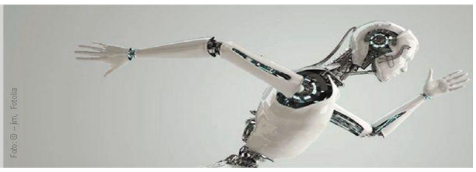
SIAS 2015
8th INTERNATIONAL CONFERENCE ON THE SAFETY OF INDUSTRIAL AUTOMATED SYSTEMS



From risks to requirements – a round robin test

Timo Malm[1], Tor Stålhane[2], Charlotte de Bésche[3], Outi Venho-Ahonen[1] & Marita Hietikko[4]

[1]VTT Technical Research Centre of Finland Ltd, Tampere, Finland
{timo.malm, outi.venho-ahonen}@vtt.fi
[2]Norwegian University of Science and Technology, Trondheim, Norway
stalhane@idi.ntnu.no
[3]SP Technical Research Institute of Sweden, Borås, Sweden
{charlotte.debesche}@sp.se
[4]VTT Expert Services Ltd, Tampere, Finland
{marita.hietikko}@vtt.fi

Abstract

It is important to define the correct required safety level for safety-related control systems. A too high level causes exaggerated costs, since more components and validation resources are required to reach a higher level of safety. On the other hand, a too low level causes too low safety requirements and the risk for an accident will thus increase. The most important methods to assess risks and define corresponding requirements for control systems in the machinery sector are the ISO 13849-1 [5] and IEC 62061 [6] methods. We have run a round robin test to study how safety assessors estimate the parameters of risks and find the required SIL (Safety Integrity Level) and PL (Performance Level). The goal is to compare the properties of the methods. ISO 13849-1 has fewer parameters and the scale is simple (1 or 2), but the result has six levels, including a zero level. IEC 62061 has more dynamics in its parameters, but the result has only four levels, including a zero level.

We used nine cases related to mobile work machines and seven cases related to industrial robots. So far we have had 19 answers to the mobile work machine experiment and 17 answers to the robot experiment. For each mobile work machine case there was also a standard example, which resembled our case and it was therefore possible to compare the results to the result given by the standards. This paper will present the results of the experiment and discuss the reasons for the observed outcome and what should be done to obtain a more correct and uniform safety assessment.

Keywords:

risk assessment, safety, machinery, 13849-1, 62061

Introduction

It has been observed that 40 % of the faults contributing to programmable electronic systems related incidents emerge during the safety requirements specification phase of a system life cycle [1]. In addition, an average of 30 % of the software related defects are made in the requirements specification phase. The share is, however, much higher (60%) for excellent (almost fault free) software [4]. The major part of defects origin at the early life cycle phases of programmable electronic systems. Therefore, it is important to focus on the early life cycle phases of systems: safety requirements specification and risk assessment.

In the CompSoft project engineers and other specialists were asked in an online enquiry, which methods are applied in the machinery sector for risk assessment. A total of 72 answers were gathered from Finland, Sweden and Norway. According to the answers almost 70% applied ISO 13849-1, over 40% applied ISO 12100, over 30% applied IEC 61508 and less than 30% applied the IEC 62061 method in risk analysis – it was possible to choose more than one alternative. This means that the methods applied (ISO 13849-1 and IEC 62061) are quite relevant when considering the risk levels and corresponding control system requirements (Safety Integrity Level=SIL or Performance Level=PL).

When analysts perform risk assessment they get different results depending on their background. Risk assessment should result in specific PL or SIL demands in order to set requirements for the control systems. Too strict requirements lead to expensive systems and too low requirements cause systems to be unsafe.

In round robin tests the test persons analyse identical cases. In our case two methods are applied for each case. The applied methods result in SIL (IEC 62061) and PL (ISO 13849-1) requirement levels for the safety function of a control system. In most cases the safety function is supposed to be obvious, but it was possible to leave the question empty, if the question or safety function remains unclear.

The general objective of the project is to support risk assessment and safety requirements specification phases of safety related control system design by combining well-tried methods, techniques and principles. The aim is to apply the IEC 62061 (annex A) and ISO 13849-1 (annex A) standards, and to find ideas for how to improve or integrate them to support the design process better. This paper shows the results of the round robin test and some ideas for future development.

Parameters of risk

Risk assessment can be done for several purposes, such as defining hazards and their consequences, comparing risks and defining significant risks and related requirements. The purpose of the risk assessment here is to define risks and corresponding requirements. When the hazard is found and the relating significant risks are identified, we must also define requirements that can be used to minimize the risk.

The two standards used in the experiment are both based on the idea that the assessor shall assign values to parameters through a qualitative scheme – e.g. according to ISO 13849-1 “Possible to avoid” gives Av = 2. The EN 62061 standard [6] has four parameters – see Table 1and Table 2, while ISO 13849-1 standard [5] only has three parameters – see Figure 1.

Table 1. The SIL requirement parameters according to IEC 62061

Frequency and duration Fr		Probability of hzd. event, Pr		Avoidance Av	
<= 1 hour	5	Very high	5		
>1hour - <= day	5	Likely	4		
>1 day - <= 2 weeks	4	Possible	3	Impossible	5
>2 weeks - <= 1 year	3	Rarely	2	Possible	3
>1 year	2	Negligible	1	Likely	1

Table 2. The SIL requirement estimation according to IEC 62061.

Consequences	Severity Se	Class Cl = Fr + Pr + Av				
		3 – 4	5 – 7	8 - 10	11 - 13	14 - 15
Death, losing an eye or an arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3
Reversible, medical attention	2			OM	SIL 1	SIL 2
Reversible, first aid	1				OM	SIL 1

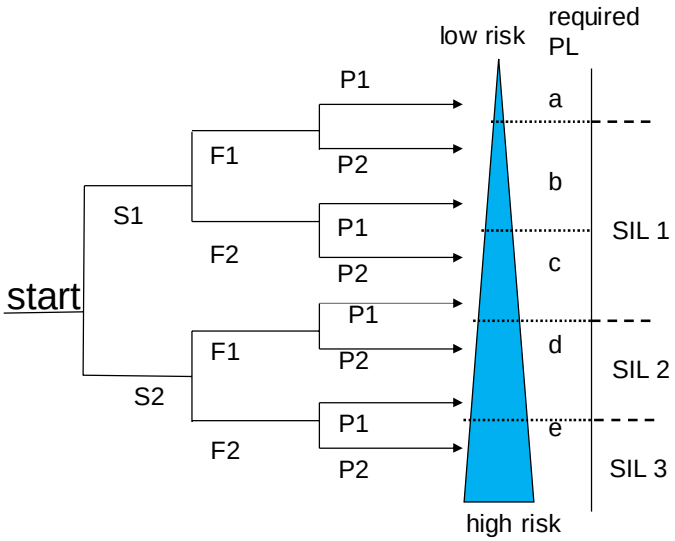


Figure 1. ISO 13849-1 decision tree for risk assessment.

ISO 13849-1 uses a decision tree to assign a risk to a system. The model uses three factors: S (severity) with the values S1 – slight injury and S2 – irreversible injury, F (occurrence frequency) with the values F1 – seldom and F2 – frequent or continuous and P (possibility to avoid the consequences) with the values P1 – possible to avoid under specific conditions and P2 scarcely possible. The decision tree is shown in Figure 1.

When we want to compare these two models for risk assessment, there are some problems that need to be addressed.

- The ISO 13849-1 has two alternatives for each of the parameters severity, frequency, exposure and avoidance, while EN 62061 has four alternatives for severity, five values for frequency and exposure and three alternatives for avoidance. In addition, EN 62061 has an extra parameter – the probability of the hazardous event.
- The ISO 13849-1 has five risk levels – a to e – of which four are mapped onto three SIL levels and "PL a" corresponds to SIL 0. As a consequence of this, both “PL b” and “PL c” are mapped onto SIL 1.
- The ISO 13849-1 uses a conditional probability Pr to assess P(danger | event). Considering that most people, including safety assessment experts, have problems assessing probabilities, a conditional probability might be beyond their capability. See for instance [7].

Round robin tests

The mobile work machine experiment and the robot experiment are realized by applying a round robin test. The purpose is to compare the two risk assessment methods, which are used to give us the requirements for the safety functions. Our aim is to evaluate how objective the methods are and discover if there is a difference between the methods. All the parameters gathered in the assessment are also evaluated in order to see how the parameters affect the results.

The methods used in the risk estimation are based on the SIL assignment process presented in EN 62061 and the risk graph for determining required PL_r for safety function presented in ISO 13849-1. In all cases the risk

analysis text was prefilled and only the parameters should be filled in. All the test persons conducted the risk assessment for nine cases (either robot or mobile machine cases) and both used both the IEC 62061 and the ISO 13849-1 method. Background information of the persons or groups that analysed the cases was also collected.

When calculating average values in the round robin tests, the PLs are converted to SILs according to the following formula, using linear interpolation between the fixed numbers/letters (see Figure 4 and Figure 5):

PL a→0.5; PLb→1; PL c→1.3; PL d→2; PL e→3 (1)

Both SILs and PLs use a logarithmic scale and therefore comparison between them can be applied in corresponding parts of the scales for average calculations. All the other transformations are according to ISO 13849-1 probabilities, but “PL a” has no equivalence to SIL and is set to the middle value between SIL 0 (almost no risk) and SIL 1, which gives us a rough estimation and keeps the numbers easier to apply. SIL 0 is not described in the standards, but we assume that the distance from SIL 0 to SIL 1 is the same as from SIL 1 to SIL 2. This definition is more like risk and severity perspective than probability perspective since the probability of SIL 0 is not defined.

Mobile machine experiment

There are nine mobile machine cases related to tractor loaders, articulated wheeled loaders (loaders with a pivot joint, which allows the vehicle to “bend” or pivot on that joint), steel tracked dozer and movable elevating work platforms. The cases were selected from ISO/TS 15998-2 [9] and EN 280 [8] in order to enable us to compare our results to the standard’s results. The case descriptions are short since the texts were from the standards, which aim to have relatively wide scope. The applied examples are not in the normative part of the standards. All case descriptions gave hints to aid the analyst in choosing severity, frequency, exposure and possibility to avoid hazard, which are related to the parameters of risk. The analyst needed to estimate the required parameters for each case and the template (Excel) calculated the corresponding risk level (SIL and PL). The nine cases were chosen so that the cases cover both high and low risk examples. According to the corresponding machine standards (ISO/TS 15998-2 and EN 280), performance levels (PL) 0, a, b, c, d and e were included. The analysis was typically made in about 40 minutes, which indicates that the information for each case is quickly understood and analysed.

An example of the figure and case description is shown in figure 2.

Figure 2: Figure for case 1

Case: Tractor Loader- Backhoe Traveling <40 km/h Unexpected brake apply. Machine stops very abruptly, and may skid. Steering remains functional, but is limited. Bystander may be crushed between machine and hard surface. Bystander may be run over.

Robot experiment

The robot experiment resembled the work machine experiment in its setup, but with the difference that the nine hazards were all collected from the same robot cell. The cases are unfortunately not found in any standard, but they are possible real life cases. The robot test was sent to persons from institutes working with risk assessment and persons from the industry.

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

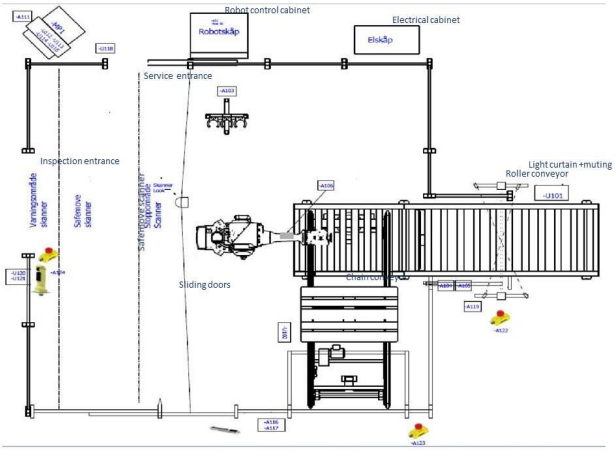


Figure 3: Robot case diagram

The robot cases have a more detailed description than the machinery cases as shown in the example below:

- **Hazard:** Moving elements
- **Hazardous event:** Robot or machine moves in unpredictable way or speed.
- **Harm:** impact/ punch/ crushing
- **Foreseeable sequence of events:** Unintentional impact on operating devices. Workers unintentionally impact operating device, e.g., changing speed or range of robot or starting chain conveyor.

- **Hazardous situation (when):** The system stands near a passage/entrance in a factory. Many people pass by. Both visitors and different workers.

Results of the experiments

The results of the mobile work machine experiment and robot experiment are first considered separately and then common features are discussed in the summary part of the section.

Mobile machine experiment results

Table 3 and Table 4 show how the test persons have answered the mobile work machine cases. On the left hand side of the tables we show the PL/SIL levels and at the bottom is the case number and above this, the answer suggested by a standard. The bold numbers (value can be seen also at the std. row) indicate the risk levels suggested by the standard. We see that there is some variation in all the nine cases although the average is usually the most common answer. This is true both for SILs and PLs. The SIL estimation concentrates on SIL 2 although according to the suggestions in the standards the results were more spread. There is slightly more variation regarding PLs than SILs.

Table 3. The number of answers to the mobile work machine cases according to the ISO 13849 method.

PL									
e	0	0	1	0	2	1	2	6	3
d	9	6	4	12	9	10	2	5	2
c	8	12	11	4	7	7	2	5	7
b	1	0	1	2	1	0	4	1	1
a	0	1	2	1	0	1	7	1	5
0	1	0	0	0	0	0	1	1	0
std	-	c	b	c	e	d	c	d	c
Case	1	2	3	4	5	6	7	8	9

Table 4. The number of answers to the mobile work machine cases according to the IEC 62061 method.

SIL									
3	1	1	1	3	2	3	1	9	3
2	15	14	10	11	15	12	2	4	4
1	1	0	2	3	2	2	3	3	3
0	2	4	6	2	0	2	12	3	8
std	-	c	b	c	e	d	c	d	c
Case	1	2	3	4	5	6	7	8	9

Figure 4 shows PL values converted to SIL values according to formula (1). In most cases the analysts arrived at roughly the same results as the standards, but in cases 1 and 5 the results were different. In case 1, the standard estimates that the risk is low (SIL 0), whereas the mean value of analysts is about 1.5. In this case the driver may hit his head to the windshield at low speed or drive over a bystander because of braking. The standard assumes that heavy braking is possible in a case of failure and no means, e.g., ABS, are required to decrease braking. In case 5, the standard risk/requirement is SIL 3, whereas the average is less that SIL 2. In this case steering is lost while the machine may be in traffic. The traffic possibility is, however, not specifically mentioned in the text. When a machine may be driven in traffic the risk is estimated to be high. In both of these cases additional knowledge about the risk levels and more time for the analysis could have resulted in answers which are closer to the standards.

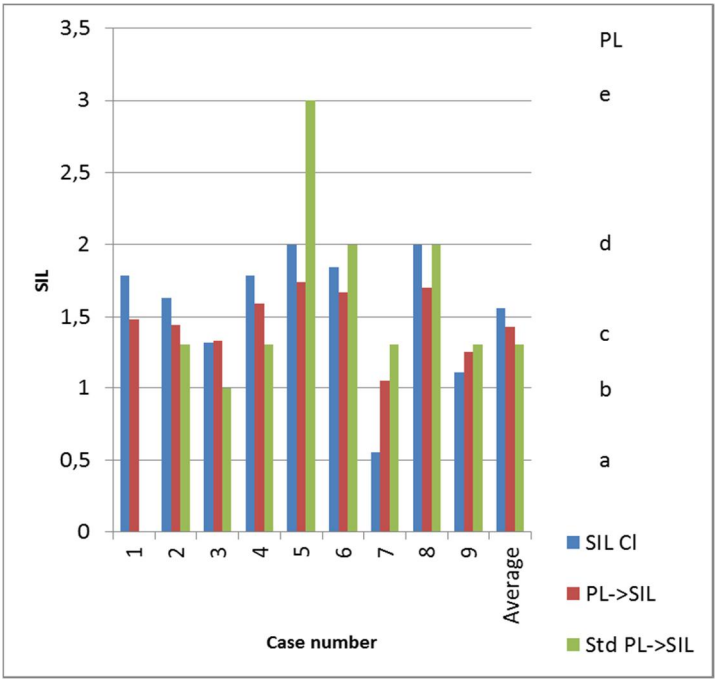


Figure 4. The average value and standard suggestion for each mobile machine case.

Robot experiment results

Table 5 and Table 6 show the answers of the robot experiment. In the tables the “correct answer” according to the expert group, are in bold and can be seen also at the std. row. For case 1 and 8 there is no right answer since no safety functions are needed. The graphs look similar, as should be expected.

Table 5. The number of answers of the nine robot cases according to the ISO 13849 method.

PL									
e	1	1	1	0	2	5	0	0	3
d	3	12	7	9	3	5	10	4	8
c	2	4	9	6	3	3	7	1	5
b	0	0	0	0	6	3	0	1	0
a	1	0	0	0	3	1	0	0	1
0	0	0	0	0	0	0	0	0	0
std		c	a	c	e	d	c		d
Case	1	2	3	4	5	6	7	8	9

Table 6. The number of answers of the nine robot cases according to the IEC 62061 method.

SIL									
3	1	2	1	1	1	8	2	0	2
2	2	14	12	12	5	3	13	2	11
1	1	1	2	0	5	3	2	4	2
0	3	0	2	2	6	3	0	0	2
std		2	1	2	2	2	2		2
Case	1	2	3	4	5	6	7	8	9

Figure 5 shows the average answers to each case.

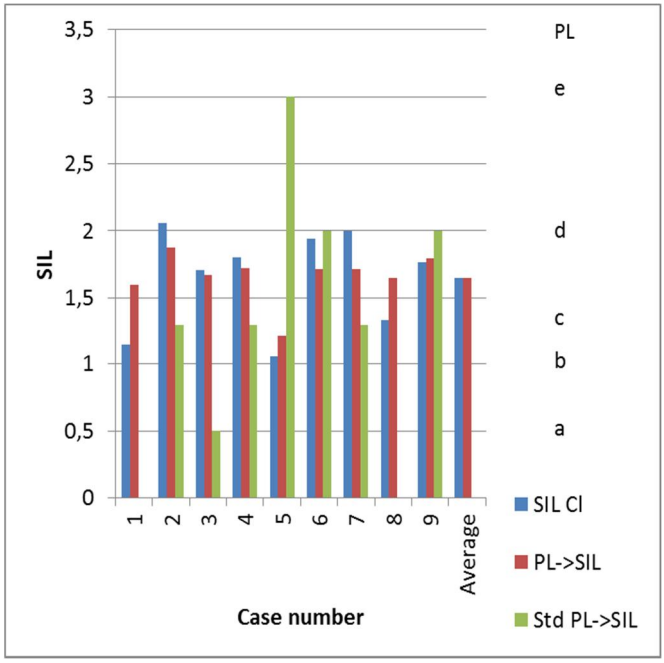


Figure 5. Average values for each nine robot cases and the expert judgement.

In general, it is more common to assess the risk to a value higher than, or equal to the recommended value than that it is assessed to a lower value.

Case 5 was generally assessed to a much lower level than the expert judgement. In this case a product was dropped by the robot and an access button was the safety means. The difference between the assessors' and the expert judgement was probably due to too little information about the system and the case.

Case 3 was generally assessed to be at a higher risk level than the expert assessment (c instead of a). The case was about unintentional start-up and interlocking doors were the safety means. According to the case description there are instructions for service technician to always use a padlock on the door before going into the cell to make sure the door cannot be closed and interlocked. The mitigation by instructions for padlock shall be calculated into the assessment according to IEC 62061, but people seem to have missed this information.

Summary of the experiments

Table 7 shows a cross-tabulation of the SIL and PL answers from both the mobile work machine and the robot cases. Each cell shows how many times the analysts choose specific PL (ISO 13849 method) and for the same case corresponding SIL (IEC 62061 method). The cells with text in bold indicate the equivalence between SILs and PLs, i.e. if all numbers were in these cells all test persons would have arrived at the same risk levels with both methods. However, we see that the bottom left corner has more values (97) than the top right corner (50). This indicates that the test persons have assessed the risks to be higher when applying the IEC 62061 standard than when using the ISO 13849 standard. The difference is clear when the risk is at the intermittent level – close to PL c. For example: in 62 out of 93 cases the test persons estimated the risk level to be SIL 2 when in the same cases the PL assessment was PL c. The calculated average value for the robot experiment of the methods was about the same (see Figure 5, the average column), but at the mobile machine experiment the IEC 62061 standard gave slightly higher values (see Figure 4). The total average SIL when applying the IEC 62061standard is 1.6, and applying the ISO 13849 standard is 1.3 (transformation according to formula (1)).

Table 7. Cross-tabulation of all mobile machine and robot cases.

SIL \ PL	0	a	b	c	d	e
0	3	21	10	16	5	2
1	0	3	8	18	9	1
2	0	0	2	68	84	7
3	0	0	1	1	22	18

Table 7 shows also that SIL 0 is chosen much more often than PL 0 – 57 vs. 3 times. PL a corresponds to SIL 0, but yet there is disproportion between PL 0/PL a and SIL 0. When studying the answers more closely we see that when applying the IEC 62061 method, the severity factor is often set to "1" or "2" which often results in SIL 0. In addition, SIL 3 is chosen more often (40) than PL e (27).

We registered the expertise of all analysts and in most cases the persons did have several areas of expertise. For the mobile work machine experiment we used the expertise groups risk assessment, automation, machinery, research and work machines. For the robot experiment the expertise groups were electronic components, robots, software, system integrator and distributor/agent. In both cases the amount of test persons in each group was relatively small and there was also overlap between the groups.

The differences between the expertise groups were relatively small. In mobile work machine experiment the lowest risk levels were given by the work machine experts i.e. the persons who know best the work machines. The average value for work machine experts was SIL 1.37 and the total average was SIL 1.64 according to IEC 62061 method calculations. In the robot experiment the robot specialist evaluated the risks to be at a slightly higher level than the other participants. The value was SIL 1.78 and the average was SIL 1.67. Based on the data available, we cannot say that the experts who know the specific technology give lower or higher risk level answers than other technology experts.

Discussion

The round robin test included nine cases related to mobile work machines and nine cases related to a robot cell. In all cases two methods were applied to assess the risk level. The test persons (analysts) did not use a lot of time for each case and usually they did not have additional material like standards to support their decisions. Therefore, the decisions are mainly based on experience and by using each participant's background knowledge. The information given for each the mobile work machine case was short and focused on the parameters of the risk. For the robot case there was more material and all cases were related to the same robot cell. More information might give more accurate results, but on the other hand the parameter descriptions were given more precisely at the mobile work machine test

It is often claimed that the analysis tool should be calibrated to the relevant branch of technology in order to reach valid results [3]. This refers to the tacit information and culture related to each branch of technology. In our case the analysts were not able to do any comparison with the practise of the relevant branch of technology. This may result in a wider range of answers, but does not matter when we are comparing the standards. When comparing the results of the standard methods the analysts estimated the risk parameters, assuming that the risk is at the same level and yet, by choosing different parameters, the level of the assessed risk may be different.

The two experiments (machinery and robot cell) had quite different case descriptions as shown in the experiment descriptions above. If we use one of the standard readability formulas – in this case Kincaid [11] – we find that the readability index correlates strongly with the number of correctly identified risk levels when using the ISO 13849. The table below shows readability and number of correctly identified risk levels for the machinery.

Table 8. Number of matches between standard answer and analyst answer in mobile machine experiment.

Case	ISO 13849	Kincaid
1	0	12,4
2	12	73,8
3	1	35,6
4	4	51,5
5	2	48,9
6	10	63,9
7	2	50,3
8	5	46,6
9	7	61,9

The correlations are as follows:

Table 9. Correlation of readability and "correct" answers.

Experiment	Correlation	p
Machinery	0.90	0.00
Robot cell	0.69	0.04

It seems safe to assume that the readability of the case description strongly influences the analyst's ability to arrive at the correct risk level when using the ISO 13849 standard. No such relationship was identified for the IEC standard.

When we apply the IEC 62061 method, SIL 1 is a quite rare result compared to the ISO 13849 method. In addition, according to the standards (mobile work machine experiment), the risk should have been assessed to SIL 1 in five out of nine cases, but in none of the cases the SIL 1 got the majority of the results and only in one case was it the average. Figure 6 presents the distribution of all answers which shows the difference between the two methods. This indicates that the IEC 62061 standard tends to give SIL 0 and SIL 2 values more often than SIL 1 values.

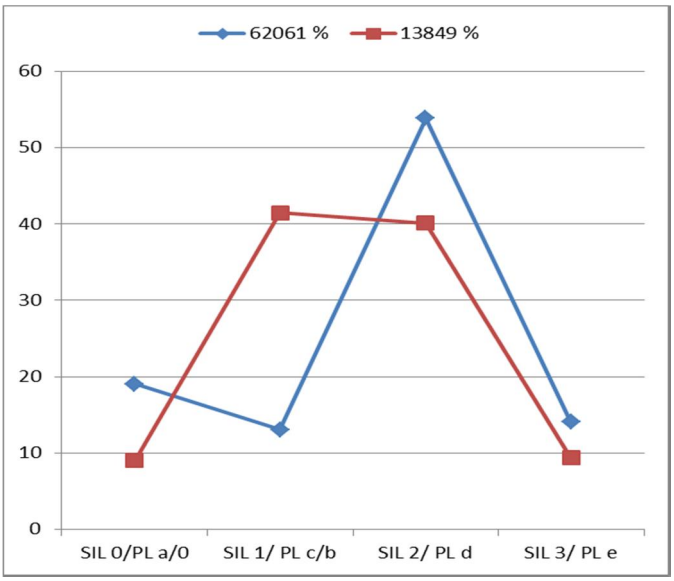


Figure 6. Distribution of answers (%) in mobile machine and robot cases. There were totally 299 answers in the experiments.

In the matrix of the IEC 62061 standard (see Table 2) SIL 1 is available only in three cells of the matrix and it is not available when severity is high (Severity=4). This leads to low number of SIL 1 results in the risk analysis. The ISO 13849 risk graph (see Figure 1) or the matrix (see Table 10) show that half the matrix cells leads to either PL b or PL c, which both are associated to SIL 1. One could claim that in machinery systems there should be more SIL 1 safety functions than SIL 2 safety functions, but the IEC 62061 method does not support this assumption.

Table 10. The ISO 13849 risk graph presented as a matrix form.

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

The number of answers in the mobile machine experiment according to parameters (ISO 13849-1) is presented in Table 11. Severity 0 cases are not included in the table since in those cases the other parameters were not estimated. The table resembles Table 10, but the amounts of answers are included.

Table 11. The amounts of answers in the mobile machine experiment according to severity, frequency and avoidance factors (ISO 13849).

\Avoid	P1		P2	
Sev\Freq	F1	F2	F1	F2
S1	a= 18	b= 6	b=5	c=4
S2	c=59	d=24	d=35	e=15

The amount of answers according to severity and class (Cl) are described at Table 12 (IEC 62061 matrix). The table can be associated with Table 2 and the SIL values are in the corresponding cells. SIL 2 is in **bold**, SIL 1 is in *italic*s. In addition, the SIL requirements are also shown in the cells. Table 12 shows that a large amount of the answers (27) are just below SIL 1 at the "other measures" area (according to IEC 62061; see also Table 2). The class factor (Cl=Fr+Pr+Av) shows that most of the answers are in the middle (8-10). This may be related to the cases, but it is also possible that the analysts tend to avoid extreme values. This is a quite common response, known as the end-aversion bias or the central tendency [12].

Table 12 and Table 11 also show that a large amount of analysts estimated the severity to the highest level. This may be related to the cases or that the analysts tend to find the highest severity possible. When applying the IEC 62061 method this leads to at least SIL 2. In order to have more SIL 1 than SIL 2 values when the severity is 4, the Cl values 3 – 7 should result in SIL 1. If also the "OM" cells (Table 2) corresponds to SIL 1 the result would be closer to the ISO 13849 method result. One point is that in nearly all of the hazardous cases a good analyst can find a scenario in which a person is killed, but the probability can be very low. More precise estimation will be presented at the final report of the project.

Table 12. The amounts of answers in mobile machine experiment according to severity and class ranging (IEC 62061).

	Cl=Fr+Pr+Av				
Severity	3-4	5-7	8-10	11-13	14-15
4	SIL 2: 3	SIL 2: 31	SIL2: 50	SIL3: 23	SIL 3: 1
3	0	20	*SIL 1: 18*	SIL 2: 3	SIL 3: 0
2	0	3	5	*SIL 1: 0*	SIL 2: 0
1	0	4	2	2	*SIL 1: 1*

In the results, the severity parameter is often given the highest value. The question is if the severity level really is high or if the analysts estimate the severity level to be too high. There were different risk levels in the cases, but the severity parameter of the standards were considered only in five mobile machine cases, i.e. the cases picked from the ISO 15998-2 standard [9]. This means that comparison of parameters against the standards is not done for the complete set of the cases.

In most of the cases the answers of the test persons are close to the standards and the average was a little higher than the standard's suggestion. This indicates that the analysis methods tend to result in higher risk levels than the standard suggests. However, it is possible that more available information for the analysts could result in values closer to the standards.

Since the two standards use different number of parameters and different texts for guiding the parameter value selection, we might expect large differences in the parameter value assessments. This is, however, not the case. As the diagrams below (see Figure 7, Figure 8 and Figure 9) show, the parameters in the two standards that are comparable follow the same paths. The diagrams are from the mobile work machine experiment.

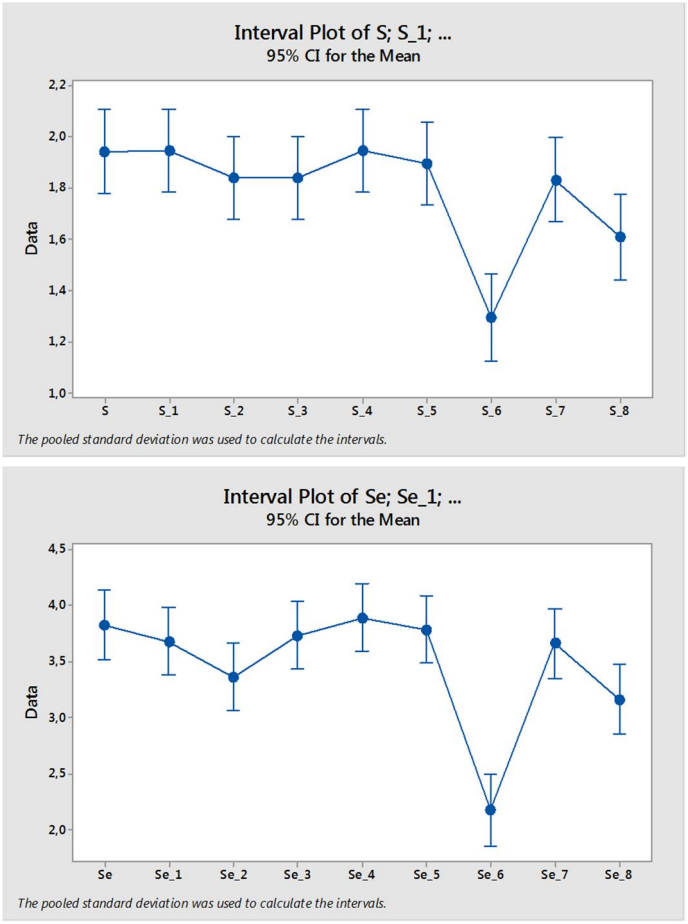


Figure 7. Paths for mean value of severity (S, Se). Above ISO 13849 method and below IEC 62061 method.

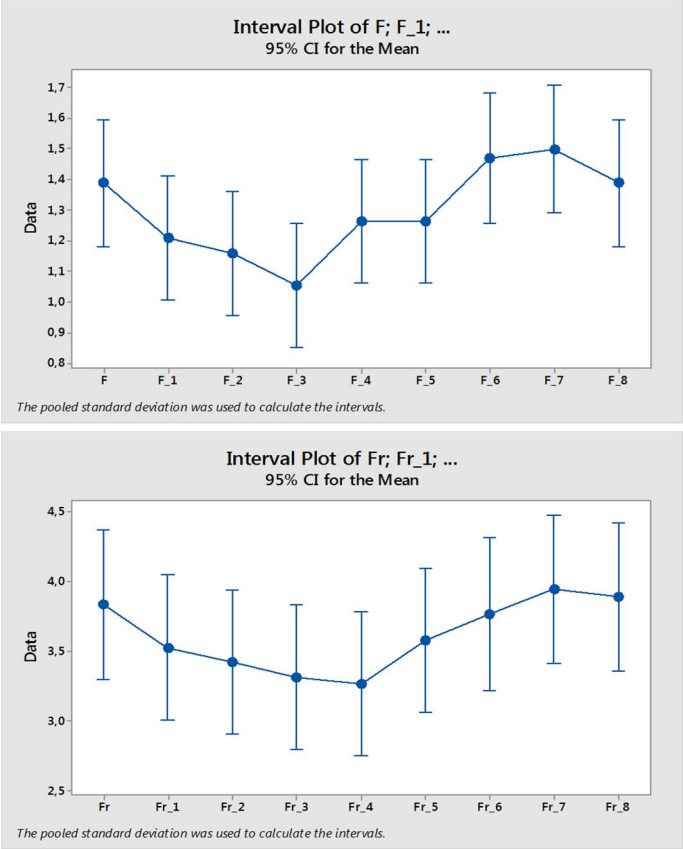


Figure 8. Paths for mean value of frequency (F, Fr). Above ISO 13849 method and below IEC 62061 method.

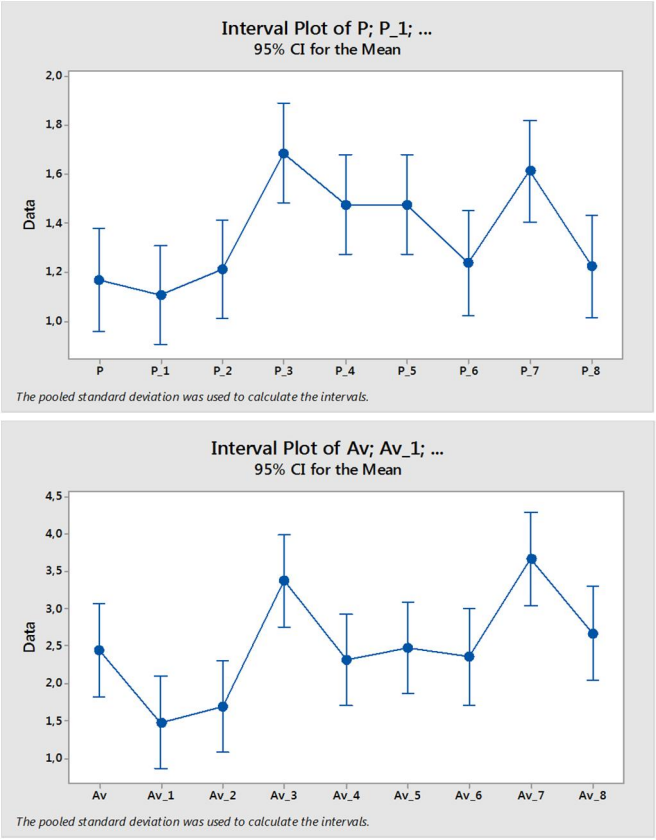


Figure 9. Paths for mean value of probability to avoid hazard (P, Av). Above ISO 13849 method and below IEC 62061 method.

If this is true, the mean values for each parameter should show a high degree of correlation. We computed the Spearman correlation for each comparable parameter pair and got the results shown in Table 13.

The two standards have the following risks assessments formulas:

- ISO 13849-1:
  R = S * P(harmful event) * P(not avoid)
- IEC 62061:
  R = S * P(harmful event) * P(harm | harmful event) * P(not avoid)

The parameter not found in ISO 13849 is the conditional probability P(harm | harmful event) since this standard assumes that a harmful event always will lead to harm. As mentioned earlier, the assessment of conditional probabilities is probably beyond the capability of most assessors.

Since hazard avoidance already is included in the P(not avoid) factor, the P(harm | harmful event) factor is related to near misses, i.e., P(near miss) = 1 – P(harm | harmful event). However, in many branches of industry the registration of near miss events is not complete and consistent and it is unreasonable to assume that assessors have access to this type of information.

Table 13: Standard parameter correlations

Moving machinery		
Parameters	Spearman correlation	Level of significance
S – Se	0.83	0.005
F – Fr	0.82	0.007
P – Av	0.71	0.032
Robot		
Parameters	Spearman correlation	Level of significance
S – Se	0.90	0.001
F – Fr	0.92	0.001
P – Av	0.43	0. 249

Conclusion

It can be seen that the distribution of parameters in both IEC 62061 method and ISO 13449 method give relatively similar results for each case. This is as expected since the analysts have been analysing the same cases. Yet there is a difference between final PL and SIL results. The IEC 62061 method does not give SIL 1 as often as the ISO 13849 method gives the corresponding result PL b or PL c. Instead, the IEC 62061 method results more often SIL 0 and SIL 2. The cases in the mobile machine experiment were chosen from standards and they indicate that there should have been more SIL 1 results than the IEC 62061 method results show. This means that when applying the IEC 62061 method, the analyst should consider all SIL 0 and SIL 2 results and decide if SIL 1 could be closer to the final result.

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

When using ISO 13849 the readability of the case description is important, while when using IEC 62061, the assessor needs access to near miss information. The work of Hendrickx et al. [10] shows that assessors prefer case description over relative frequency information. If near miss information is not available, the assessors should use ISO 13849 and stay away from IEC 62061.

Acknowledgement

The project was made together with VTT (Finland), NTNU (Norway) and SP (Sweden). The major part of funding in Finland came from the Finnish Work Environment Fund. The rest of the funding for each partner was own funding of all participants. It is also remarkable how many companies from Finland, Norway and Sweden gave their support by answering the questions and making analysis for the test cases.

References

[1] Chambers C, Croll PR, Bowell M. A study of incidents involving programmable electronic safety-related systems. Interacting with computers, vol. 11. Elsevier Science B.V; no. 6, June 1999. p. 597–609.

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

[3] IEC 61508-5. 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 5: Examples of methods for determination of safety integrity levels. 97 p

[4] Jones C. Software quality in 2012: A survey of the state of the art. Namcook Analytics LLC. 2008 (achieved 9.6.2015). 25 p. http://sqgne.org/presentations/2012-13/Jones-Sep-2012.pdf

[5] SFS-EN ISO 13849-1. 2008. Safety of machinery — Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS 180 p.

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

[7] Kahneman, Daniel; Tversky, Amos: On the reality of cognitive illusions. Psychological Review, Vol 103(3), Jul 1996, 582-591

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

[9] ISO/TS 15998-2. 2012. Earth-moving machinery -- Machine control systems (MCS) using electronic components -- Part 2: Use and application of ISO 15998. 58 p.

[10] Hendrickx, L., Vlek, C., and Oppewal, H.:"Relative importance of Scenario Information and frequency Information in the Judgement of Risk". Acta Psychologica, 72 (1984), p 41 – 63

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

[12] Choi, B.C.K. and Pak, A.N.P.: A catalog of Biases in Questionnaires, Public Health Research - Practice and Policy. Vol. 2, no. 1, January 2005.

Corresponding address

Timo Malm

VTT Technical Research Centre of Finland Ltd, Box 1300, FI-33720 Tampere, Finland