Article citation info:
FUCHS P, ZAJICEK J. Safety integrity level (SIL) versus full quantitative risk value. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2013; 15 (2): 99–105.

Pavel FUCHS
Jaroslav ZAJICEK

SAFETY INTEGRITY LEVEL (SIL) VERSUS FULL QUANTITATIVE RISK VALUE

NIENARUSZALNOŚĆ BEZPIECZEŃSTWA A WARTOŚĆ RYZYKA

Safety management of technical equipment is not possible without risk assessment. Therefore, many standards are available for risk assessment, e.g. ISO 13824:2009 General principles on risk assessment of systems involving structures or ISO/IEC 31010:2009 Risk management – Risk Assessment Techniques. In different industrial sectors risk assessment is fundamental step to determine required safety integrity level (SIL), eventually performance level (PL), which guarantees risk linked to some equipment on acceptable level. Standards applied for risk management based on SIL in different industrial sectors differ in methods used for risk evaluation and SIL determination. IEC 61508-5 accepts the use of qualitative, semi-quantitative or quantitative approach for risk evaluation and SIL determination. The standard uses hazardous event severity matrix as an example of qualitative approach for SIL determination, the standard furthermore uses layer of protection analysis (LOPA) as an example of semi-quantitative approach. The standard also uses Risk graph method as an example of both qualitative and semi-quantitative approach. IEC 62061 only presents one semi-quantitative approach for risk evaluation and SIL determination based on combination of probability and severity of consequences. This approach is different from the approach presented in IEC 61508-5. Similarly ISO 13849-1 recommends the use of qualitative method combining probability and severity of consequences for risk evaluation and PL determination, however, distinctly from IEC 61508-5 as well as IEC 62061. All these standards evaluate risk in the first step and in the second step they set safety systems reliability requirements, which should lower risk onto an acceptable level. The elemental question is, how exactly these standards evaluate risk in their methods. Another question is what acceptable level of risk is implicitly hidden in their requirements for choice of SIL and PL. This paper addresses these questions.

***Keywords**: safety, SIL and PL determination, risk evaluation, tolerable level of risk, semiquantitative analysis.*

Zarządzanie bezpieczeństwem urządzeń technicznych nie jest możliwe bez oceny ryzyka. Dlatego też istnieje wiele norm związanych z oceną ryzyka, np. ISO 13824:2009 Ogólne zasady dotyczące oceny ryzyka w systemach obejmujących konstrukcje lub ISO/IEC 31010:2009 Zarządzanie ryzykiem - Techniki oceny ryzyka. W różnych gałęziach przemysłu ocena ryzyka jest podstawowym krokiem na drodze do określenia wymaganego poziomu nienaruszalności bezpieczeństwa (SIL), oraz ewentualnie poziomu wydajności (PL), który gwarantuje, że ryzyko w odniesieniu do niektórych urządzeń pozostanie na akceptowalnym poziomie. Normy stosowane w zakresie zarządzania ryzykiem w oparciu o SIL w różnych gałęziach przemysłu różnią się jeśli chodzi o metody stosowane do oceny ryzyka i określenia SIL. IEC 61508-5 akceptuje zastosowanie jakościowego, pół-ilościowego lub ilościowego podejścia do oceny ryzyka oraz określenia SIL. Norma ta wykorzystuje macierz ciężkości zdarzeń niebezpiecznych jako przykład podejścia jakościowego do określenia SIL; ponadto, norma wykorzystuje analizę warstw zabezpieczeń (LOPA) jako przykład podejścia półilościowego. Norma wykorzystuje również metodę wykresu ryzyka jako przykład podejścia zarówno jakościowego jak i półilościowego. IEC 62061 prezentuje jedno pół-ilościowe podejście do oceny ryzyka i określenia SIL łącząc prawdopodobieństwo i ciężkość następstw. To podejście różni się od metody stosowanej w IEC 61508-5. Podobnie ISO 13849-1 zaleca stosowanie metody jakościowej łączącej prawdopodobieństwo i ciężkość następstw dla oceny ryzyka i określenia PL, jednak w sposób odmienny od IEC 61508-5 oraz IEC 62061. Wszystkie powyższe normy dokonują oceny ryzyka w pierwszym etapie zaś w drugim etapie ustalają one wymagania odnośnie niezawodności systemów bezpieczeństwa, które powinny obniżyć ryzyko do akceptowalnego poziomu. Podstawowym pytaniem jest jak dokładnie powyższe normy dokonują oceny ryzyka przy użyciu swoich metod. Inną kwestią jest to, jaki dopuszczalny poziom ryzyka jest domyślnie ukryty w ramach ich wymagań dotyczących wyboru SIL i PL. Niniejszy artykuł odnosi się do powyższych zagadnień.

***Słowa kluczoewe**: bezpieczeństwo, określenie SIL i PL, ocena ryzyka, dopuszczalny poziom ryzyka.*

1. Introduction

For effective risk management it is necessary to be able to assess the risk accordingly. Risk assessment in technical practice becomes one of the fundamental elements to prove that a piece of equipment is sufficiently safe. This can be furthermore seen in standards in various industrial sectors. These standards require risk assessment for equipment or a device and prove the risk is acceptable. The standards then offer different approach for risk evaluation; qualitative, semi-quantitative and quantitative. These standards do not generally provide specific instructions on how to proceed while assessing risk for individual cases. The standards only provide generic recommendations with respect to variety of unsafe events and their consequences. When standards these generic cases specify more in depth by using examples, they do so in the form of appendices listed as informative, hence non-obligatory.

Fundamental standards of functional safety are IEC 61508-5 [1] and IEC 61511-x [2]. Principles from these two have been adopted in various industrial sectors related to functional safety, i.e. IEC 62061 [3], ISO 13849-1 [4], IEC 61513 [5], EN 50129 [6] and more. These listed standards are the result of historical development of understanding the function of safety systems for reducing the risk resulting from operating technical equipment. When the requirements are laid down in the standards need to be applied to a specific technical solution it is necessary to appropriately understand the essence of risk and its evaluation. Examples of risk evaluation given in standards cannot be then carelessly applied. This could lead to underestimating or overestimating of the risk level and as a result safety management would be ineffective.

This article presents the analysis of simplified approaches to determining safety integrity from three international standards IEC 61508-5, IEC 62061 and ISO 13849-1. The purpose of this article is to point out some common solutions and weaknesses of risk evaluation as well as assessing its acceptability for using these standards.

2. Risk and safety integrity according to specified standards

2.1. Risk and SIL according to IEC 61508-5

IEC 61508-5 Annex E (informative) standard provides a quantitative method to determine SIL titled Risk Graph Method (Fig. 1).

This simplified procedure is based on the following equation

$$R = (f) \text{ of a specified } (C) \qquad (1)$$

and assumptions $C_1 < C_2 < C_3 < C_4$; $F_1 < F_2$; $P_1 < P_2$; $W_1 < W_2 < W_3$.

where

R is the risk with no safety-related systems in place;

f is the frequency of the hazardous event with no safety-related systems in place;

C is the consequence of the hazardous event (the consequences could be related to harm associated with health and safety or harm from environmental damage).

This produces the following four risk parameters:

- consequence of the hazardous event (C);
- frequency of, and exposure time in, the hazardous zone (F);
- possibility of failing to avoid the hazardous event (P);
- probability of the unwanted occurrence (W).

Safety integrity level (SIL) of safety-related system is specified against intolerable risk by the target failure measures presented in Table 1.

Table 1. Safety integrity levels according to IEC 61508-5 – target failure measures for a safety function

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function [1] (PFDavg)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	≥1E-5 to <1E-4	≥1E-9 to <1E-8
3	≥1E-4 to <1E-3	≥1E-8 to <1E-7
2	≥1E-3 to <1E-2	≥1E-7 to <1E-6
1	≥1E-2 to <1E-1	≥1E-6 to <1E-5

2.2. Risk and SIL according to IEC 61508-5

IEC 62061 Annex A (informative) provides a semi-quantitative method for determining SIL. This method is based on risk matrix (Fig. 2) [7].

This simplified procedure is based on the following equation:

$$R = (Cl) \text{ of a specified } (Se) \qquad (2)$$

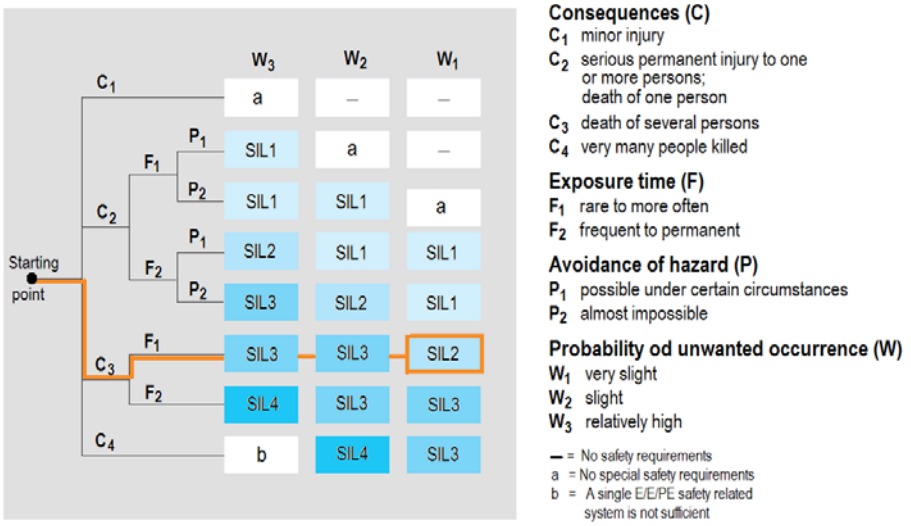

Fig. 1. The risk elements evaluation and SIL requirements determination according to IEC 61508 5

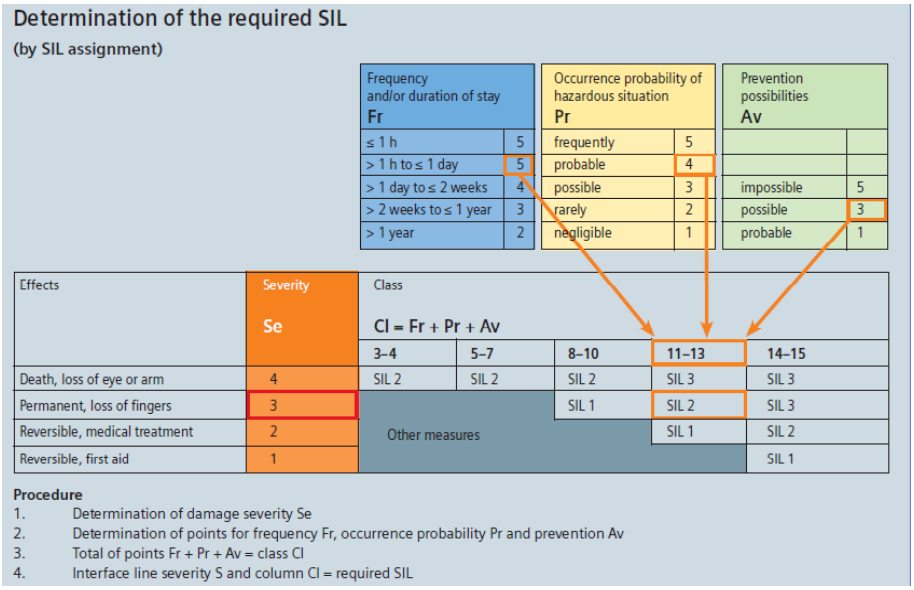

Fig. 2. The risk elements evaluation and SIL requirements determination according to IEC 62061

where
R is the risk with no safety-related systems in place;
Cl is the frequency of the hazardous event with no safety-related systems in place;
Se is the severity of consequence of the hazardous event (the consequences could be related to harm associated with health and safety).

This produces the following four risk parameters:
– consequence of the hazardous event (*Se*);
– frequency and duration of exposure to hazard (*Fr*);
– prevention possibilities (*Av*);
– occurrence probability of the hazard ous situation (*Pr*).

Safety integrity levels (SILs) of safety function according to IEC 62061 are different from SILs according to IEC 61508-5 and its target failure measures are presented in Table 2.

Table 2. Safety integrity levels according to IEC 62061 – target failure measures for a safety function

Safety integrity level (SIL)	Probability of a dangerous failures per hour [h^{-1}]
3	≥1E-8 to <1E-7
2	≥1E-7 to <1E-6
1	≥1E-6 to <1E-5

2.3. Risk and PL according to ISO 13849-1

ISO 13849-1 similarly as IEC 61508-5 in Annex A (informative) uses qualitative method based on risk graph to evaluate safety integrity, see Figure 3 [7]. With the only difference that for safety integrity of safety function the term performance level (PL) is being used.

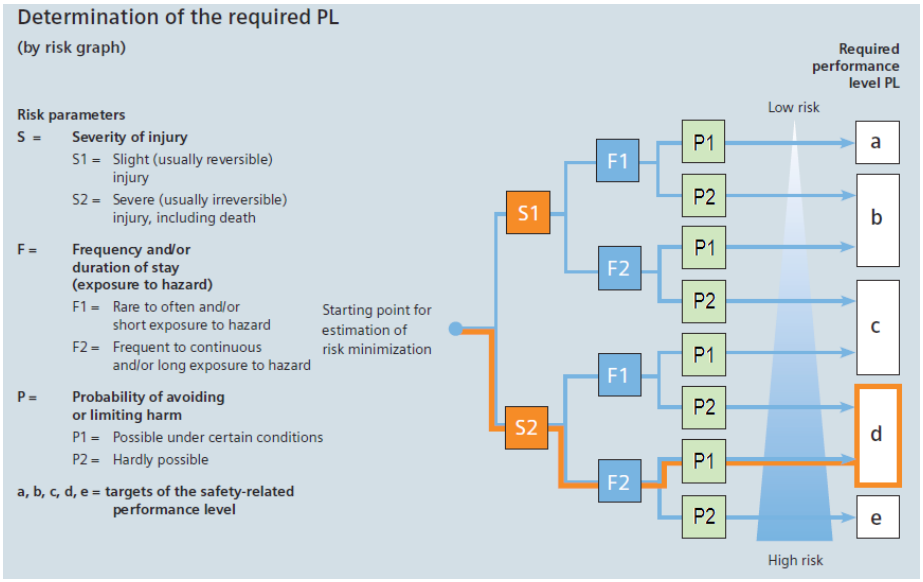

Fig. 3. The risk elements evaluation and PL requirements determination according to ISO 13849-1

This simplified procedure is based on the following equation:

$$R = (X) \text{ of a specified } (S) \tag{3}$$

where
R is the risk with no safety-related systems in place;
X is the frequency of the hazardous event with no safety-related systems in place;
S is the severity of consequence of the hazardous event (injury).

This produces the following three risk parameters:
– severity of injury (*S*);
– frequency and/or duration of exposure to hazard (*F*);
– possibility of avoiding or limiting harm (*P*).

Performance level (PL) of safety function according to ISO 13849-1 and its target failure measures are presented in Table 3.

Table 3. Safety integrity levels according to ISO 13849-1 – target failure measures for a safety function

Performance level (PL)	Average probability of a dangerous failure per hour [h^{-1}]
a	≥1E-5 to <1E-4
b	≥3E-6 to <1E-5
c	≥1E-6 to <3E-6
d	≥1E-7 to <1E-6
e	≥1E-8 to <1E-7

3. Correctness of risk evaluation and safety integrity level

3.1. Fundamental consideration of the problem addressed

Risk evaluation is linked with aleatoric uncertainty and epistemic uncertainty. Aleatoric uncertainties are given by natural randomness in the behaviour of the investigated subject. Epistemic uncertainties come from lacking knowledge of the investigated subject. The use of simplified methods then only has meaning if simplification does not radically increase epistemic uncertainties. Furthermore, only if epistemic uncertainty from knowledge of the subject's risk is not amplified by epistemic uncertainty of simplified risk evaluation.

The main purpose of this study is to find out to what extent is risk evaluation appropriate where simplified methods have been used. The result of this investigation is then better recognition of regularities valid for using simplified risk evaluation methods, hence lowering epistemic uncertainties associated with these methods.

Assessment is carried out for approaches given in IEC 61508-5, IEC 62061 and ISO 13849-1 and described in chapter 2. Their common designator is that they express the risk by the product of probabilities and consequences. Several parameters are used for it, see table 4.

It would seem that the approach according to ISO 13849-1 is different because it contains the probability (frequency) of undesirable event on an object which is a source of risk. The contradiction is only apparent. Approach according to IEC 61508-5, IEC 62061 assumes random occurrence of hazardous events in time, while ISO 13849-1 assumes the risk is permanent. The difference in approach is evident from Figure 4. In the end, both approaches evaluate risk as the product of probabilities and consequences, and determine the safety integrity level as a measure of risk reduction.

It is evident that for the quantitative risk evaluation the probability of consequence of undesirable events is given by the product of proba-

Table 4. Risk evaluation parameters according to IEC 61508-5, IEC 62061 and ISO 13849-1

Standard	Probability parameters			Consequence parameter
	Occurrence	Exposure	Avoidance	
IEC 61508-5	W	F	P	C
IEC 62061	Pr	Fr	Av	Se
ISO 13849-1	–	F	P	S

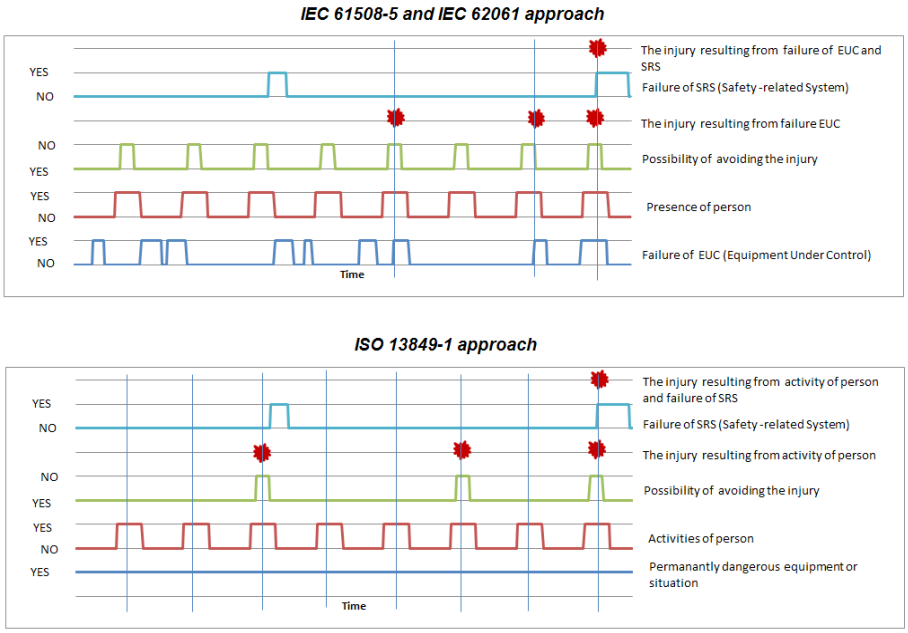

Fig. 4. The difference in dangerous situations

bility parameters and consequences. Thus, multiplying the values of all parameters takes place. If the values of these parameters are known, it is possible to evaluate the risk exactly.

The actual parameter values are not used when using the simplified approaches. Parameters are separated into zones. I instead of using the actual values, verbal (qualitative) evaluation or relative (semi-quantitative) evaluation expressed for example in points is used in these zones. Based on the given set of rules, see chapter 2, risk is then evaluated and assigned to safety integrity level. These features are common for selected standards IEC 61508-5, IEC 62061 and ISO 13849-1. Differences lie only in the evaluation parameters and rules used. Therefore, the investigation is focused on what impact on correctness lies within the choice of evaluation parameters and rules used for risk evaluation.

3.2. The assessment of the correctness of the simplified approach to IEC 61508-5

The method of determining safety integrity level (SIL) is based on a qualitative risk evaluation. Zones of parameters *C*, *F*, *P* and W and their ranges are assigned with verbal description. According to the description, parameter zones *C*, *F* and *P* can be seen as arranged in a sequence complied by a geometric scale without a specified quotient. For parameter *W* can be assumed that its scale is prepared according to geometric sequence with an unknown quotient.

If the simplified approach is correct, the results must match the results obtained when using fully quantitative risk evaluation. Each level of functional safety (-, a, 1, 2, 3, 4, b) is covered by successive risk intervals. With the appropriate set of parameter zones *C*, *F*, *P* and *W*, they should not overlap, see Figure 5.

Assessing the correctness of the simplified approach was based on examining whether the zone parameters *C*, *F*, *P* and *W* could be set so there was clear risk coverage through the SIL. Hence, inequality must then apply:

$$R < R_a < R_1 < R_2 < R_3 < R_4 < R_b \qquad (4)$$

If the inequality is not satisfied, risk is then overlapped by two or more SIL and simplified approach cannot be considered as correct.

Using simulation in Matlab results were found for all combinations of integers in the range <2; 20> quotients scales with geometric sequence of parameters *C*, *F*, *P* and *W*. Total number of $19^4 = 130\,321$ possibilities were examined in accordance with the simplified approach. The observed number of overlaps of two or more SIL is shown in Table 5 and Figure 6.

If the simplified risk evaluation method was as good as the exact quantitative method, column "0" in Table 5 would have value 130 321. The distribution of non-zero values and their size suggests how sensitive is the simplified method for accurate estimation of the *C*, *F*, *P* and *W* parameters. When possible risk estimates were generated, "brutal" combinations

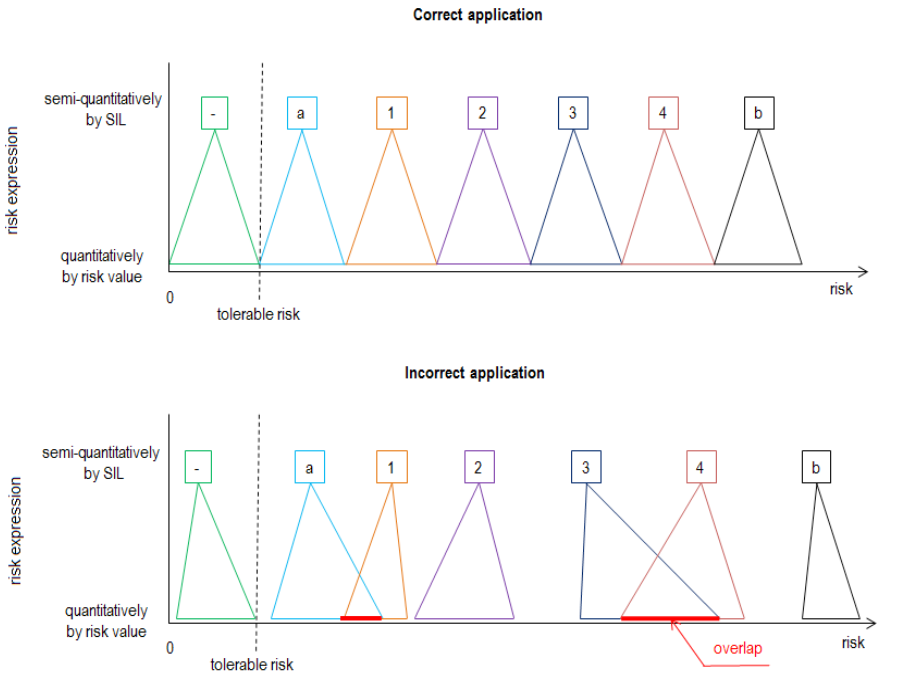

Fig. 5. Risk covered by SIL

Table 5. Number of overlaps (IEC 61508-5)

Overlap range	Number of couples of SIL category which overlap						
	0	1	2	3	4	5	6
One (next) SIL category	0	0	0	14	82	2 114	128 111
Two SIL categories	2	169	16 107	26 263	27 773	6 007	0
Three SIL categories	2 995	4 695	50 819	57 508	14 304	0	0
Four SIL categories	58 236	14 490	41 143	16 452	0	0	0
Five SIL categories	108 870	0	21 451	0	0	0	0
Six SIL categories	124 922	5 399	0	0	0	0	0

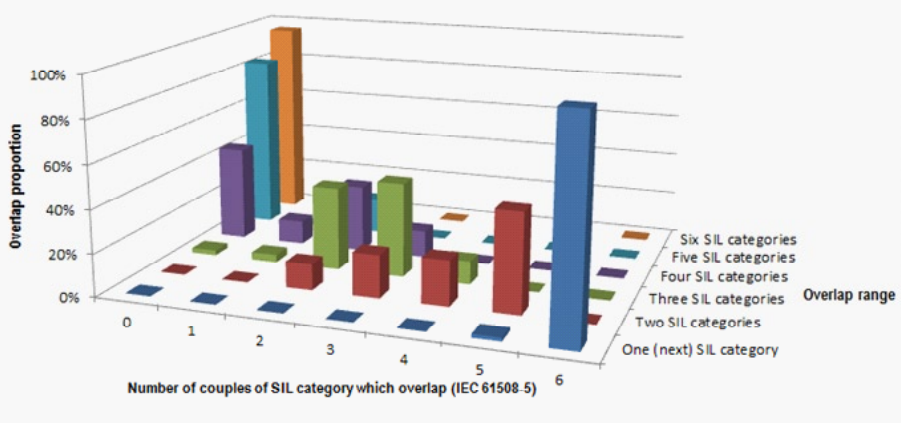

Fig. 6. Graph of overlap proportion (IEC 61508-5)

were also generated; these would not be used in a real application of the simplified method. These "brutal" combinations are represented for example by value 5 297 quotients combinations where the overlap goes over six SIL categories. Yet it is clear from the presented results that the simplified approach leads to significant inaccuracies in risk evaluation and SIL determination. Each combination of the *C*, *F*, *P* and *W* parameters determined SIL incorrectly, see value 0 in column "0" in Table 5. It cannot therefore be considered as correct.

3.3. The assessment of the correctness of the simplified approach according to IEC 62061

The method of determining safety integrity level (SIL) in this standard is different from the method specified in IEC 61585. It is based on semi-quantitative risk evaluation. It uses four parameters (*Se*, *Fr*, *Pr* and *Av*), which are assessed by points and reflected in the risk matrix where SIL determination takes place. Given that the score of probability parameters *Fr*, *Pr* and *Av* sums into a single endpoint parameter *Cl*, the use of geometric scales with the same quotient Q is apparent. Thus the sum arises from this relationship.

$$Q^{Fr} \cdot Q^{Pr} \cdot Q^{Av} = Q^{Fr+Pr+Av} \tag{5}$$

It represents the scales only on two levels, it is unnecessary to examine the scale composition (whether it is arithmetic or geometric) and can be considered as a scale drawn up in accordance with geometric sequence with an unknown quotient.

Again, as for IEC 6158-5, if the simplified approach is correct, the results must be consistent with the results obtained when using the fully quantitative risk evaluation. Each level of functional safety (1, 2, 3) covers successive risk intervals. When the correct parameters zones are set for *Se*, *Fr*, *Pr* and *Av*, they should not overlap. Therefore, inequality must apply.

$$R_1 < R_2 < R_3 \tag{6}$$

If the inequality is not satisfied, the risk is then overlapped by two or more SIL and the simplified approach cannot be considered as correct.

Results were found for all combinations of integers in the range <2; 20> quotients scales with geometric sequence parameters *Se*, *Fr*, *Pr* and *Av* by doing a simulation in Matlab. However, since parameters *Fr*, *Pr* and *Av* must always have the identical quotient, the possible number of quotients combinations is $19^2 = 361$. This is the total number of examined options for the simplified approach of risk evaluation. The observed number of overlaps is shown in Table 6 and Figure 7.

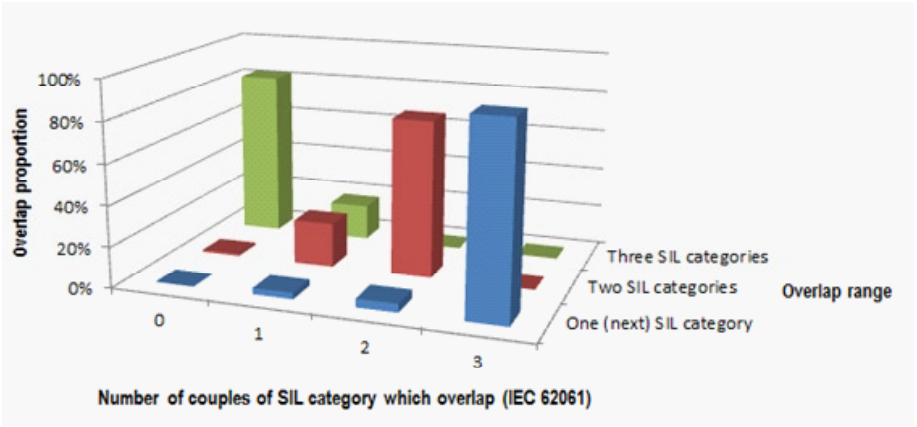

Fig. 7: Graph of overlap proportion (IEC 62061)

It can be clearly seen that even this simplified approach leads to significant inaccuracies in evaluating risk and determining SIL. Each combination of the *Se*, *Fr*, *Pr* and *Av* parameters determined SIL incorrectly, see value 0 in column "0" in Table 6. It cannot therefore be considered as correct.

Table 6. Number of overlaps (IEC 62061)

Overlap range	Number of couples of SIL category which overlap			
	0	1	2	3
One (next) SIL category	0	11	15	335
Two SIL categories	4	79	278	0
Three SIL categories	298	63	0	0

3.4. The assessment of the correctness of the simplified approach according to ISO 13849-1

Similarly to IEC 61508-5 the method for determining safety integrity level (PL) is in this standard is based on qualitative risk evalu-

ation. It only uses three parameters. Parameter zones *S*, *F* and *P* and their scope are assigned with verbal description. Given that the scales only have two levels, it is then unnecessary to examine their composition (whether it is arithmetic or geometric) and can be regarded as scales based on geometric sequence with an unknown quotient. Again, as in IEC 61508-5, if the simplified approach is correct, the results must be consistent with the results obtained when using the fully quantitative risk assessment. Each level of functional safety (a, b, c, d, e) is covered by successive risk intervals. When the correct parameters zones are set for *S*, *F* and *P* they should not overlap. Therefore, inequality must apply.

$$R_a < R_b < R_c < R_d < R_e \tag{7}$$

If the inequality is not satisfied, the risk is then overlapped by two or more SIL and the simplified approach cannot be considered as correct.

Results were obtained by doing a simulation in Matlab for all combinations of integers in the range <2; 20> quotients scales with geometric sequence parameters *S*, *F* and *P*. In total $19^3 = 6\,859$ possible risk evaluation options were examined according to the simplified approach. The observed number of overlaps is shown in Table 7 and Figure 8.

Table 7: Number of overlaps (ISO 13849-1)

Overlap range	Number of couples of PL category which overlap				
	0	1	2	3	4
One (next) PL category	2 109	0	4 750	0	0
Two PL categories	6 459	400	0	0	0
Three PL categories	6 859	0	0	0	0
Four PL categories	6 859	0	0	0	0

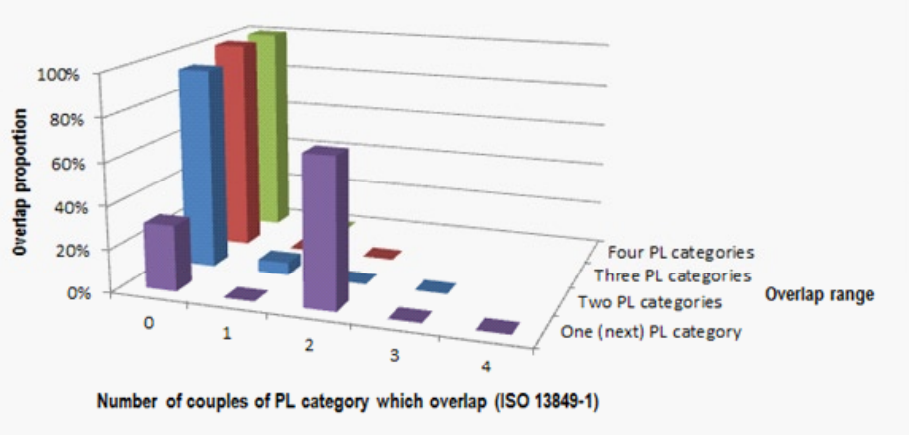

Fig. 8. Graph of overlap proportion (ISO 13849-1)

It can be clearly seen from the presented results that the simplified approach according to ISO 138491 is more robust than IEC 615085 and IEC 62061 in terms of resistance to inappropriate composition of risk parameter scales. This fact can be also observed from the concentration of values in column "0" in Table 7. Even this approach is not resistant against its improper use and it cannot be regarded as entirely correct.

4. Conclusion

IEC 61508 5, IEC 62061 and ISO 138491 standards do not indicate any primary sources with references to the fundamental works in the discipline around risk. The standards generally recommend applying quantitative risk evaluation but for practical application they only offer informative guidelines for qualitative and semi-quantitative risk evaluation in the form of graphs or risk matrices, from these then arise the requirements for SIL. Without taking into account the nature of the subjects that are sources of the risk, applying these standards can result into a series of serious errors.

In particular, simplified approaches of risk evaluation presented in the informative annexes of IEC 615085 and IEC 62061 are highly dependent on the correct understanding of the risks. They are very sensitive to the methods of composition scales of risk parameters. Therefore, the risk evaluation of complex systems (power plants, chemical plants, railway vehicles, etc.) should apply simplified methods uniformly to all devices that make up the entire system. Correct SIL determination cannot be guaranteed for qualitative or semi-quantitative risk evaluation of complex systems in accordance with those standards including ISO 13849-1. Fatal errors may occur; these can be partially eliminated by using a unified method for setting risk parameters (probability and consequence) for all suppliers of the equipment which then forms the complex system. This implies that the same range of scales should be used for all cases for assessing the probability and consequences. The risk of the equipment is in this case expressed implicitly. Tolerability of the risk is not clearly established. It is hidden. It is derived from the scales of probability and consequences; and the decision of which combination of probability and consequences begins to apply the lowest SIL.

This problem does not occur when the fully quantitative risk evaluation is used. Uniformity of the method used for evaluation is guaranteed. If the level of tolerability of risk is set the same for all devices of the complex system, there are no contradictions in determining the required SIL. The risk is expressed explicitly when the quantitative method is used. It is clearly defined whether the risk of the equipment is tolerable or not. This is due to setting the threshold value of tolerability for individual and societal risks, potentially economic or environmental risks. The requirements for SIL are clearly specified to achieve tolerable levels of risk.

Acknowledgement:
This paper has been elaborated in the framework of the project Opportunity for young researchers, reg. no. CZ.1.07/2.3.00/30.0016, supported by Operational Programme Education for Competitiveness and co-financed by the European Social Fund and the state budget of the Czech Republic.

References

1. IEC 61508 5:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: Examples of methods for the determination of safety integrity levels.

2. IEC 61511 x:2003, Functional safety – Safety instrumented system for the process industry sector.
3. IEC 62061:2005, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.
4. ISO 13849-1:2006, Safety of machinery – Safety-related parts of control system – Part 1: General principles for design.
5. IEC 61513:2001, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.
6. EN 50129:2003, Railway applications – Communication, signalling and processing systems – Safety-related electronic systems for signalling.
7. http://www.automation.siemens.com/mcms/infocenter/dokumentencenter/ce/Documentsu20Brochures/e20001-a230-m103-v5-7600.pdf

Assoc. Prof. Pavel FUCHS
Technical University of Liberec
Studentska str., 2-46117 Liberec, Czech Republic
e-mail: pavel.fuchs@tul.cz

Jaroslav ZAJICEK, Ph.D.
Technical University of Ostrava
17. listopadu str.,15-70833 Ostrava – Poruba, Czech Republic
e-mail: jaroslav.zajicek@vsb.cz