norms (over 93%) or legislation and directives (over 80%). Another important source for conducting requirements is risk assessment work (almost 70%), and about 43% of respondents receive safety requirements directly from their customers. Previous experience of designers and users is also used to formulate safety requirements. Apparently, legislation is followed and standards provide good advice, but in some cases they are not on the respondents' top four list.

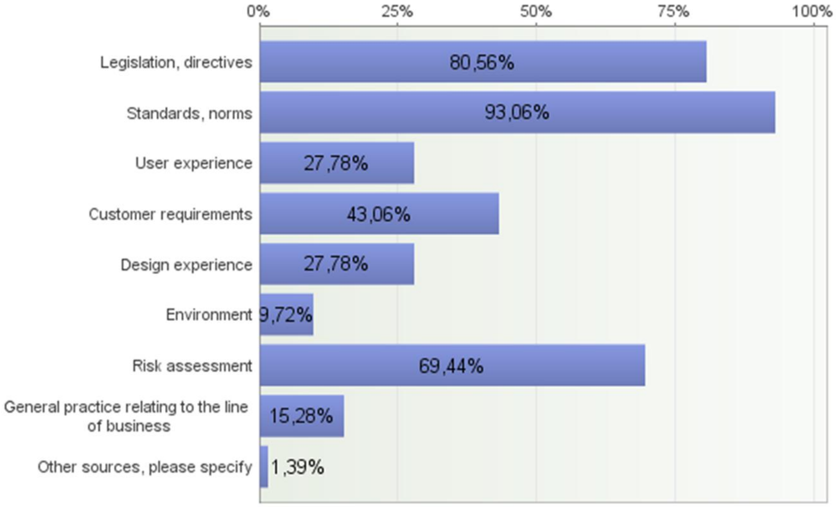


Figure 12. Sources of safety requirements. Number of respondents: 72. Respondent were requested to give 1–4 main sources of safety requirements.

Respondents were also requested to estimate resources and costs related to risk assessment (see Figure 13). Nearly half of the respondents considered the share of risk assessments to be between 1 and 5% of the design resources. Almost one-fourth estimated it to be 5 to 10%. The average of the answers is about 5%.

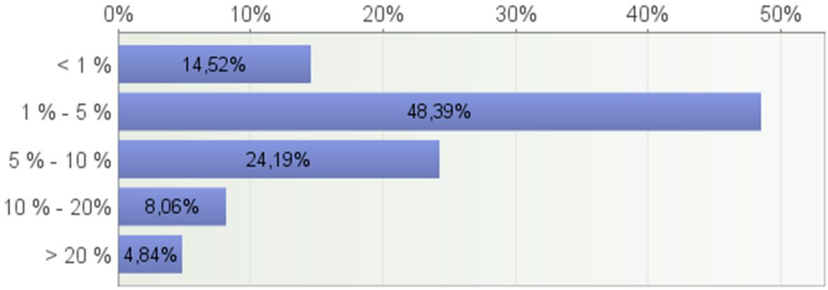


Figure 13. Share of risk assessment resources

We also had other questions concerning resources and costs: the respondents were asked to estimate the additional costs or resources when developing the control system from an existing SIL1 (or PL c) product to a SIL2 (or PL d) product and when changing the standard system to a safety system without changing the main properties of the product. Figure 14 shows the distribution of answers to the first question. The average of the answers is about 80%. The answers are fairly evenly distributed over the options 0–20%, 20–50% and 50–200%. This indicates that the answer is unclear and depends on the background of the respondent or the resources vary depending on the cases. One interesting detail was that managers typically estimated costs to be higher than other task groups did (task groups are presented in Figure 7) and researchers had more optimistic estimations as they ended up with slightly lower costs.

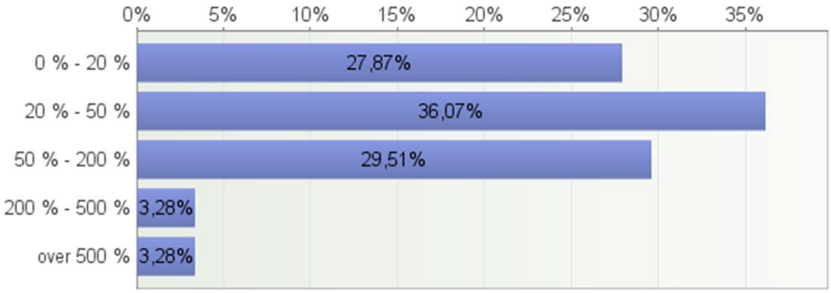


Figure 14. Additional costs/resources when developing (including design, coding, testing, etc.) the control system from an existing SIL1 (or PL c) product to a SIL2 (or PL d) product without changing the main properties of the product. Number of respondents: 61.

Figure 15 presents estimations of the additional costs or resources in the common situation of changing a standard system to a safety system without changing the main properties of the product. The costs or resources are estimated to be slightly higher than in the previous case (Figure 14). This indicates that increasing safety level from no to low require more resources than increasing safety level from 'low to moderate'. The average amount of additional resources in the 'no to low' case is about 120%.

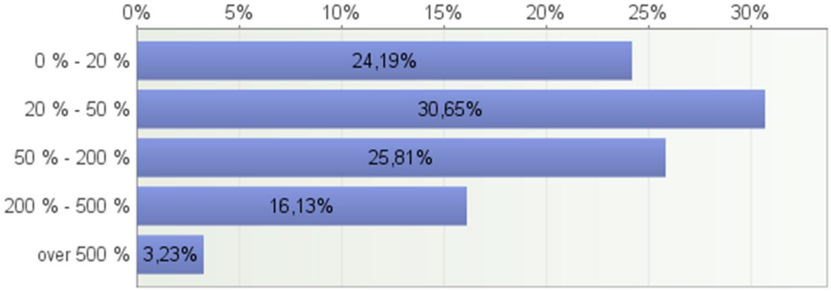


Figure 15. Additional cost/resources when changing a standard system to a safety system without changing the main properties of the product. Number of respondents: 62.

The questionnaire also focused on sorting out the sources of some quantities and parameters such as mean time to failure (MTTF) or mean time between failures (MTBF) and diagnostic coverage (DC). The two first-mentioned were typically decided from standards or manufacturers' data sheets while there was more deviation in the answers concerning diagnostic coverage. However, the main sources were congruent with the MTTF/MTBF question. A positive observation was that manufacturers' data sheets were the most common source of MTTF/MTBF calculations, since they are supposed to have the most accurate values. For DC sources, FMEDA and expert judgement result in relatively low values, since specific DC values are seldom received from other sources. Manufacturers' data sheets are typically available for specific safety devices and, perhaps, the respondents remembered this when answering the questions. Figure 16 and Figure 17 present the answers from 71 respondents capable of answering these particular questions.

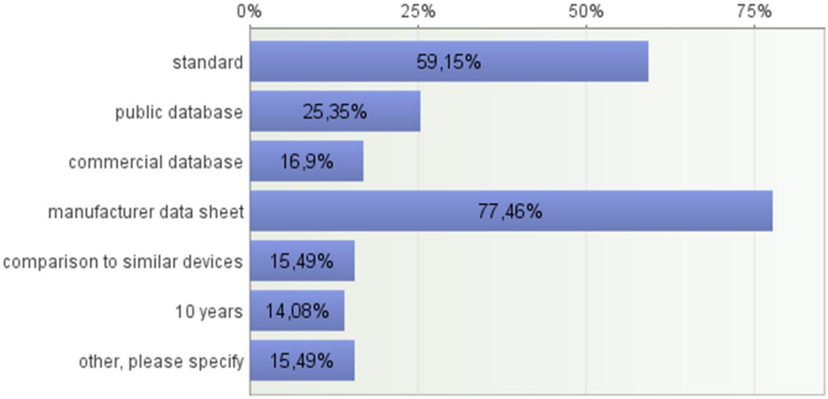


Figure 16. Sources for deciding the Mean time to failure (MTTF) or Mean time between failures (MTBF). Number of respondents: 71. Respondents were able to choose one or more options.

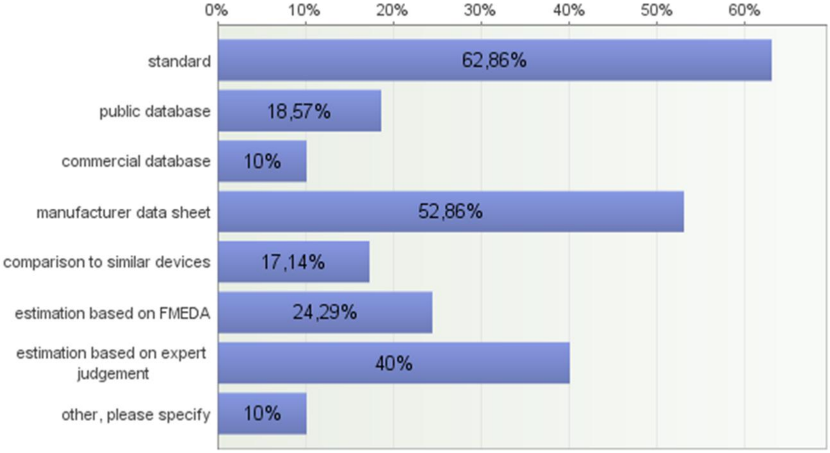


Figure 17. Sources for deciding the diagnostic coverage (DC). Number of respondents: 71. Respondents were able to choose one or more options.

3. Round robin test experiments related to risk assessment

A round robin test is an interlaboratory test that includes measurements, analyses or experiments. It is performed independently for a certain sample by multiple independent scientists and experts from different institutes or enterprises. A round robin test is executed according to a pre-determined plan.

In this study, the objective of the round robin test is

- to find the criteria for the selection of methods and techniques
- to find the best methods and techniques for risk assessment and safety requirements specifications
- to find the strengths and weaknesses of methods used in the early safety life cycle phases of safety-related control system (SRCS) design using a comparative approach
- to find uniform principles, practices and methods used in different institutes

The mobile work machine experiment and the robot experiment were realized by applying a round robin test. The purpose was to compare the two risk assessment methods that were used to give us the requirements for the safety functions. Our aim was 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 each parameter affects 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 the required PL_r for the safety function presented in ISO 13849-1. In all cases, the risk analysis text was prefilled and only the parameters had to be filled in. All the test persons conducted the risk assessment for nine cases (either robot or mobile machine cases) and used both the IEC 62061 and ISO 13849-1 methods. Background information on the persons or groups that analysed the cases was also collected.

When calculating average values in the round robin tests, the PLs are converted into SILs according to the following formula, using linear interpolation between the fixed numbers/letters (see Figure 19 and Figure 22):

$$\text{PL a}\rightarrow 0.5;\ \text{PLb}\rightarrow 1;\ \text{PL c}\rightarrow 1.3;\ \text{PL d}\rightarrow 2;\ \text{PL e}\rightarrow 3 \qquad (1)$$

Both SILs and PLs use a logarithmic scale, and the comparison between them can therefore 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 equivalent SIL and is set to the middle value between SIL 0 (almost no risk) and SIL 1, which gives us a rough estimation and makes 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 that from SIL 1 to SIL 2. This definition is more like the risk and severity perspective than the probability perspective since the probability of SIL 0 is not defined. [Malm et al. 2015.]

3.1 Mobile work machine experiment

The mobile work machine experiment was realized by applying a round robin test to compare two risk assessment methods resulting in requirements for the safety functions. The aim of this study was to test how objective the methods are and if there is a difference between the methods. All the parameters gathered in the assessment are also evaluated in order to see how each parameter affects the results.

3.1.1 Description

Risk estimation studies for nine mobile work machine cases (see Appendix A) were conducted by persons from industry and research. The mobile work machine cases were selected so that there is a requirement for the safety function set by a corresponding C type standard i.e. the risk level is already estimated in the standard. The risks are reduced by applying the safety functions. The methods used in the risk estimation are based on the SIL assignment process presented in EN 62061 and the risk graph for determining the required PL_r for the safety function presented in ISO 13849-1. All the persons or groups made the risk assessment for all nine cases and applied both the IEC 62061 and ISO 13849-1 methods.

All the examples were collected from standards in order to obtain a basic level for the risks and to have both high and low risk cases. The written descriptions of the hazard situations were copied from the standards ISO 15998-2 and EN 280 so that the descriptions were neither translated nor modified. Cases 7 to 9 had some additional sentences in order to complete the idea presented in the standard. The examples presented in the standards are applied here as test cases and are not normative requirements i.e. in each case the risk level may differ from the standard suggestion if risk assessment proves it.

Information on the background and experience of persons or groups that analysed the cases was also collected (risk assessment, mobile work machines, machine automation, machinery and research). Otherwise the study was made anonymously. The first tests were done at the Safe Technology seminar organized by the Mechanical Engineering and Metals Industry Standardization in Finland

(MetSta). During that session, six groups (2-4 persons) and two individuals had one hour to do the risk assessment and discuss the results. The rest of the answers were gathered later by email.

There are nine mobile machine cases related to tractor loaders, articulated wheeled loaders (loaders with a pivot joint that 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 [ISO/TS 15998-2 2012] and EN 280 [EN 280 2013] in order to enable us to compare our results with those of the standard. The case descriptions are short since the texts were from the standards, which aim to have a relatively broad scope. The applied examples are not in the normative part of the standards. All the case descriptions gave hints to aid the analyst in choosing severity, frequency, exposure and possibility of avoiding the 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 covered both high and low risk examples. According to the corresponding machine standards (ISO/TS 15998-2 and EN 280), the performance levels (PL) 0, a, b, c, d and e were included. The analysis was typically done 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 18.

Figure 18. Figure for case 1.

Case 1: 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.

3.1.2 Results

Table 11 and Table 12 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, at the bottom is the case number and above this, the answer suggested by a standard. The bold numbers (value can also be seen in the std. row) indicate the risk levels suggested by the standard. We see that there is some variation in all 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 out. There is slightly more variation for PLs than SILs.

Table 11. 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 12. 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 19 shows the 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 analysts' mean value is about 1.5. In this case the driver may hit his head on the windscreen 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 safety functions, such as ABS (anti-lock braking system), are required to reduce the braking. In case 5, the standard risk/requirement is SIL 3, whereas the average is less than SIL 2. In this case, steering is lost while the machine may be in traffic. The traffic possibility, however, is 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 closer to the standards.

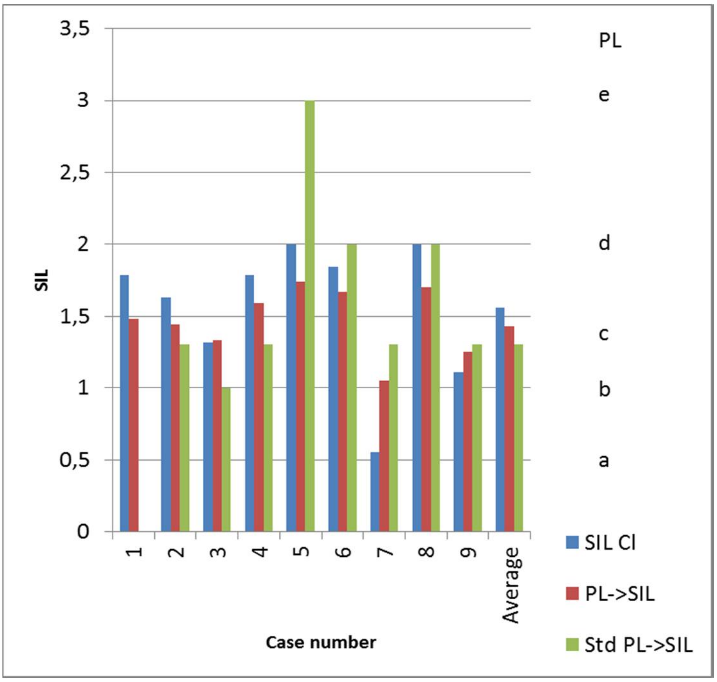


Figure 19. Average value and standard suggestion for each mobile machine case.

Table 13 shows cross-tabulation between the answers with the IEC 62061 method and the ISO 13849 method. The yellow cells represent the equivalence between the requirements according to the standards. If all the answers were in the yellow cells then the analysts would have reached the same conclusions using both methods. The lower left corner indicates that SIL has a higher value than PL and vice versa for the upper right corner. It can be seen that in 34% of the cases, the IEC 62061 method gives a higher value than the ISO 13849 method, and the situation is the opposite in 15% of the cases. The answer was similar in 51% of the cases.

Table 13. Cross-tabulation of answers made with the IEC 62061 method and the ISO 13849 method of the same cases in the mobile work machine experiment.

SIL \ PL	o	a	b	c	d	e
0	3	16	6	11	1	2
1	0	2	4	10	3	0
2	0	0	1	42	42	2
3	0	0	0	0	13	11

Figure 20 shows average values for the way different expert groups have answered. The number of participants in each group is relatively small and each analyst may have been a member of several expertise groups. It is interesting that the work machines group (specialists of the machines under control) has the lowest average value. However, the number of answers is so small that the statistical significance is low.

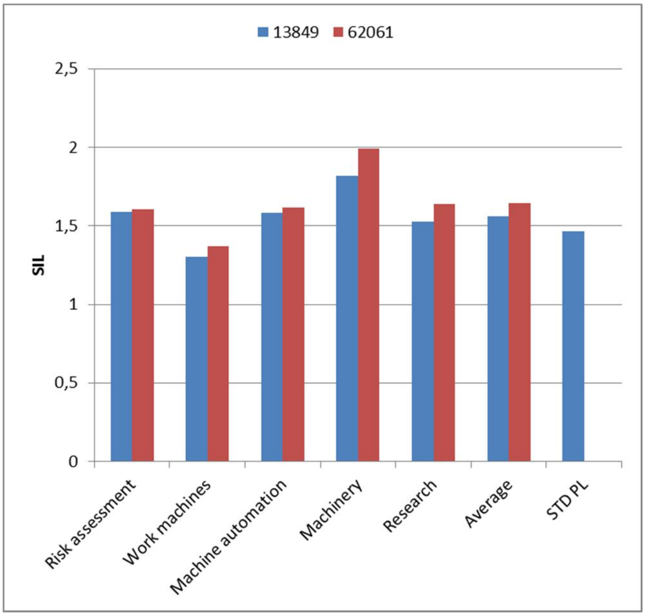


Figure 20. Average answers of expertise groups.

The distribution of parameters can be seen in Table 14 and Table 15. Severity is usually estimated to be high, but other parameters are more scattered.

Table 14. Distribution of parameters applying the IEC 62061 method.

Param.\Cl.	1	2	3	4	5
Severity	9	8	41	108	☒
Frequency	1	33	48	32	52
Probability	8	112	44	1	1
Avoiding	30	14	52	3	30

Table 15. Distribution of parameters applying the ISO 13849 method

Param.\Cl.	1/low	2/high
Severity	33	133
Frequency, exposure	117	49
Possibility of avoiding hazard	107	59

3.2 Robot experiment

This study also focused on the comparison between the two standards ISO 13849-1 and IEC 62061. The test resembles the mobile work machine test and the same equations have been used to analyse the results.

3.2.1 Description

The robot experiment resembled the work machine experiment in its set-up, 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 industry. The delivered material is described in Appendix B.

To have some kind of ‘right’ answer to compare our results with, an expert assessment was made by two persons working with risk assessments. All personnel involved in making the cases were excluded from the experiment.

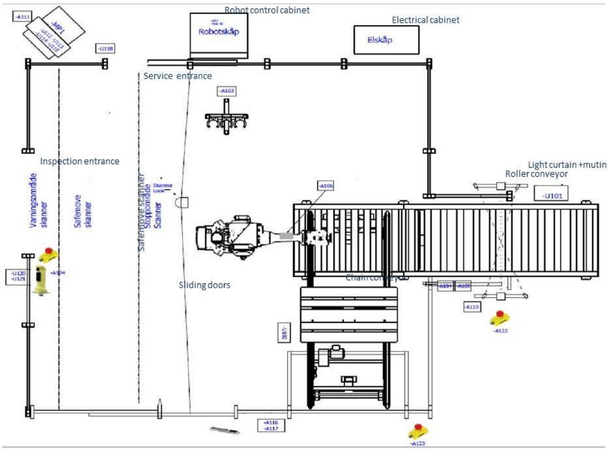


Figure 21. Robot case diagram

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 a way or at a speed that is unpredictable.
- **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: visitors and different workers.

Each person made a risk assessment for these same nine cases, using each of the two standards. The standards have one method each for deciding the required level of safety, the PL (performance level) in ISO 13849-1 and SIL (safety integrity level) in IEC 62021. The methods resemble one another, but there are different numbers of factors involved as well as different numbers of levels to decide severity, frequency of exposure, etc. As for the mobile work machine experiment, information on the background and experience of the persons performing the assessment task was also collected in the robot experiment (there were some more categories, including software, since the test persons had more widespread backgrounds in this case).

3.2.2 Results

Table 16 and Table 17 show the answers of the robot experiment. In the tables, the ‘correct answer’ according to the expert group is in bold and can also be seen in the std. row. For cases 1 and 8 there is no right answer since no safety functions are needed. The graphs look similar, as expected.

Table 16. 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 17. Number of answers in 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 22 shows the average answers to each case. ‘SIL Cl’ refers to the IEC 62061 method, PL -> SIL refers to the ISO 13849 method and ‘Std PL -> SIL’ refers to the expert judgement when applying the ISO 13849 method.

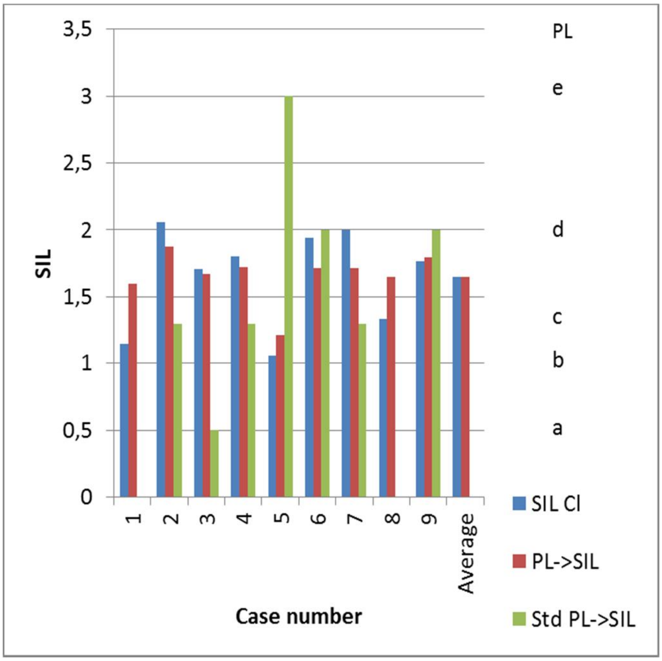


Figure 22. Average values for each of the nine robot cases and the expert judgement.

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 to assess a lower value.

Case 5 was generally assessed at 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-ups, and interlocking doors were the safety means. According to the case description, there are instructions for the 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 the padlock shall be calculated in the assessment according to IEC 62061, but people seem to have missed this information.

Table 18 shows the relationship between the answers of the two standards. The yellow boxes represent the correct correlation, i.e. the requirement level is similar according to the standards.

Table 18. Cross-tabulation between IEC 62601 and ISO 13849-1.

SIL \ PL	o	a	b	c	d	e
0	0	5	4	5	4	0
1	0	1	4	8	6	1
2	0	0	1	26	42	5
3	0	0	1	1	9	7

3.2.3 Conclusions of the robot experiment

In most cases the risk was assessed to be higher or equal to the recommended value.

As shown in Table 18, it is also more common to have a stricter judgement when using IEC 62061. The risk and required level of safety is assessed a little higher with that standard. This same result was noticed for both the robot risk experiment and the mobile work machine risk experiment.

Influence from experience and field of work:

- People who are not used to working with risk analysis or the expressions PL and SIL have a hard time understanding the gist of a the ‘safety function’. When performing the risk assessment, they assess the factors’ severity etc. for all hazards including those that are not associated with a safety function (SF). One opinion was that all risks have to be assessed and taken care of, whether the measure is an SF or not.
- In the survey (see Section 2.3) some people did not cross the alternative risk assessment as a source of requirements. This might have been because some of them only manufacture part of a safety function and therefore do not make a risk assessment in its normal sense. The risk analysis is performed when the part is integrated into a whole SF.
- When different companies perform risk analyses, the results differ from almost no material at all to a vast investigation.
- Some machine builders do not include safety functions that are mandatory according to standards in the risk assessment, since they always have to be included in the machine. When it comes to things that are mandatory, however, they still have to fulfil a certain level of security.

3.3 Summary of the mobile work machine and robot experiments

Table 19 shows a cross-tabulation of the SIL and PL answers from the mobile work machine and the robot experiments. Each cell shows how many times the analysts choose a specific PL (ISO 13849 method) and for the same case the corresponding SIL (IEC 62061 method). The cells with text in bold indicate the equivalence between SILs and PLs, i.e. if all the numbers were in these cells, all the 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 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 total average SIL when applying the IEC 62061standard is 1.63 and when applying the ISO 13849 standard 1.64 (transformation according to formula (1)), i.e. the average is about the same.

Table 19. 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 19 also shows that SIL 0 is chosen much more often than PL 0 – 57 vs. 3 times. ‘PL a’ corresponds to SIL 0, yet there is a 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 had 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 also electronic components, robots (instead of mobile work machine), software, system integrator and distributor/agent. In both cases, the number of test persons in each group was relatively small and there was also an overlap between the groups.

The differences between the expertise groups were relatively small. In the mobile work machine experiment the lowest risk levels were given by the work machine experts, i.e. the persons who know the work machines best. 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 that of 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.

3.4 Discussion on the mobile work machine and robot experiments

The round robin test included nine cases related to mobile work machines and nine cases related to a robot cell. In all the cases, two methods were applied to assess the risk level. The test persons (analysts) did not spend much time on each case and they did not usually have additional material like standards or data to support their decisions. The decisions are therefore mainly based on experience and on using each participant's background knowledge. The information given for each mobile work machine case was short and focused on the parameters of the risk. A picture was supplied in order to define the size and type of the machine. No general description was given. For the robot case, there was more material and all cases were related to the same robot cell. More information may give more accurate results. However, the parameter descriptions may have been given even more precisely in the mobile work machine test

It is often claimed that the analysis tool should be calibrated for the relevant branch of technology in order to reach valid results [IEC 61508-5]. This refers to the tacit information and culture related to each branch of technology. In our case the analysts were not able to make any comparisons with the practice 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 was at the same level, and yet, by choosing different parameters, the level of the assessed risk might have been 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 [Dragan & Woo 2010] – we find that the readability index correlates strongly with the number of correctly identified risk levels when using ISO 13849. The table below shows readability and the number of correctly identified risk levels for the machinery.

Table 20. Number of matches between the standard answer and the analysts' answer in the 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 described in Table 21.

Table 21. 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.

The deviation of severity is lower than the deviation of frequency and avoidance. Probability (in ISO 62061) has the lowest deviation. It is probably unclear how to define frequency and avoidance. The standard deviation of SILs or PLs is at about the same level (0.88–0.84). The difference between the standard requirement and the estimated values shows that the accuracy of IEC 62061 is 0.69 and for ISO 13849-1 it is 0.89.

When we apply the IEC 62061 method, SIL 1 is a quite rare result compared to the results when using the ISO 13849 method. In addition, according to the standards (mobile work machine experiment), the risk should have been assessed as SIL 1 in five out of nine cases, but SIL 1 did not get the majority of the results in any of the cases and it was average in only one case.

Figure 23 presents the distribution of all the answers, showing 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.

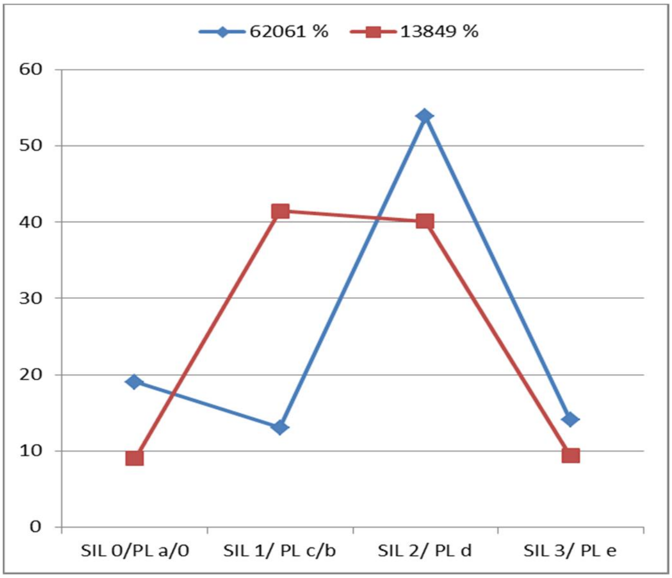


Figure 23. Distribution of answers (%) in mobile machine and robot experiments. There were a total of 299 answers in the experiments.

In the matrix of the IEC 62061 standard (see Table 6), SIL 1 is only available in three cells of the matrix and is not available when the severity is high (severity=4). This leads to a low number of SIL 1 results in the risk analysis. The ISO 13849 risk graph or the matrix (see Table 22) shows that half of the matrix cells lead to either PL b or PL c, both of which are associated with SIL 1. It could be claimed 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 22. The ISO 13849 risk graph presented in 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 23. ‘Severity 0’ cases are not included in the table since in those cases the other parameters were not estimated. The table resembles Table 22, but the number of answers is included.

Table 23. Numbers 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 numbers of answers according to severity and class (Cl) are shown in Table 24 (IEC 62061 matrix). The table can be associated with Table 6 and the SIL values are in the corresponding cells. SIL 2 is in **bold** and SIL 1 is in *italic*s. The SIL requirements are also shown in the cells. Table 24 shows that a large number of the answers (27) are just below SIL 1 in the ‘other measures’ area (according to IEC 62061; see also Table 6). 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 quite a common response, known as the end-aversion bias or the central tendency [Choi & Pak 2005].

Table 24 and Table 23 also show that a large number of analysts estimated the severity at 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 the ‘OM’ cells (Table 6) also corresponded to SIL 1, the result would be closer to the ISO 13849 method result. 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.

Table 24. Numbers of answers in the mobile machine experiment according to severity and class range (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*

Table 25 shows the share of answers for each class (Cl) and severity for both the mobile work machine and for the robot experiments. The table shows in detail how each CI number has answers and also allows testing of other possibilities to define SILs.

Table 25. Share of answers (%) in the mobile work machine and the robot experiment according to severity and class range (IEC 62061).

Summary %

	CI=Fr+Pr+Av												
Severity	3	4	5	6	7	8	9	10	11	12	13	14	15
4	0.0	1.4	1.4	6.4	9.5	9.8	12.8	10.5	6.1	3.7	3.4	1.0	0.0
3	0.0	0.0	2.7	2.7	3.7	5.7	4.4	2.0	1.4	1.0	0.3	0.0	0.0
2	0.0	0.0	0.3	0.0	1.0	2.0	2.0	0.7	0.7	0.0	0.0	0.0	0.0
1	0.0	0.0	1.0	0.0	0.3	0.3	0.7	0.0	0.3	0.0	0.3	0.0	0.3
0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Table 26 shows one possible way to change the parameter limits to obtain results relatively similar to those obtained by the ISO 13849 method, especially regarding SIL 1 and SIL 0. The changed parameter limits are underlined. In practice, this means that some cells, which result in SIL 0 or SIL 2, are changed to SIL 1. The results of this experiment/proposal are presented in Table 27.

Table 26. How to change the parameter limits of the IEC 62061 method to obtain similar results to those with the ISO 13849 method.

SIL values new proposal

	CI=Fr+Pr+Av												
Severity	3	4	5	6	7	8	9	10	11	12	13	14	15
4	1	1	1	1	1	2	2	2	3	3	3	3	3
3	0	0	0	1	1	1	1	1	1	2	2	3	3
2	0	0	0	0	0	0	1	1	1	1	1	2	2
1	0	0	0	0	0	0	0	0	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0

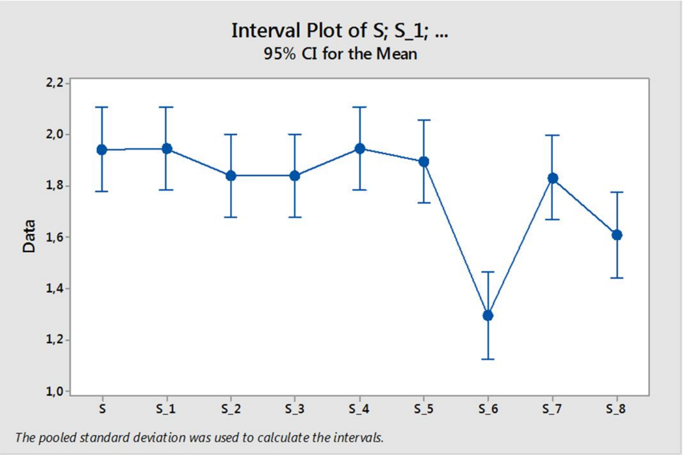
Table 27. Result when applying the parameter limits presented in Table 26 and summary of shares presented in Table 25.

	Shares %			
	SIL 3	SIL 2	SIL 1	SIL 0
IEC 62061	14	54	13	18
New prop. IEC 62061	14	34	43	8
ISO 13849	9	41	42	8

In the results, the severity parameter is often given the highest value. The question is whether 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 was only considered in five mobile machine cases, i.e. the cases picked from the ISO/TS 15998-2 standard [ISO/TS 15998-2 2012]. The severity was high in four cases and low in one case.

In most of the cases, the answers by the test persons are close to those of the standards and the average was a little higher than that suggested by the standards. 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 those of the standards. A similar observation was found in previous research by Hietikko, Malm and Alanen: Risk estimation studies in the context of a machine control function [Hietikko et. al. 2011].

Since the two standards use different numbers 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 (Figure 24, Figure 25 and Figure 26) show, the parameters in the two standards that are comparable follow the same paths. The diagrams are from the mobile work machine experiment.



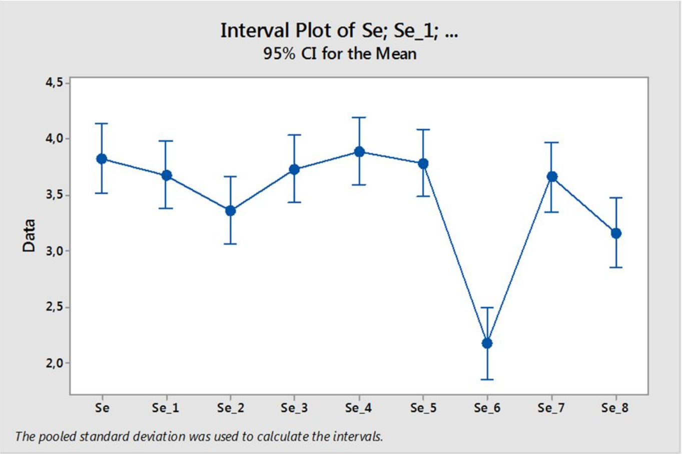


Figure 24. Paths for the mean value of severity (S, Se). ISO 13849 method above and IEC 62061 method below.

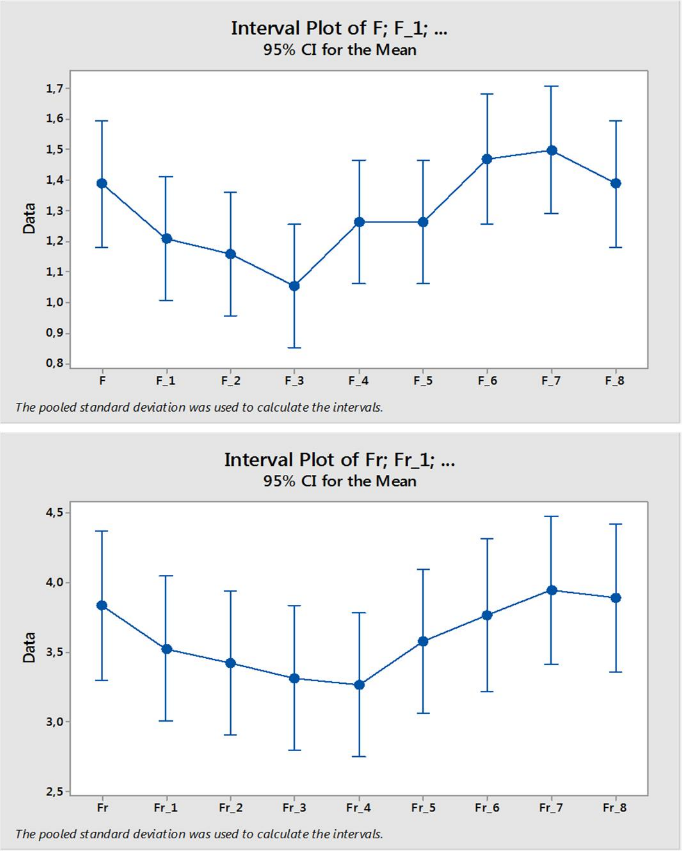


Figure 25. Paths for the mean value of frequency (F, Fr). ISO 13849 method above and IEC 62061 method below.

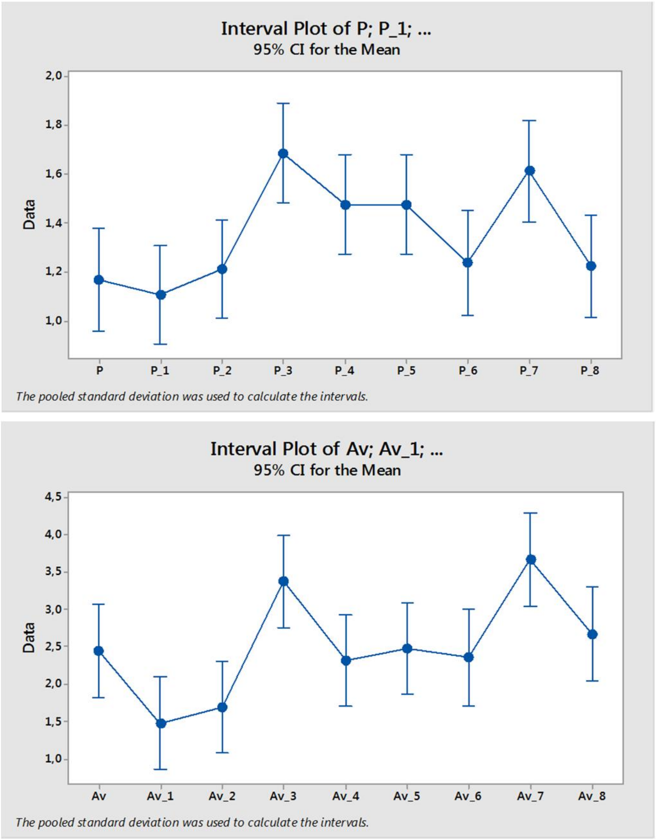


Figure 26. Paths for the mean value of probability of avoiding hazard (P, Av). ISO 13849 method above and IEC 62061 method below.

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 obtained the results shown in Table 28.

The two standards have the following risks assessment 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 happens only according to the frequency parameter (probability is 100% or included in the frequency parameter).

Since hazard avoidance is already 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. According to the standard IEC 62061, the parameter is related to the predictability of the occurrence.

Table 28. 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

3.5 Conclusions of the round robin test

We see that the distribution of parameters in both the IEC 62061 method and the ISO 13449 method give relatively similar results for each case. This is as expected since the analysts analysed the same cases. Yet there is a difference between the 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 more often results in 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 shown. 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.

One might think that by applying two different methods, like the IEC 62061 and ISO 13849 methods, the result would be better. Table 19 shows how analysts have answered the corresponding cases according to the methods in standards IEC 62061 and ISO 13849-1. In most cases, the results are similar and there is usually only one level difference between the results. However, according to the IEC 62061 method, SIL 0 may even correspond to PL e according to the ISO 13849 method. The reason is usually the severity parameter since moderate severity often leads to SIL 0.

In the mobile work machine experiment, one case was chosen to have the lowest risk (SIL 0) and one the highest risk (SIL 3) according to the corresponding standards. These extreme values were often not found by the analysts. If little information is available, the analysts tend to avoid extreme results. In these two cases, more information from standards could have resulted in more answers similar to the standard.

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. [1984] shows that assessors prefer case descriptions over relative frequency information.

3.6 Demonstration tool

A demonstration tool was made that enables risk level estimation to be filled in automatically after the parameters of the risk and their criticality are defined. This means that parameters can be filled in first and the level corresponding the parameters can be defined later in the table (see Table 29). The text corresponding to the parameters can be written in the table and the analysis tool will read the table and fill in the analysis according to the ‘Severity’ and ‘CI’ parameters. Table 29 shows how the cells can be changed to correspond more to the ISO 13849 method results according to the round robin experiments. The values in parenthesis correspond to the IEC 62061 method results if the plain number differs from the standard. The colours in the table indicate the original IEC 62061 method results (red= SIL 3; blue= SIL 2; green= SIL 1; white= SIL 0/no requirements).

Table 29. Example of the demonstration tool.

	CI=Fr+Pr+Av												
Severity	3	4	5	6	7	8	9	10	11	12	13	14	15
4	1 (2)	1 (2)	1 (2)	1 (2)	1 (2)	2	2	2	3	3	3	3	3
3	0	0	0	1 (0)	1 (0)	1	1	1	1 (2)	2	2	3	3
2	0	0	0	0	0	0	1 (0)	1 (0)	1	1	1	2	2
1	0	0	0	0	0	0	0	0	1 (0)	1 (0)	1 (0)	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0

By changing the values presented in Table 29, it is possible to obtain the ISO 13849 method by removing the ‘Pr’ factor (set to ‘0’) and allowing only parameter numbers ‘1’ and ‘2’. The change from the IEC 62061 method to the ISO 13849 method by applying the tool is presented in Table 30. It can be seen that although the ISO 13849-1 standard presents the method as a risk graph, the method can also be presented in a matrix format.

Table 30. How to apply the ISO 13849 method and the tool (see Table 29).

	Frequency + Avoidance		
Severity	2	3	4
4			
3			
2	c	d	e
1	a	b	c

In the same way as in Table 30, many other analyses that contain severity and three other parameters can be processed with the tool. The idea of the tool is to:

1. define the draft table, standard values are a good guess,
2. define the parameters in the analysis of each case and
3. define the table precisely by determining what the parameter levels mean from the risk point of view.

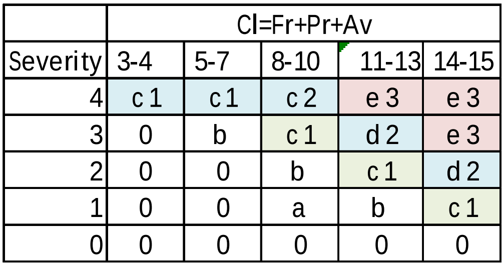
It is also possible to apply a summarizing matrix function (requires a Visual Basic macro to run the function) that shows the severity and probability of each case. Table 31 shows the results when all the mobile work machine cases are filled in, in the table (empty answers and no risk answers are not shown). The letters ‘a’ to ‘e’ correspond to the ‘Cl’ number of the IEC 62061 method (‘a’=3-4; ‘b’=5-7; ‘c’=8-10; ‘d’=11-13; ‘e’=14-15). The colours in the matrix indicate the risk level. This kind of approach shows the severity of the risks.

Table 31. Example of the tool view, which shows all the cases of the mobile work machine experiment. Empty cells are not shown.

-	a	b	c	d	e
1		26, 49, 122, 127,	119, 132,	116, 168,	130,
2		14, 39, 115,	118, 129, 131, 169, 170,		
3		34, 35, 48, 51, 52, 53, 58, 70, 96, 108, 125, 128, 146, 147, 153, 157, 159, 165, 166,	16, 45, 54, 72, 74, 75, 87, 91, 106, 110, 117, 120, 134, 148, 150, 154, 163, 167,	46, 124, 151,	
4	33, 43, 84,	1, 6, 15, 17, 22, 24, 25, 30, 32, 36, 38, 41, 47, 50, 56, 57, 71, 76, 77, 81, 89, 90, 93, 94, 95, 109, 113, 114, 121, 140, 171,	4, 5, 7, 8, 9, 10, 11, 12, 13, 18, 19, 23, 27, 28, 29, 31, 37, 42, 44, 55, 62, 63, 64, 65, 66, 67, 68, 69, 73, 79, 80, 82, 83, 85, 88, 92, 99, 100, 101, 102, 103, 104, 107, 111, 112, 141, 149, 155, 156, 160,	3, 21, 40, 59, 60, 61, 78, 86, 97, 98, 105, 126, 136, 137, 138, 139, 142, 143, 144, 145, 161, 162, 164,	135,

A coarser tool was also made that shows a modified IEC 62061 method results and suggested PL (see Table 32). The tool does not allow quick modifications in the table, instead the functions in the cells need to be modified in order to obtain the necessary results. Table 32 shows the table that represents the results of the tool.

Table 32. Tool providing modified answers when applying the IEC 62061 method.



	CI=Fr+Pr+Av				
Severity	3-4	5-7	8-10	11-13	14-15
4	c 1	c 1	c 2	e 3	e 3
3	0	b	c 1	d 2	e 3
2	0	0	b	c 1	d 2
1	0	0	a	b	c 1
0	0	0	0	0	0

4. Discussion

This project ‘Compsoft’ and the resulting report focus on risk assessment used to estimating safety-related control system requirements. Several functional safety standards deal with the topics and they present several different methods. The risk is defined as a function that consists of a severity part and a probability part. The probability is divided into several parameters, which are not the same in all standards.

A questionnaire on risk assessment for estimating safety-related control system requirements helps to understand which methods are applied and their importance. The ISO 13849-1 standard seems to be the most important standard for the purpose, but other standards are also applied. For specific sectors of industry, the sector standards are important since they consider the specific features related to the sector.

The standards bring out factors that are important to the specific branch of technology. For example, controllability is an important factor for vehicles and mobile work machines, but, in general, machinery and process industry standards do not consider it. Control category (e.g. safety control function or warning) is also an important parameter for military systems. It could be possible to apply the ISO 13849 or IEC 62061 method by changing the parameter meanings to match each specific industrial sector. The method would then not be exactly according to the standard but it might match the case better if the tool was well calibrated for the sector.

A round robin test was done to study the differences between the methods used in the ISO 13849-1 and the IEC 62061 standards. They are both meant for the machinery sector, but they do differ. The ISO 13849 method has only three parameters, and each parameter has only two levels, but it results in 5 + 1 levels. IEC 62061 has four parameters and they each have three to five levels, but results in only 3 + 1 levels. The ISO 13849 method emphasizes a relatively low risk level, which is divided into two parts, compared with the IEC 62061 method, i.e. PL ‘b’ and PL ‘c’ equal SIL 1 and PL ‘a’ is below SIL 1. The round robin test shows that the IEC 62061 method does not result in SIL 1 very often. One remark in the test was that the IEC 62061 method more often shows no risk/no requirements than the ISO 13849 method. Both methods are sensitive to the severity parameter since it has a greater effect on the result than other parameters. Both methods show at least a moderate risk level (SIL 2 or PL c) if the severity parameter is high. In other standards such as ISO 26262 (ASIL) and ISO 25119 (AgriPL), a very low probability or good controllability may result in no safety requirements (only quality management) even if other parameters like severity are high. We should consider whether a very low probability/exposure can reduce a high severity risk even to a low risk level. ‘The probability to avoid or limit the hazard’ is a parameter that should be revised if it were able to reduce the risk to a low level.

When risk estimation process starts, there is already much information that is wasted because the risk estimation method does not use it, but begins the risk estimation by estimating basic parameters. The silent information can be applied by calibrating the analysis to the branch of technology. Could the beginning be a default risk level that is typical of a specific risk type and then the parameters shift the level up or down? This kind of approach is not studied in the project, but it could result in a more objective and accurate analysis.

5. Conclusions

Risk assessment processes are changing slowly as more experience is gained to support changes. In the draft ‘ISO/IEC 17305 Version 4 Safety of machinery – Design of control system to realize safety functions’, the SIL/PL assignment parameters have changed a little compared with ISO 13849-1 and IEC 62061. However, the ISO/IEC 17305 project is cancelled and the changes will be in the future in the ISO 13849 and the IEC 62061 standards.

The results of the round robin test show that there are differences between the IEC 62061 SIL and ISO 13849-1 PL assignment. The risk assessment does not always give a similar result. If the difference in low risk cases is taken into account then the results can be similar.

The technical report ISO/TR 14121-2 states that ‘Risk assessments are not scientific exercises; therefore, resources are best spent on risk reduction efforts rather than the optimizing of risk ratings.’ However, a wrong rating could lead to a dangerous or expensive solution, and it is often worthwhile paying attention to correct risk and requirement levels.

References

Chambers, C., Croll, P.R. and Bowell, M. 1999. A study of incidents involving programmable electronic safety-related systems. Interacting with computers, Vol. 11, No. 6, pp. 597–609.

Choi, B.C.K. and Pak, A.N.P. 2005. A catalog of Biases in Questionnaires. Public Health Research – Practice and Policy, Vol. 2, No. 1, 13 p.

Dragan, M. and Woo, A. 2010. The Methodology Used to Assess the Readability of the NNAAP Examination. NNAAP and MACE Technical Brief, February 2010.

EN 280. 2013. Mobile elevating work platforms. Design calculations. Stability criteria. Construction. Safety. Examinations and tests. 98 p.

Hendrickx, L., Vlek, C. and Oppewal, H. 1984. Relative importance of Scenario Information and frequency Information in the Judgement of Risk. Acta Psychologica, Vol. 72, No. 1, pp. 41–63.

Hietikko, M., Malm, T. and Alanen, J. 2011. Risk estimation studies in the context of a machine control function. Reliability Engineering and System Safety, Vol. 96, No. 7, pp. 767–774. Doi-link: 10.1016/j.ress.2011.02.009

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.

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.

ISO 26262- parts 1 -10. 2011. Road vehicles — Functional safety. ISO (the International Organization for Standardization).

Jones, C. 2012. 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

Malm, T., Stålhane, T., de Bésche, C., Venho-Ahonen, O. and Hietikko, M. 2015. From risks to requirements – a round robin test. SIAS – 8th International Conference on the Safety of Industrial Automated Systems. Königswinter Germany. 9 p.

SFS-EN 62061. 2005. Safety of machinery – Functional safety of safety-related electrical, electric and programmable electronic control systems. 198 p.

SFS-EN ISO 12100. 2010. Safety of machinery. General principles for design. Risk assessment and risk reduction. Finnish Standards Association SFS. 172 p.

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.

Round robin test. Wikipedia. retrieved 16.9.2015.

Appendix A: Test cases of mobile work machines

The first six cases were picked from ‘ISO/DTR 15998-2 (currently ISO/TS) Earth-moving machinery – Machine characteristics, electrical and electronic systems, operation and maintenance’. The standard also gives parameters for severity, frequency and possibility of avoiding hazard. Cases 7, 8 and 9 are related to the safety functions of EN 280.

Table 33. Test cases of mobile work machines

1. 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.
2. Steel tracked dozer traveling at speeds <12 km/h. Complete loss of all brakes for stopping. - Operator can only allow machine to coast to a stop or use blade to stop. -Steering does not remain functional. Bystander may be crushed between machine and hard surface. Bystander may be run over. Bystander is not frequently present in potential path of the machine. There is no possibility to steer machine. Bystander can move out of machine’s path in some cases. Machine speed is initially lower than most EMM (earth moving machinery).
3. Compact machine <20 km/h. Machine begins to propel with FNR in Neutral. - Operator is compelled to be present in cab. - Operator still has service brake. Bystander may be crushed between machine and hard surface. Bystanders close the machine and in the path less than 10% of time. Operator can stop the machine in the normal operating position. Operator will instinctively apply braking. Bystander can move out of machine’s path.
4. Articulated Wheeled Loader. Machine boom moves without command. Operator is not compelled to be in the operator station. Operator may be greasing machine, or otherwise near moving parts. Operator typically in harm’s way, much less than 10% of time. If operator is near moving part, it may be very difficult to get away quickly enough to prevent injury.
5. Articulated Wheeled Loaders < 40 km/h Complete loss of Primary Steering and Emergency Steering (Either steers uncommanded or not at all while propelling). - Operator has braking to stop the machine. - Operator is not warned prior to loss of steering. Potential to hit higher speed vehicle with multiple passengers. Multi-passenger vehicles in the path of machine is much less than 10% of time. Operator can stop the machine. Vehicle may be able to avoid the loader.

6. Articulated Wheeled Loaders < 40 km/h. Complete loss of all steering (either steers uncommanded or not at all while propelling). - Operator has braking to stop the machine. - Operator is not warned prior to loss of steering. Bystanders can be beside the machine. Machine is not driven on roads.

7. Moveable elevating work platform (MEWP). Ability to hold the boom in position. The boom is moving slowly downwards.

8. Moveable elevating work platform is equipped with stabilizers to prevent falling of the machine. One stabilizer fails to move correctly.

9. The controls of MEWP are duplicated (up and ground level). Only one control device may be in use and interlocking device is supervising the function. The interlocking device fails to detect the situation and the MEWP can be driven from two positions at a time.

Appendix B: Test cases of robot experiment

The cases were built around a robot cell explained with text and pictures to the persons performing the assessment task.

Explanation of case:

A robot is working inside a fenced cell. New details come into the cell on pallets via a roller conveyor. The roller conveyor has a sensor that identifies pallets and triggers the start of the conveyor whenever a pallet is placed on the conveyor. In the passage into the cell, there is a light curtain with muting function. The robot processes the details and puts them on a new pallet when they are finished. When a pallet is full of finished details it is transported on the chain conveyor to the finished product pick-up spot.

The passage of new products into the cell is protected with a light curtain with muting (see risk analysis and picture to the right). The pick-up place at the end of the chain conveyor is protected with sliding, interlocking doors outside of a mechanical protection tunnel. When the doors are open, the cell is shut down with auto stop.

The side of the cell where the chain conveyor is located is in a passage where many people pass, including visitors and workers. The side where the Electrical cabinet is placed is situated next to a wall so that the only expected entrance in the area is from service people or persons with mandate and knowledge to change parameters of the system.

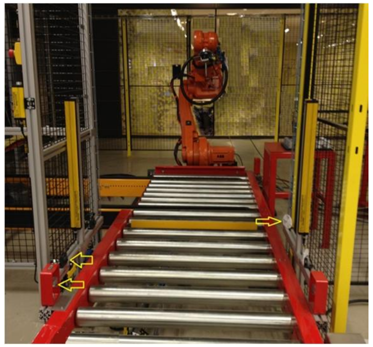


Figure 27. A photo describing the robot cell.

A regular check of one detail is part of the normal process. Daily the operator enters the cell to make an ocular check of a detail being presented in the robot grip. Entrance is made through the inspection entrance where Safemove SW is sustaining safe circumstances. More information about how the SW works can be found at: Safemove website.

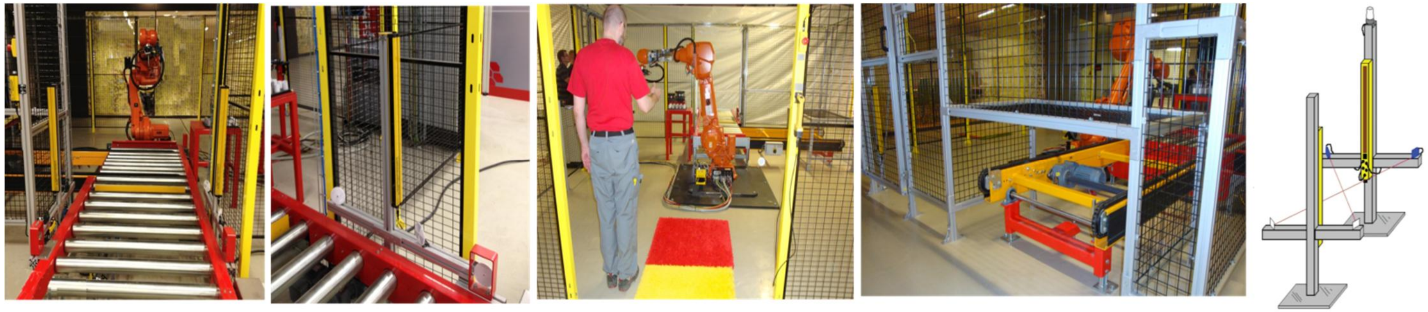


Figure 28. Photos that describe the robot experiment.

Table 34. Test cases of the robot case.

No.	Hazard	Hazard-ous event	Harm	Foreseeable sequence of events	Hazardous situation (when)	Explanation/Comment	Safety function
1	Moving elements	Robot or machine moves in unpredictable way or speed.	impact/ punch/ crushing	Unintentional impact on operating devices. Workers unintentionally impact operating device, e.g. changing speed or range of robot or starting chain conveyor.	The system stands near a passage/ entrance in a factory. Many people pass by. Both visitors and different workers.		The operating devices are placed on electronics enclosure cabinet or manoeuvring platform outside of protecting fence. The risk of impact is considered to be low. (No safety function)

No.	Hazard	Hazardous event	Harm	Foreseeable sequence of events	Hazardous situation (when)	Explanation/Comment	Safety function
2	Moving elements	Unexpected restart of system	impact/ punch/ crushing	Power loss of the system. Operator steps inside cell to check function of part of system when the power suddenly comes back.	Special random (unplanned) occasions.		"Zero voltage stop" is used in cell so that if the cell gets a power loss (or power supply is to weak acc. to a specified limit) the system is shut down and has to be reset with the reset button before restart is possible.
3	Moving elements	Unintentional restart of machines/ robot	impact/ punch/ crushing. Person gets trapped.	An open door is closed from the outside and the cell is started when a service technician is working under one of the conveyors, where he is not immediately spotted.	Service / repair of system	There are instructions that persons entering the cell for installation, service etc. are to place a padlock on the handle of the door through which they entered so that closing and interlocking of that door is not possible.	Doors (also sliding door at chain conveyor) are designed as interlocking protections. Start/ restart is only possible when doors are closed and interlocked.

4	Moving elements / Emergency stop	Unexpected restart of system	impact/ punch/ crushing of person. Damage of property.	The system is not checked before restarting system after an emergency stop. Sensors or operator trigger a new start of system or part of system while person or details in wrong position/ inside of cell, possibly in the way of machines/ moving parts.	Emergency situation	An emergency stop triggers an instant stop (category 1 or 0). This does not allow machines or details/ products in work to be placed in a position for start of process. To remain safe that no person or goods gets stuck or punched / crushed, a rigorous check of the cell has to be performed and thereafter, a reset has to be pressed before being able to restart system. -There are instructions to always check goods, machines and to make sure no one is inside of cell before pressing reset. (When resetting cell all emergency areas are relatively easy spotted).	Reset button has to be pressed before a restart is possible.

5	Falling objects.	Product falls from robot grip and hits operator.	Impact (from falling object). Object weighs about 2kg.	Robot holds detail in a position that forces operator to walk or stand under detail and risk that the object falls on operator.	Interactive daily detail check human/ robot. (Ocular visitation of product.)	Operator performs a regular visual check of detail. This is performed by operator entering cage and checking a detail that the robot presents in its grip. -There are instructions that operator shall never walk or work under robot arm or grip. (The robot movement is limited via safe move SW which can limit the robot movement to avoid or limit positions that forces this passage).	There is an access button that shall be pressed before entering the risk area. When activated, the robot brings the next finished detail to an "inspection position" where it presents the product in its grip for the operator to check it. When button is activated it shines with an intermittent light and when robot is in inspection position it shines with a constant light.

6	Machinery mobility / moving parts	Robot movement.	impact/ punch/ crushing/ fall	Robot and operator interaction. Robot moves and hits operator or makes him step back and fall to avoid being hit.	Interactive daily detail check human/ robot. (Ocular visitation of product.)	Safe move can also be provided with a mat sensing and triggering the safety zones instead of the scanner. Slow speed and limited moving area for robot are possible with safe move software.	Safe move software (from ABB) is installed for robot. There is a scanner that activates the safety in 4 safety zones where the safety is activated in the following steps: slowing down robot movement, confirming and keeping reduced speed, stopping the robot (safely) and confirming and sustaining stop state. If operator enters too fast the robot comes to an immediate stop with a reset demand.
7	Machinery mobility / moving parts	Incorrect entrance of person.	impact/ punch/ crushing	Person enters the cell or the risk area in an incorrect way (not via the entrance button and / or the door).	Installation and random unintended entrance.		Interlockable sliding doors (see above) to protect tunnel to chain conveyor.
8	Moving parts (Chain conveyor).	Incorrect entrance of person when machinery moves.	impact/ punch/ crushing	Operator enters via the opening for the chain conveyor or reaches in to transmission.	When fetching finished parts pallet.		Tunnel is built around conveyor so that trespassing is not easy (according to prescriptions in SS-EN 619) and operator cannot reach dangerous moving parts. - Transmissions of conveyors are encapsulated. (No safety function).

9	Moving parts (Roller conveyor and robot)	Operator falls into risk area.	impact/ punch/ crushing	Operator falls over roller conveyor into robot / risk area.	Mainly when loading new pallet of products to be processed.	The roller conveyor is protected with a light curtain with muting. The muting is of basic type showing in the picture below. The first sensor detects the pallet with new products and starts the conveyor. The two cross-beams are to be affected at the same time to mute curtain. A pallet has the right width for the conveyor and affects both beams simultaneously. A person falling onto the conveyor will either break only one beam or affect the light curtain first.	Access via roller conveyor is protected by a light curtain with muting for product pallets (see comment). If person reaches in or falls over conveyor the light curtain will trigger an auto stop.

Series title and number

VTT Technology 241

Title	**From risks to requirements** Comparing the assignment of functional safety requirements
Author(s)	Timo Malm, Outi Venho-Ahonen, Marita Hietikko, Tor Stålhane, Charlotte de Bésche & Johan Hedberg
Abstract	Risks are categorized, e.g. to prioritize them and to select safety systems and devices with adequate safety properties. A functional safety level that is too high causes exaggerated costs, since more components and validation resources are required to reach a higher level of safety. A functional safety level that is too low leads to inadequate safety requirements and an increase in the risk of accidents. A questionnaire was conducted of the machinery sector to find out which methods were applied in risk assessment and about the functional safety SIL/PL assignment process in the machinery sector. The ISO 13849-1 method is the most common, but the IEC 62061 method is also applied. A round robin test was conducted to compare and check how well the methods matched each other. The assessors estimated the parameters of the risks and assigned the required SIL (Safety Integrity Level) and PL (Performance Level). Nine cases related to mobile work machines and nine cases to industrial robots were used in the experiment. There were 19 assessors in the mobile work machine experiment and 17 in the robot experiment. For each mobile work machine case there was also a standard example that resembled the test case, making it possible to compare the results with the standards. The study shows that in most cases the results correspond to each other, though there are some exceptions. The IEC 62061 method rarely results in SIL 1 but instead in SIL 0 or SIL 2. The IEC 62061 and ISO 13849-1 methods both result in at least a moderate risk level if the severity parameter is high, whereas some other standards (related to the vehicles) clearly drop the risk level if the probability parameter is low or the controllability good. The next ISO 13849-1 (2016), will have also probability parameter, which enables in this case low risk level. An Excel tool was presented to fine-tune the risk levels by applying the risk matrix. The aim was to calibrate the risk levels to match the case better without changing the parameters. Thus, the new risk levels were presented immediately according to the defined risk matrix.
ISBN, ISSN, URN	ISBN 978-951-38-8384-3 (URL: http://www.vttresearch.com/impact/publications) ISSN-L 2242-1211 ISSN 2242-122X (Online) http://urn.fi/URN:ISBN:978-951-38-8384-3
Date	December 2015
Language	English, Finnish abstract
Pages	58 p. + app. 9 p.
Name of the project	Compsoft - Comparing best practices of safety related control system development
Commissioned by	
Keywords	Functional safety, risk assessment, safety requirements, machinery
Publisher	VTT Technical Research Centre of Finland Ltd P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111

Julkaisun sarja ja numero

VTT Technology 241

Nimeke	**Riskeistä vaatimuksiin** Toiminnallisen turvallisuuden vaatimustasojen vertailu
Tekijä(t)	Timo Malm, Outi Venho-Ahonen, Marita Hietikko, Tor Stålhane, Charlotte de Bésche & Johan Hedberg
Tiivistelmä	Riskien luokittelua käytetään mm. kohteiden priorisointiin ja turvalaitteiden tason valintaan. Väärä luokittelu voi johtaa liian alhaisiin turvallisuusvaatimuksiin ja edelleen vaaratilanteisiin. Liian korkeat turvallisuusvaatimukset johtavat puolestaan liian kalliisiin järjestelmiin. Hankkeessa tehtiin kysely, jossa selvitettiin, kuka tai mikä toteuttaa riskin arvioinnin ja toiminnalliseen turvallisuuteen liittyvän luokittelun ja miten. Todettiin, että SFS-EN ISO 13849-1 -standardissa esitelty menetelmä on yleisin ja SFS EN 62061 -standardin menetelmääkin käytetään laajalti. Ensin mainitussa määritetään PL (Performance Level = turvallisuuden suoritustaso) ja jälkimmäisessä SIL (Safety Integrity Level = turvallisuuden eheystaso). Nämä kaksi menetelmää valittiin tarkempaan tarkasteluun. Tavoitteena oli selvittää, kuinka hyvin menetelmät vastaavat toisiaan ja miten analysoijat valitsevat parametrit. Tehdyssä round robin -testissä analysoijat arvioivat kunkin kohteen riskiä valitsemalla siihen parhaiten sopivat parametrit kummallakin menetelmällä. Yhdeksän riskiä liittyi erilaisiin liikkuviin työkoneisiin ja yhdeksän robottisoluun. Työkonetestiin saatiin 19 vastausta ja robottitestiin 17 vastausta. Liikkuviin työkoneisiin liittyvät testitapaukset oli valittu siten, että standardeista löytyi tapauksiin esikuva, johon oli mahdollista verrata vastauksia. Round robin -testi osoitti, että enimmäkseen menetelmät antavat samankaltaisia tuloksia, mutta SFS EN 62061 -menetelmällä saadaan selvästi harvemmin tulokseksi SIL 1 ja vastaavasti useammin SIL 0 tai SIL 2. Toinen havainto oli se, että molempien standardien menetelmissä päädytään vähintään kohtalaiseen riskiin, jos vakavuusparametri on korkea. Monissa muissa toiminnallisen turvallisuuden standardeissa (liittyen esim. ajoneuvoihin ja maatalouskoneisiin) riski voi olla pieni, jos todennäköisyys on pieni tai ajoneuvon hallittavuus on hyvä. Hankkeessa tehtiin myös Excel-työkalu, jolla voidaan taulukkoa muuntamalla hienosäätää kohteiden riskitasoa muuttamatta parametreja.
ISBN, ISSN, URN	ISBN 978-951-38-8384-3 (URL: http://www.vtt.fi/julkaisut) ISSN-L 2242-1211 ISSN 2242-122X (Verkkojulkaisu) http://urn.fi/URN:ISBN:978-951-38-8384-3
Julkaisuaika	Joulukuu 2015
Kieli	Englanti, suomenkielinen tiivistelmä
Sivumäärä	58 s. + liitt. 9 s.
Projektin nimi	Compsoft - Comparing best practices of safety related control system development
Rahoittajat	
Avainsanat	Functional safety, risk assessment, safety requirements, machinery
Julkaisija	Teknologian tutkimuskeskus VTT Oy PL 1000, 02044 VTT, puh. 020 722 111

VTT TECHNOLOGY 241 From risks to requirements

From risks to requirements

Comparing the assignment of functional safety requirements

This report compares how functional safety requirements are defined by applying risk assessment according to the ISO 13849-1 and IEC 62061 standards. A round robin test was applied for the comparison. The test included two experiments: one for mobile work machines and one for a robot cell. Both included nine cases, and a total of 299 risk estimations applied both methods. It was possible to obtain statistics on how the analysts estimated the risks and if there were differences between the methods. It is arguable whether the methods gave the right results – at a minimum, a calibration of the method is required to match the risk level of a specific industrial sector. A demonstration tool was made to check how the calibration could be done without changing the parameters by applying a risk matrix.

ISBN 978-951-38-8384-3 (URL: http://www.vttresearch.com/impact/publications)
ISSN-L 2242-1211
ISSN 2242-122X (Online)
http://urn.fi/URN:ISBN:978-951-38-8384-3