Michał Ciucias, Waldemar Nowakowski, Daniel Pietruszczak

Safety of industrial automation systems

JEL: R41 DOI: 10.24136/atest.2019.124
Data zgłoszenia: 05.04.2019 Data akceptacji: 26.06.2019

In order to minimize the risks associated with the automation of industrial processes, it is necessary to unify standards of safety assessment. The aim of this article is the comparative analysis of safety assessment methods of industrial automation systems. Authors presented two techniques of ensuring safety based on risk analysis, i.e. Performance Level (PL) and Safety Integrity Level (SIL) in relation to the applicable standards and regulations.

Słowa kluczowe: safety, industrial automation systems, PL, SIL.

Wstęp

The safety of automation systems is one of the important safety elements in the industry. The risk associated with the operation of these systems must be at an acceptable level [8, 9, 11, 19]. Therefore, it is necessary to consider methods of risk analysis during the design, construction and maintenance of industrial automation systems. Risk is understood as the probability of an undesirable event. An undesirable event is an event (damage, failure, human error) whose occurrence causes a threat. In any technical system, new undesirable events may occur at different times, which may trigger a sequence of secondary events and the transition from a state of emergency to losses called an accident or a disaster. The amount of loss usually refers to human life and health, material loss and ecological damage [13, 14]. Several basic steps can be distinguished in the risk assessment process. The first is the identification of the technical system. The aim of this stage is to get to know the research object, the conditions of its work, the manner of service, etc. Then, the hazard identification during which the identification of dangerous events that may occur during the operation of the technical system is carried out. As part of this stage, an accurate description of potential events is prepared while their causes, effects and possible safeguards are identified. Based on the collected information, the risk is estimated. These three stages are part of the risk analysis. After assessing the risk, risk evaluation should be carried out and a decision about the acceptability or not of the occurring risk should be made. If the risk is not acceptable, further action should be taken to reduce the risk, referred to as the safety function, and then the entire estimation procedure should be repeated [10, 12, 15, 16]. The level of security of industrial automation systems is determined by one of two possible parameters [1, 2, 17]: Performance Level - can be used in relation to electrical, mechanical, pneumatic and hydraulic solutions applied to improve safety. Safety Integrity Level - can be used only to evaluate electrical, electronic and programmable solutions applied to improve safety.

1.Performance Level

The Performance Level (PL) is also defined as a measure of the reliability of a given safety function. A hazardous situation for the operation of machines has been classified according to five levels of safety. Starting from "PL a" (low) to the level "PL e" (high). The required safety level PL, in accordance with EN ISO 134849-1, is calculated and defined as part of the risk assessment [4].

The performance level PL is determined by means of individual structures using the following parameters, i.e.:

- category, structural requirements (Category, SRP / CS architecture);
- mean time until a dangerous failure of each control subsystem (MTTFd: Meantime to dangerous failure);
- diagnostic coverage (DC: Diagnostic coverage);
- common cause failure (CCF: Common cause failure).

1.1.Category, structural requirements (Category; SRP/CS architecture)

The EN ISO 13849-1 standard lists categories (table 1) and presents examples of structures illustrated in the form of diagrams (Figure 1-4) [4]. These schemes are called simplified reliability block diagrams. An important task in assessing the security of the industrial automation system is to assign the actual structure to a specific category.

Tab. 1. Determining the system category [4]

Category	System behavior
B	A fault can lead to loss of security
1	As in category B, but the probability of a fault is lower than in category B.
2	A fault can lead to the loss of the safety function between two periodic inspections and the loss of the safety function is detected by the control system in the next test.
3	In the event of a single fault, the safety function is always met. Only some faults will be detected. The loss of safety function may occur after accumulation of undetected faults.
4	When failures occur, the safety function is always met. Faults will be detected in a timely manner to overcome the loss of the safety function.

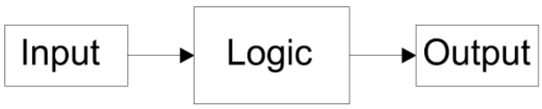

Fig. 1. Category B (own study based on [4])

The single-channel structure in a typical arrangement (Fig. 1) includes a sensor (Input), a logic part (Logic) and an actuator (Output).

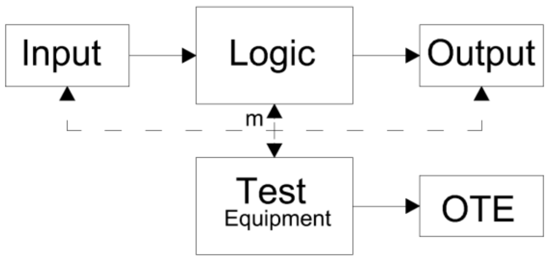

Fig. 2. Category 2 (own study based on [4])

A single-channel structure consisting of a sensor (Input), a logic part (Logic), an actuator (Output), an additional external monitoring system (Test equipment), and output of test equipment.

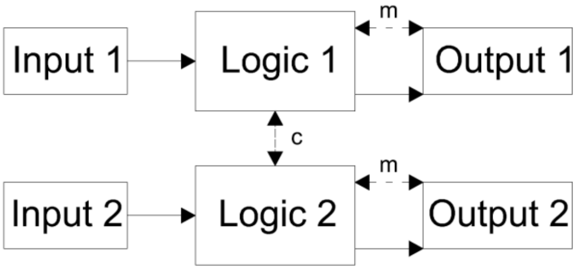

Fig. 3. Category 3 (own study based on [4])

Category 3 and 4 are characterized by a two-track (redundant) structure. This means that there is a sensor, a logic part and an actuator in each channel. Categories have additional track monitoring functions as well as mutual track monitoring.

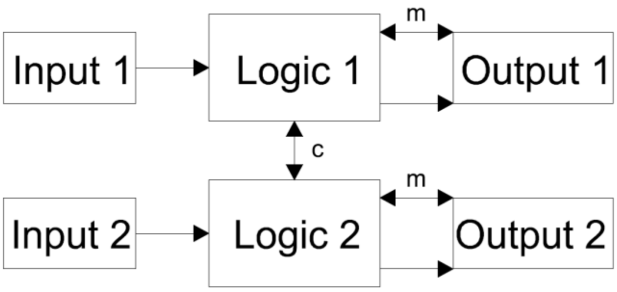

Fig. 4 Category 4 (own study based on [4])

where:

Interconnection

c Cross monitoring

m Monitoring

m Monitoring (practical troubleshooting possible)

Figure 5 shows selected subsystems of the safety function.

Fig. 5. Subsystems of the safety function. (Own study based on[7])

1.2. Mean time to dangerous failure of each control subsystem (MTTFd)

MTTFd parameter informs about the amount of time that middlingly elapses between further dangerous damages of components. The value of MTTFd is calculated with taking into account the type of subsystem and it is qualitative definition of safety function.

For the estimation of the MTTFd of each control channel (subsystem), one of the procedures shall be used in the order given:

– use manufacturer's data;
– use methods described in table C included in EN ISO 13849-1 [4];
– choose 10 years of use.

In case the manufacturer does not provide the MTTFd value then table C included in EN ISO13849-1 [4] presents four methods for calculating MTTFd for individual parts[7]:

Analyzing the first method one can see in table C typical MTTFd values (in years) for mechanical and hydraulic parts. In the second method for hydraulic parts, with appropriate assumptions, a specific value of 150 years is indicated. In the third method in which we deal with mechanical, pneumatic and electromechanical parts, MTTFd is determined from the following formula:

$$MTTF_d = \frac{B10_d}{0,1 * n_{op}} \quad (1)$$

where:

$B10_d$ - average number of operating cycles achieved before 10% of the samples fail to the dangerous condition. $B10_d$ value should be designated for every consuming component being a part of control system's elements relevant to maintaining safety [22].

n_{op}- number of activity cycles per years;

$$n_{op} = \frac{d_{op} * h_{op} * 3600s/h}{t_{cycle}} \quad (2)$$

where:

d_{op}-operation days per years [d/y];

h_{op}-operation hours per day [h/d];

t_{cycle}-mean time between two activity cycles [s/cycle];

$$T10_d = \frac{B10_d}{n_{op}} \quad (3)$$

$$MTTF_d = \frac{T10_d}{0,1} \quad (4)$$

where:

$T10_d$ – time until 10% of the components fail dangerously;

The calculation of $MTTF_d$ for electronic components based on fourth method is made on the basis of MTTFd values contained in the tables for the elements from which the formula is created:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d,i}} \quad (5)$$

where:

N - number of elements.

The mean time MTTFd is divided into three ranges and is summarized in Table 2.

Tab. 2. Determining the system category [4]

Index	Range $MTTF_d$
Low	3 years ≤$MTTF_d$< 10 years
Medium	10 years ≤$MTTF_d$< 30 years
High	30 years ≤$MTTF_d$< 100 years

1.3.Diagnostic Coverage (DC)

Diagnostic coverage is a measure of the number of dangerous failures detected by the diagnostic system. Diagnostic coverage reduces the likelihood of dangerous hardware failures thanks to automatic diagnostic tests. They are determined according to the following formula:

$$DC = \sum \lambda_{DD} / \sum \lambda_{Dtotal} \quad (6)$$

where:

λ_{DD}- the probability of a detected dangerous failure;

λ_{Dtotal}- the probability of total dangerous failures;

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \dots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \dots + \frac{1}{MTTF_{dN}}} \quad (7)$$

where:

d1, d2, dn represent the separate SRP / CS parts

The calculated diagnostic coverage assumes the ranges included in the Table 3.

Tab. 3. Determining the coverage [4]

Index	Range of diagnostic coverage
Low	DC<60%
Medium	60%≤DC<90%
High	90%≤DC<99%

1.4. Common cause failure

CCF parameter defines persistence of the system on occurrences which makes simultaneous failures of two or more separate channels in multichannel's systems which in consequence may guide to failure in function connected with safety. Table 4 presents measures and requirements for protection against this type of damage. When a precautionary measure is applied to the subsystem, the total number of points is allocated. The CCF test is only valid for categories 2, 3, 4. Resistance to CCF is appropriate if the sum of points is greater than or equal to 65.

Tab. 4. Measures and requirements against CCF [4]

MEASURE / REQUIREMENT		Points
Separation	Separation between signal paths (electric and hydraulic lines), sufficient surface and air distances	15
Diversity	Different technologies or physical principles, e.g. first channel programmable electronic and second channel hardwired; digital and analog measurement; components of different manufacturers	20
Design, Experience, Application	Protection against over-current, over-voltage	15
	Application of well-tried components	5
Analysis assessment	Carrying out a failure mode and effect analysis (FMEA) to avoid common-cause failures in design	5
Training, Competence	Raising the competence of designers through training in the direction of understanding the causes and effects of failures caused by a common cause	5
Environmental influences	Research on the EMC compatibility	25
	Subsystem tests with regard to environmental factors	10

1.5. Designation of the PL for the subsystem and system

Once all the parameters have been determined, you define the PL of the subsystem based on Figure 6. If there is a need for a more accurate reading of the value, we use table No. 6, which takes into account the additional parameter PFHd (Probability of a dangerous failure per hour). The PL of the entire system is determined by tables 5 and 6. If the obtained PL is greater than or equal to that required for the PLr function, it is assumed that the given safety system meets the requirements.

Tab.5. Probability of a dangerous failure per hour [4]

Performance Level	Probability of a dangerous failure per hour (PFH_d) [1/h]
a	$\geq 10^{-5}$ and $<10^{-4}$ 〈0.001% to 0.01%〉
b	$\geq 3 \times 10^{-6}$ and $<10^{-5}$ 〈0.0003% to 0.001%〉
c	$\geq 10^{-6}$ and $<3 \times 10^{-6}$ 〈0.0001% to 0.0003%〉
d	$\geq 10^{-7}$ and $<10^{-6}$ 〈0.00001% to 0.0001%〉
e	$\geq 10^{-8}$ and $<10^{-7}$ 〈0.000001% to 0.00001%>

Tab.6. Designation of the PL of the system based on knowledge of the PL of the subsystems [4]

Lowest PL of subsystem	Number of subsystems having the following PL	=>	Maximum possible PL of system
a	>3	=>	Impermissible
	≤3	=>	a
b	>2	=>	a
	≤2	=>	b
c	> 2	=>	b
	≤ 2	=>	c
d	> 3	=>	c
	≤ 3	=>	d
e	> 3	=>	d
	≤ 3	=>	e

1.6. Validation of the PL

The aim of validation is counterchecking if the SRECS safety system fulfills given it requirements contained in SRCF specification.

All requirements for running category validation are included in EN ISO 13849-2 [21], more precisely: [3]

– requirements relating to the precise level of security assurance;
– requirements for specifying categories in accordance with the standard,

Documentation for validation should come from the project and be verified and validated in order to give an opinion on the design of the machine in question. The Validation should be prepared on the basis of prepared safety plan. The validation protocol should contain information pertinent to the course of the validation process, the criteria of mistakes removal and report from the conducted research. If

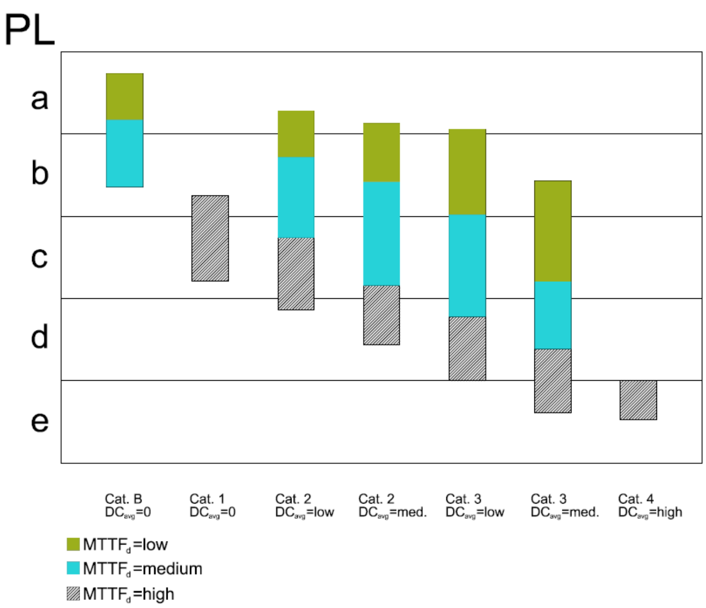

Fig. 6. Relationship - PL and Cat, DC, MTTFd. (Own study based on [18])

any defects are noted in the documentation, it is returned to the person preparing it. The above-described process is repeated for each of the safety functions.

2.Safety Integrity Level (SIL)

Safety integrity level (SIL), is a measure of the safety of electrical, electronic and mechanical devices, and it may also refer to software. SIL is determined on the basis of EN 62061 [6] or EN IEC 61508 [5], which contain a methodology for testing whether selected control system structures meet defined safety requirements. The EN 62061 standard defines SIL in 3 levels 1-3, where 3 is the highest level. The use of SIL means that a cyclic control is carried out, which includes elements such as: procedures of conduct, connection diagrams, and for risk assessment - information on failure rates justified by inspections. The risk assessment supported by SIL is a qualitative assessment.

The EN IEC 61508 standard defines two types of systems [5]: Systems operating On-demand, occasionally (low functional load). Low probability of system malfunction while handling the request; Systems operating continuously or frequently (high functional load). There is a probability of dangerous damage per hour. Obtaining the necessary level of safety integrity for the industrial automation system takes place in five stages. First step involves assigning SIL and determining the structure of the SRECS (Safety Related Electrical Control System). The estimation of the required SIL level is performed for each dangerous occurrence with the breakdown into the parameters included in Fig. 7.

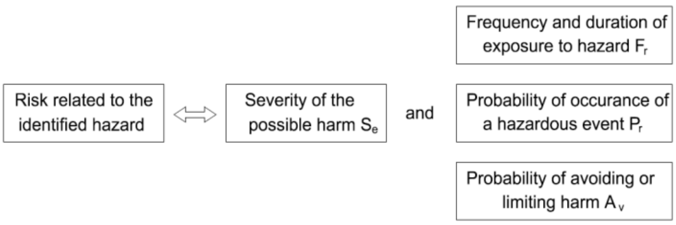

Fig.7. Risk estimation according to EN ISO 62061 [6]

The severity of injuries or damage to health can be portrayed by taking into account reversible, irreversible injuries and death. The injury score is presented in Table 7.

Tab. 7. "Injury severity score (Se)" according to EN ISO 62061 [6]

Consequences	Severity (Se)
Irreversible: death, loss of the eye or arm	4
Irreversible: limb fractures, loss of fingers	3
Reversible: medical personel required	2
Reversible: first aid required	1

When specifying Fr, we pay attention to aspects such as:

- Frequency of staying in the danger zone in different operating modes (normal operation, preservation, cleaning);
- What types of tasks are performed.

Tab. 8. "Classification of frequency and exposure time" according to EN ISO 62061 [6]

Frequency and exposure time (F_r)	
Frequency and exposure time	Time > 10 min
≤ 1 h	5
> 1h to ≤ 1 day	5
> 1 day to ≤ 2 weeks	4
> 2 weeks to ≤ 1 year	3
> 1 year	2

When discussing the probability of a dangerous event, we must consider two basic concepts:

- Predictability of hazardous elements in different parts of the machine in different modes of operation;
- Behavior of people interacting with the machine such as stress, fatigue, lack of experience.

Tab.9. "Probabilistic classification (Pr)" according to EN ISO 62061 [6]

Probability of occurence	Probability (Pr)
Very high	5
Convenient	4
Possible	3
Rare	2
Negligible	1

The Av parameter is connected with machine construction and has been classified by three variants presented in the Table 10.

Tab.10. "*Probability* of *avoiding or* limiting harm (Av) Classification" according to EN ISO 62061 [6]

Probability of *avoiding or* limiting harm (Av)	
Impossible	5
Rare	3
Probable	1

For each severity level Se, the loss probability class C_l is calculated using the following relationship:

$$C_l = F_r + P_r + A_v \quad (8)$$

The SIL estimation is made using the following table:

Tab. 11. "SIL assignment matrix" according to EN ISO 62061 [6]

Severity (Se)	Class (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3	-	-	SIL 1	SIL 2	SIL 3
2	-	-	-	SIL 1	SIL 2
1	-	-	-	-	SIL 1

Function blocks are created owing to a detailed division of the safety functions. (Figure 8)

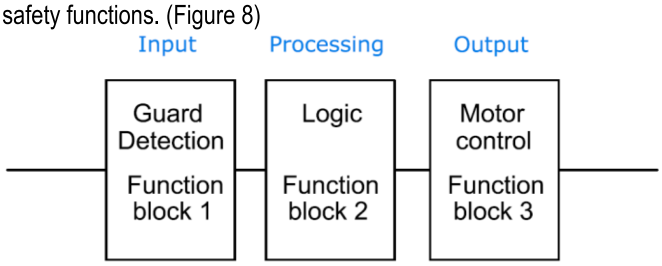

Fig. 8. Division into function blocks. (Own study based on [20])

Next step covers the exchange of security requirements for each function block and the allocation of blocks to the subsystem in architecture (Figure 9). Failure of any subsystem will lead to failure of the safety related control function.

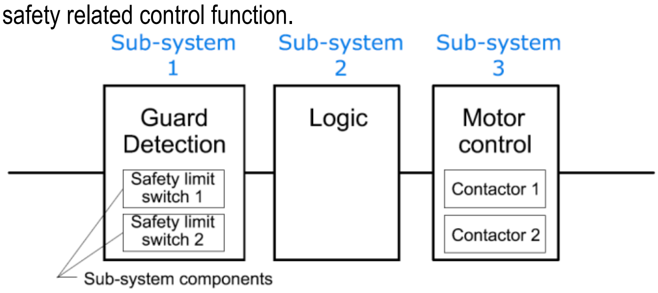

Fig. 9. Assignment of function blocks (own study based on [20])

In this step it is significant to make selection of components for each of the subsystems (Figure 10).

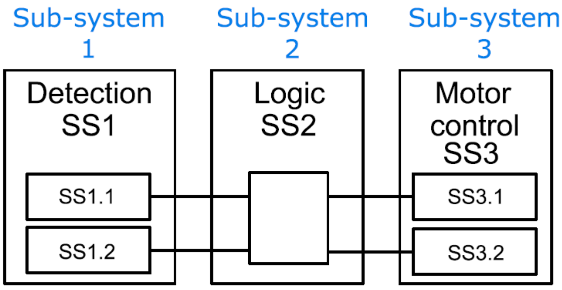

Fig. 10. Selecting components (Own study based on [20])

According to EN ISO 62061 [6], the last matter to do is designing the diagnostic function. SIL subsystems are created on the basis of chosen architecture. There are four basic subsystems architecture:

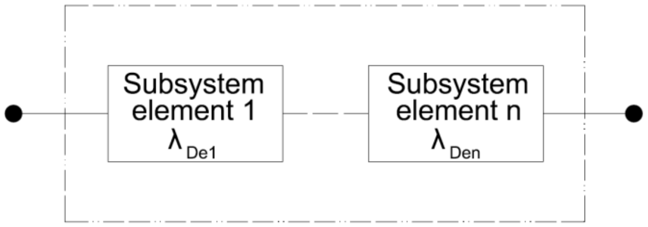

Fig. 11. Subsystem architecture type A [6]

The simplest architecture of subsystem is a single channel without any diagnostic function.

$$\lambda_{DSSA} = \lambda_{DE1} + \cdots + \lambda_{DEN}$$
$$PFH_{DSSA} = \lambda_{DSSA} * 1h \quad (9)$$

where:
λ_{DSSA} - intensity of subsystem's dangerous damage;
λ_{DE1} - dangerous damage's stream of the 1 element of subsystem.

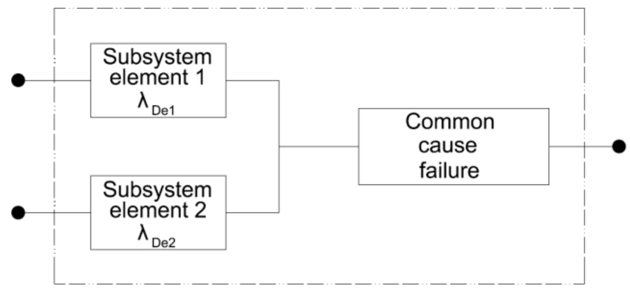

Fig. 12. Subsystem architecture type B [6]

Figure 12 shows single fault tolerant subsystem without a diagnostic function.

$$\lambda_{DSSB} = (1-\beta)^2 * \lambda_{De1} * \lambda_{De2} * T1 + \beta * (\lambda_{De1} \quad (10)$$
$$PFH_{DSSB} = \lambda_{DSSB} * 1h$$

where: β - vulnerability to damage that is caused by a common cause.

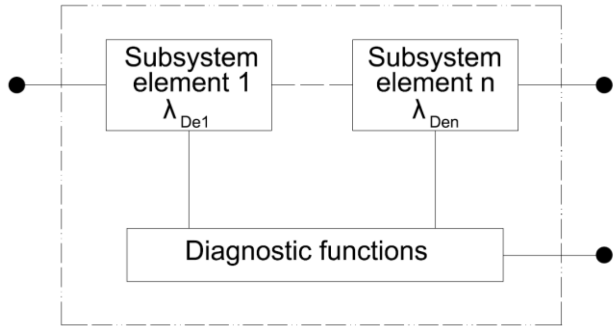

Fig. 13. Subsystem architecture type C [6]

Subsystem architecture type C shows functional representation of the fault tolerant system with diagnostic function. Diagnostic coverage is used to reduce the likelihood of a dangerous hardware failure. Diagnostic tests are performed automatically [16].

$$\lambda_{DSSC} = \lambda_{DE1}(1-DC_1) + \cdots + \lambda_{DEN}(1-DC_n) \quad (11)$$
$$PFH_{DSSC} = \lambda_{DSSC} * 1h$$

where:
DC_1 – diagnostic coverage of subsystem element 1.

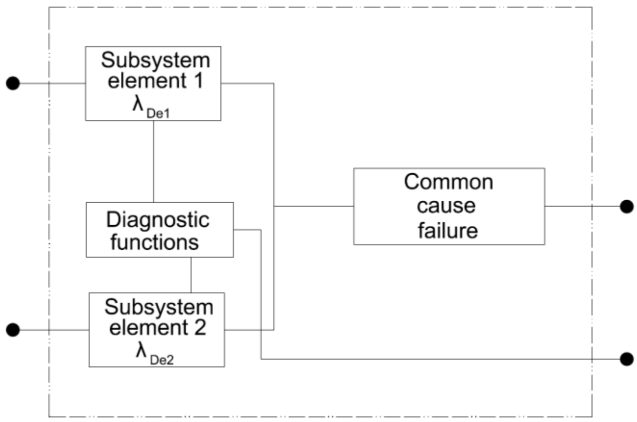

Fig. 14. Subsystem architecture type D [6]

The last subsystem D is a parallel connection of two elements and additionally has a diagnostic function.

The elements of the subsystem characterized by a different construction describes equation number 12 whereas the elements of the subsystem characterized by the same construction describes equation number 13.

Summary

The safety of industrial automation systems is becoming a subject of growing interest. Therefore, it is important to develop methods

$$\lambda_{DSSD} = (1-\beta)^2\left\{[\lambda_{DE1} * \lambda_{DE2}(DC_1 + DC_2)] * \frac{T_2}{2} + [\lambda_{DE1} * \lambda_{DE2} * (2 - DC_1 - DC_2)] * \frac{T_1}{2}\right\} + \beta * (\lambda_{DE1} * \lambda_{DE2})/2 \quad (12)$$
$$PFH_{DSSD} = \lambda_{DSSD} * 1h$$

$$\lambda_{DSSD} = (1-\beta)^2\left\{\left[\lambda_{DE}{}^2 * 2 * DC\right] * \frac{T_2}{2} + \left[\lambda_{DE}{}^2 * (1-DC)\right] * T_1\right\} + \beta * \lambda_{DE} \quad (13)$$
$$PFH_{DSSD} = \lambda_{DSSD} * 1h$$

Where:
T_2 – clearance between testing tests
T_1 – gap between periodic testing tests or time of life (for calculations it is important to assume lower value)

for assessing the level of safety and the choice of options, as well as effective ways to improve it. The authors of the article presented the concept of risk assessment of industrial automation systems. Two concepts of ensuring safety by means of automation systems, i.e. the PL and SIL methods, have been discussed in detail.

Bibliography:

1. Bornemann A., Froese Y., Landi, L. et al., Probabilities in safety of machinery-Part 1: Risk profiling and farmer matrix, Safety and Reliability: Methodology and Applications, CRC Press, pp. 1933-1942, 2015.
2. Bornemann A., Froese Y., Landi L. et al., Probabilities in safety of machinery-Part 2: Theoretical and practical design, Safety and Reliability: Methodology and Applications, CRC Press, pp. 1943-1950, 2015.
3. Dźwiarek M.: Walidacja poziomu zapewnienia bezpieczeństwa przez systemy sterowania maszynami. Journal of KONBiN 1(33), 2015 (in Polish).
4. EN ISO 13849-1:2015, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (ISO 13849-1:2015).
5. EN 61508:2010, Functional safety of electrical/electronic/ programmable electronic safety related systems. (IEC 61508:2010).
6. EN 62061:2005, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.
7. Kasprzyczak L.: Bezpieczeństwo maszyn - Wyznaczanie poziomu zapewnienia bezpieczeństwa. Journal of KONBiN 1(25) 2013 (in Polish).
8. Kornaszewski M., Chrzan M., Olczykowski Z., Implementation of New Solutions of Intelligent Transport Systems in Railway Transport in Poland, Book Series: Communications in Computer and Information Science, Volume 715, pp. 282-292, 2017.
9. Lewinski A., Perzyński T., The Reliability and Safety of Railway Control Systems Based on New Information Technologies, Book Series: Communications in Computer and Information Science, Volume 104, pp. 427-433, 2010.
10. Łukasik Z., Nowakowski W., Kuśmińska-Fijałkowska A., Zarządzanie bezpieczeństwem infrastruktury krytycznej, Logistyka 4/2014, str. 758-763, 2014 (in Polish).
11. Nowakowski W., Diagnostyka systemów automatyki kolejowej jako metoda poprawy bezpieczeństwa. Wydawnictwo UTH w Radomiu. Seria Monografie, Nr 218. Radom 2018 (in Polish).
12. Nowakowski W., Bojarczak P., Łukasik Z., Verification and Validation of Railway Control Systems Using an Expert System. In: Kováčiková T., Buzna Ľ., Pourhashem G., Lugano G., Cornet Y., Lugano N. (Eds.), Intelligent Transport Systems – From Research and Development to the Market Uptake (INTSYS 2017), Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol 222, pp. 43-50, Springer, Cham, 2018.
13. Nowakowski W., Ciszewski T., Łukasik Z., Metody oceny wpływu czynnika ludzkiego na bezpieczeństwo w transporcie. Autobusy: technika, eksploatacja, systemytransportowe, 6/2018, str. 180-184, 2018 (in Polish).
14. Nowakowski W., Ciszewski T., Łukasik Z., The Human as the Weakest Link in Ensuring Technical Safety. Proceedings of the 17th International Scientific Conference Globalization and Its Socio-Economic Consequences, Rajecke Teplice, Slovakia, Part IV, pp. 1788-1795, 2017.
15. Nowakowski W., Łukasik Z., Bojarczak P., Technical safety in the process of globalization, Proceedings of the 16th International Scientific Conference Globalization and Its Socio-Economic Consequences, Rajecke Teplice, Slo-vakia, 2016, Part IV, pp. 1571-1578, 2016.
16. Nowakowski W., Łukasik Z., Bukalski W.: Metody oceny bezpieczeństwa systemów automatyki przemysłowej, Autobusy: technika, eksploatacja, systemy transportowe, 12/2018, str. 158-162, 2018 (in Polish).
17. Piggin R., What's happening with machine safety standards and networks?, Assembly Automation, Volume 26, Issue 2, pp. 104-110, 2006.
18. Robinson S.: SIL or PL? What is the difference? MIET MInstMC.
19. Ruud S., Skjetne R., Verification and Examination Management of Complex Systems, Modeling Identification and Control, Volume 35, Issue 4, pp. 333-346, 2014.
20. Schneider Electric: General presentation. Safety Legislation and Standards.
21. EN ISO 13849-2:2008 Safety of machinery – Safety-related parts of control systems – Part 2:Validation
22. Festo: Przewodnik po technice bezpieczeństwa. Rozwiązania pneumatyczne i elektryczne (in Polish).

Bezpieczeństwo systemów automatyki przemysłowej

Rosnące wymagania dotyczące minimalizacji zagrożeń, jakie wiążą się z automatyzacją procesów przemysłowych, wymuszają potrzebę standaryzacji w zakresie oceny bezpieczeństwa. Celem artykułu jest analiza porównawcza metod oceny bezpieczeństwa systemów automatyki przemysłowej. Autorzy przedstawili dwa sposoby zapewnienia bezpieczeństwa, które wykorzystują analizę ryzyka tj.: badanie poziomu zapewnienia bezpieczeństwa PL oraz badanie poziomu nienaruszalności bezpieczeństwa SIL w odniesieniu do obowiązujących norm i przepisów.

Słowa kluczowe: bezpieczeństwo, systemy automatyki przemysłowej, PL, SIL

Authors:

mgr inż. Michał Ciucias – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, WTiE, m.ciucias@uthrad.pl

dr hab. inż. Waldemar Nowakowski - Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, WTiE, w.nowakowski@uthrad.pl

dr inż. Daniel Pietruszczak - Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, WTiE, d.pietruszczak@uthrad.pl