Kazimierz T. KOSMOWSKI
POLITECHNIKA GDAŃSKA, WYDZIAŁ ELEKTROTECHNIKI I AUTOMATYKI
ul. G. Narutowicza 11/12, 80-233 Gdańsk

Layers of protection analysis in the context of functional safety management

Prof. Kazimierz T. KOSMOWSKI

Is the associate professor and head of Automatics Department at the Faculty of Electrical and Control Engineering of Gdansk University of Technology. His field of interest includes analyses and assessments of dependability and risk of hazardous systems and processes including the functional safety of control and protection systems, and the human reliability analysis. He has published over 190 scientific works. He is a member of the board of the Polish Safety and Reliability Association.

e-mail: kazkos@ely.pg.gda.pl

Abstract

This paper presents the layer of protection analysis (LOPA) to be taken into consideration during the design of programmable safety-related control and protection systems for a hazardous process installation. Some issues concerning the solutions of the basic process control system (BPCS), safety instrumented system (SIS) and alarm system (AS), and the role of human operator in abnormal situations are discussed in the context of requirements and criteria given in international standards IEC 61508 and IEC 61511.

Keywords: layer of protection analysis, functional safety, programmable control and protection systems, alarm system, human factors.

Analiza warstw zabezpieczeń w kontekście zarządzania bezpieczeństwem funkcjonalnym

Streszczenie

Niniejszy artykuł przybliża analizę warstw zabezpieczeń (LOPA) uwzględnianą podczas projektowania programowalnych systemów sterowania i zabezpieczeń związanych z bezpieczeństwem instalacji procesowej podwyższonego ryzyka. Przedstawia się problemy dotyczące rozwiązań podstawowego systemu sterowania (BPCS), przyrządowego systemu bezpieczeństwa (SIS) i systemu alarmowego (AS) oraz rolę człowieka operatora w sytuacjach nienormalnych w kontekście wymagań i kryteriów podanych w normach międzynarodowych IEC 61508 i IEC 61511. Niektórzy producenci sprzętu i oprogramowania do zastosowań w programowalnych systemach sterowania i zabezpieczeń obiektów/ instalacji podwyższonego ryzyka proponują integrowanie systemów BPCS i SIS w warstwie sprzętowej widząc określone korzyści takich rozwiązań, chociaż wskazują również na możliwe ich wady. Autor niniejszego artykułu zarysowuje szersze podejście do problemu w kontekście projektowania systemu alarmowego i analizy roli człowieka-operatora traktowanej jak warstwa zabezpieczeń. Proponuje się przyjęcie ostatecznego rozwiązania na podstawie dogłębnej analizie i ocenie ryzyka oraz analizie niezawodności człowieka, jeśli przewidziano zadania do wykonania przez człowieka w ramach rozważanej funkcji związanej z bezpieczeństwem. Zwraca się uwagę na konieczność uwzględnienia i właściwej interpretacji norm bezpieczeństwa funkcjonalnego i poradnika metodycznego LOPA.

Słowa kluczowe: analiza warstw zabezpieczeń, bezpieczeństwo funkcjonalne, programowalne systemy sterowania i zabezpieczeń, system alarmowy, czynniki ludzkie.

1. Introduction

Nowadays across Europe there are in operation many hazardous process plants that require appropriate safety management in life time to reduce the risk to an acceptable level. Designing the inherently safe process in such plants is an important way to control risks and shape manufacturing environment. However, inherent safety is rarely achievable in many of technological processes. There are often significant risks associated with situations where hazardous or toxic materials are stored, processed or handled. Those risks should be minimized by relevant technological solutions of installations, mechanical means (e.g. physical barriers) and using the control and protection systems. They often include the basic process control systems (BPCS) and the safety instrumented systems (SIS) for implementing safety-related functions, e.g. safe shutdown of hazardous installation [1, 2].

There is increasing interest in the process industry to perform rigorous hazard analysis and based on the risk assessment results to design appropriate control and protection systems. This interest has considerably increased after publication of the international standards IEC 61508 [3] and IEC 61511 [4]. They have been then adopted as the European standards EN 61508 and EN 61511, as well as the Polish standards PN-EN 61508 and PN-EN 61511.

Today, manufacturers are looking for reduction in the cost of equipment, training, and technical support of their programmable protection systems including their closer integration with the control systems. They are increasingly focused on overall safety of a system from sensors to actuators and interested in using high integrity fieldbuses in safety-related applications in order to reduce expenses of field wiring and to obtain on-line diagnostics from devices. They are also seeking better tools for safety lifecycle management and flexible architectures that enable increased scalability [5].

This paper is devoted to some design issues of protection layers including BPCS, SIS and AS. Potential dependencies between these systems are indicated and some warnings concerning the integration of BPCS and SIS within an industrial computer network are specified. Proposals from some hardware and software producers to apply in practice integrated BPCS and SIS solutions are critically discussed to some extent. It is postulated that the decision concerning final solution should be based on detailed functional analysis and risk assessment with regard to requirements and criteria given in the standards EN 61508 and EN 61511 with regard to potential CCF (*common cause failure*) and human errors.

2. Hazard identification, risk assessment and defining safety-related functions

Modern industrial installations are equipped with complex programmable control and protection systems operating in computer networks. When designing the control and protection systems a functional safety concept [3] is more and more widely of interest, implemented in various industrial sectors, including the process industry [4]. However, there are still methodological challenges concerning the functional safety analysis and management in the life cycle. They are related to the issues of potential hardware failures and software faults, common cause failures (CCFs), functional dependencies of equipment and barriers, human errors, organisational factors, security, etc. [6, 7].

The aim of functional safety management is to reduce the risk associated with hazardous installation to an acceptable or tolerable level introducing a set of safety-related functions (SRFs) that are to be implemented using the programmable control and protection systems. The human-operator contributes to realization of given SRF through relevant HMI in relation to the functions of SCADA (*supervisory control and data acquisition*) system or DCS (*digital control system*). In the standard IEC 61511 [4] two kinds of systems are distinguished, namely BPCS (*basic process control system*), and SIS (*safety instrumented system*) designed according to the technical specification and procedures developed for abnormal situations, especially for emergencies [5, 8, 9, 10].

An important term related to the functional safety concept is the *safety integrity* [3], understood as the probability that given safety-related system will satisfactorily perform required SRF under all stated conditions within the given period of time. The *safety integrity level* (SIL) is a discrete level (from 1 to 4) for specifying the safety integrity requirements of given safety-related functions to be allocated using the electrical/ electronic/ programmable electronic system (E/E/PES) [3] or safety instrumented system (SIS) [4]. The safety integrity of level 4 (SIL4) is the highest level, which requires - when implemented in practice – a complex system architecture consisting of redundant subsystems. Their elements are partly diagnosed on-line and partly have to be periodically tested.

For the E/E/PES or SIS performing SRF two probabilistic criteria are defined for consecutive SILs (Tab. 1), namely [3]:
- the average probability of failure PFD_{avg} to perform the safety-related function on demand for the given system operating in a low demand mode, and
- the probability of a dangerous failure per hour *PFH* (the frequency) for the given system operating in a high demand or continuous mode of operation.

Tab. 1. Probabilistic criteria for safety-related functions
Tab. 1. Kryteria probabilistyczne dotyczące funkcji związanych z bezpieczeństwem

SIL	PFD_{avg}	PFH [h^{-1}]
4	[10^{-5}, 10^{-4})	[10^{-9}, 10^{-8})
3	[10^{-4}, 10^{-3})	[10^{-8}, 10^{-7})
2	[10^{-3}, 10^{-2})	[10^{-7}, 10^{-6})
1	[10^{-2}, 10^{-1})	[10^{-6}, 10^{-5})

The SIL for the given SRF is determined in the risk assessment process using a defined risk matrix, which includes areas of several risk classes, *e.g.* unacceptable, moderate and acceptable, or a risk graph [4, 9, 11].

The E/E/PE safety-related system shown in Fig. 1 consists of following subsystems: (A) input devices (sensors, transducers, converters, *etc.*), (B) programmable logic controllers, *e.g.* PLC and (C) output devices including the equipment under control (EUC). The architecture of these subsystems is determined during the design process. Each logic controller comprises the central unit (CPU), input modules (digital or analog) and output modules (digital or analog). The E/E/PE subsystems have usually KooN architecture, *e.g.*, 1oo1, 1oo2, 1oo3 or 2oo3 [1].

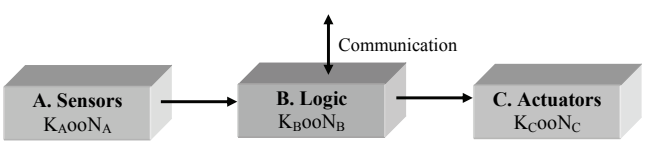

Fig. 1. Architecture of E/E/PES or SIS for realization of safety-related functions
Rys. 1. Architektura systemu E/E/PE lub SID do realizacji funkcji związanych z bezpieczeństwem

3. Layers of protection and dependency problems

3.1. Layers of protection

Hazardous industrial plants are designed according to a concept of *defense in depths* using several barriers (protection layers). Designing of a safety-related system is based on the risk analysis and assessment to determine required safety-integrity level (SIL), which is then verified in the probabilistic modeling process. It is important to include in probabilistic model potential dependencies between events representing equipment failures or human errors [7].

Fig. 2 shows typical layers of protection of in a hazardous industrial plant. An interesting methodology for preliminary risk analysis and safety-related decision-making is the layer of protection analysis (LOPA) methodology [8].

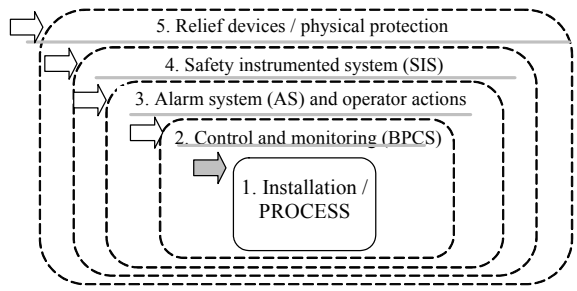

Fig. 2. Typical protection layers in hazardous industrial installation
Rys. 2. Typowe warstwy zabezpieczeń w przemysłowej instalacji podwyższonego ryzyka

The protection layer (PL) should be [8]:
- *effective* in preventing the consequence when it functions as designed,
- *independent* of the initiating event and the components of any other PL already claimed for the same scenario,
- *auditable*, i.e. its effectiveness in terms of consequence prevention and probability of failure on demand (PFD) has to be capable of validation (by documentation, review, testing, etc.).

An active PL generally comprises [11]: a sensor of some type (instrument, mechanical, or human), a decision-making element (logic solver, relay, spring, human, etc.), and an action element (automatic, mechanical, or human).

Fig. 3 illustrates the protection layers that include *Basic Process Control System* (BPCS), *human operators* and *Safety Instrumented System* (SIS). These systems should be functionally and structurally independent; however, it is not always possible in industrial practice.

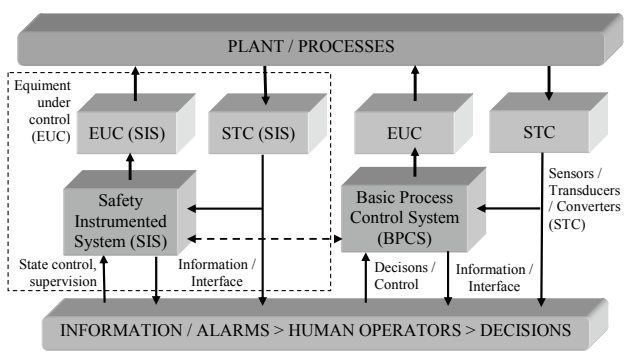

Fig. 3. Components of safety-related systems for monitoring, control and protection
Rys. 3. Elementy systemów związanych z bezpieczeństwem do monitorowania, sterowania i zabezpieczeń

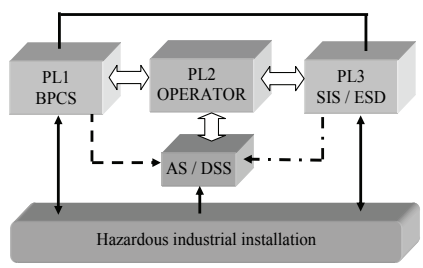

Fig. 4. OPERATOR and alarm system / decision support system (AS/DSS) as elements of protection layers
Rys. 4. OPERATOR i system alarmowy / system wspomagania decyzji (AS/DSS) jako elementy warstw zabezpieczeń

Fig. 4. illustrates potential structural and functional dependencies of three protection layers (PLs): 2, 3 and 4 shown in Fig. 2. These layers include:
- PL1 – *basic process control system* (BPCS),
- PL2 – *human-operator* (OPERATOR), who supervises the process and intervene in cases of abnormal situations or during emergencies that are indicated by an alarm system,
- PL3 – *safety instrumented system* (SIS), which can perform a function of *emergency shutdown* (ESD).

Thus, an important part of such complex system is the human-machine interface (HMI) [2, 7, 12].

The design process of the control and protection systems in a hazardous plant is presented in Fig. 5. It includes preliminary risk analysis and defining safety-related functions, determining the risk mitigation and control strategy, designing BPCS with regard to decision support system (DSS), human-machine interface (HMI) and alarm system (AS).

Selected issues of the alarm system designing were outlined by Kosmowski [7]. The research challenges in this area include man-machine interaction [13], human reliability analysis (HRA) in context [2, 14, 15].

The safety-related functions to be implemented using SIS are designed for given SIL determined during the risk analysis and assessment. The final solution proposed, including algorithms of actions and related software, has to be verified and validated according to requirements and procedures given in IEC 61508 [3] and IEC 61511 [4].

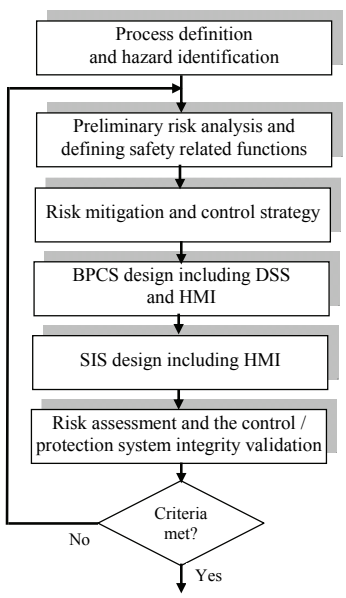

Fig. 5. The design process of programmable control and protection systems
Rys. 5. Proces projektowania programowalnych systemów sterowania i zabezpieczeń

3.2. Trends in safety instrumented solutions and dependency problem

As the users are becoming more knowledgeable about safety issues, they are performing more accurately extensive hazard and risk analysis to determine their needs for the plant protections. To reduce the cost of configuration, training, and technical support, some users consider the possibility of closer integration of the control and protection systems. It includes such aspects as field wiring and gathering diagnostic data from the devices. Thus, the users are looking to employ high-integrity fieldbuses in safety-related applications. Finally, they are interested to have better tools for safety lifecycle management and flexible architectures that enable increased scalability [5].

In the past, most manufacturers required the process control systems to be completely independent from their emergency shutdown systems. Some have even assumed that the BPCS and the SIS have to be supplied from different manufacturers to reduce the possibility of common cause failures (CCF). There were and still are some good reasons to put the safety and control functions in different controllers. They include [3, 5]:
- Avoiding dependent failures to minimize the risk of simultaneous failures within the control systems and protection systems (e.g. BPCS and SIS);
- Increasing security to prevent danger changes in programmable control and protection systems from causing any change or fault in BPCS and SIS;
- Different requirements for BPCS and SIS; a BPCS is usually designed for maximum availability, but a SIS is normally designed to fail in a safe way and has special features like extended diagnostics, software error checking, protected data storage, fault tolerance, etc.

Such advanced solutions are required for instance in nuclear power industry applications, as described in the international standard IEC 61513.

Some new solutions of functional characteristics and relations between BPCS and SIS are being also proposed as shown in Fig. 6. The benefits and challenges concerning the integration of safety-related and control systems are specified in Tab. 2.

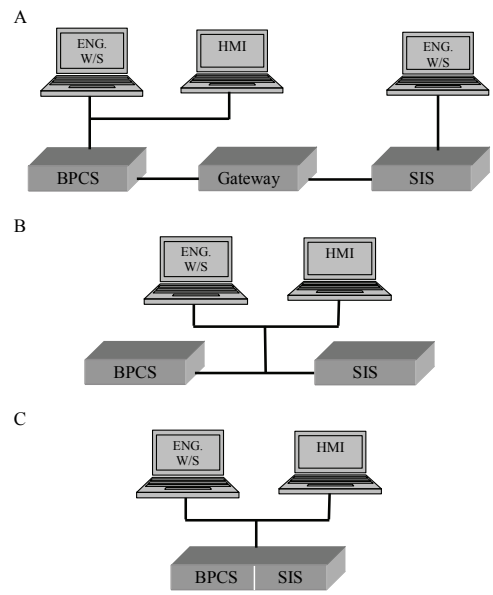

Fig. 6. Integrating of SIS with BPCS [5]: A. Interfaced, B. Integrated, and C. Common
Rys. 6. Integrowanie SIS z BPCS [5]: A. Z interfejsem, B. Zintegrowane, C. Wspólne

Tab. 2. Benefits and challenges concerning the integration of control and protection systems (adapted from [5])
Tab. 2. Korzyści i wyzwania dotyczące integracji systemów sterowania i zabezpieczeń (adaptacja [5])

Benefits	Challenges
- Similar tools - Lower training effort - Common data mapping - Significant reduction in integration efforts - Lower life-cycle and maintenance costs - Presumable more reliable transfer of information and data	- Putting hardware and software barriers between control and protection systems - Ensuring security-related access protections - Ensuring visual differentiation between control and protection environments at workstation level

The integration of the control and safety-related systems may be categorized into three levels: interfaces, integrated, and common [5]. Some suppliers of the control and protection systems offer now similar systems for either functionality, which incorporate similar HMI, configuration procedures, programming languages, and maintenance procedures. The key issue is to ensure that such two systems are separate as regards different hardware and software solutions, even though they have common configuration, operations and maintenance interface.

This allows the users to achieve the operational benefits of integration with some limitations of the safety requirements for separation. The control and protection systems can communicate transparently with each other, with a certain potential to have protection from corruption of one by the other. This allows the safety functions to be designed, reviewed, commissioned and locked in, while non-safety related code can be edited without significant restrictions. Such solutions allow offering any of these three levels of integration, depending on users' preferences. In the example described all three configurations were certified for applications up to SIL 3 [5]. They are characterized in Tab. 3.

Tab. 3. Advantages and drawbacks of BCPS and SIS integration (adapted from ARC, 2005)
Tab. 3. Korzyści i wady integracji BPCS i SIS (adaptacja [5])

Level of Integration	Advantages	Drawbacks
Interfaced	- Significant reduction of common cause failures - Preferred solution for high risk installations	- Higher installation and engineering costs - Additional training and maintenance - Gateway issues
Integrated	- Lower engineering costs - Little additional training and maintenance	- Increased risk of common cause failures - Less reliable alarming
Common	- Installation and engineering costs significantly lower - Little additional training and maintenance	- Reduction in the number of layers of protection - Possibility of failures due to common causes can be significant

3.3. Requirements and criteria concerning the design of protection layers

According to IEC 61511-2 [4] when a safety function is allocated to a safety instrumented system, it will be necessary to consider whether the application is in *demand* or in *continuous mode*. The majority of applications in the process sector operate in demand mode where demands are infrequent. Continuous mode applications, when failure would result in an immediate hazardous event, are usually rare. The targets for PFD_{avg} or *PFH* apply respectively for the mentioned cases to the safety instrumented function (see Tab. 1).

Multiple SISs may be utilized in order to achieve higher levels of risk reduction, for instance greater than 10^3. When using multiple SISs to achieve higher risk reduction, it is important that each of the SISs is independently able to carry out the safety function and that there is sufficient independence between SISs. For determining the number of IPL the use of a safety layer matrix can be used [4, 8]. An example of such a matrix is shown in Fig. 7.

Furthermore, where multiple SISs are used, one should take into account common cause failures (CCFs). CCFs such as using similar technologies, designing both systems from the same functional specification, human factors (programming, installation and maintenance), external factors (corrosion, plugging, freezing of air lines) will limit significantly the system improvement. It is necessary to take into consideration any component shared between the two or more systems.

There are also in IEC 61511 requirements concerning the BPCS as a protection layer. The BPCS may be identified as a protection layer subject to certain conditions. If functions are implemented within the BPCS for the purpose of reducing identified process risks, for each function a relevant risk reduction has to be allocated. When allocating risk reduction to functions within the BPCS, it is important to ensure that the access security and relevant change management are provided. The risk reduction that can be claimed for a BPCS function can be also determined by the degree of independence between the BPCS function and initiating events [5, 10].

When a CCF problem is identified, then the following actions can be considered [4]:
- The CCF can be reduced by changing the design of the SIS and/or the BPCS. Diversity of design and physical separation are two effective methods of reducing the likelihood of CCFs. It is often preferred approach.
- The likelihood of a common cause event should be taken into account when determining whether the overall risk reduction is adequate.

It should be noted that any sensors or actuators which are shared by the BPCS and SIS are very likely to introduce CCFs and such a solution has to be avoided.

The quantitative risk matrix can be used for evaluation of the risk reduction by combining the likelihood and the impact severity rating of hazardous events [8]. A similar approach can be applied to develop a safety layer matrix that indicates potential risk reduction by using a number of protection layers. Such matrix is shown in Fig. 7. It should be scaled and verified for industrial installation considered.

Number of PLs	Safety integrity level (SIL) required								
3	C	C	C	C	C	C	C	SIL1	SIL1
2	C	C	SIL1	C	SIL1	SIL2	SIL1	SIL2	SIL3 B
1	SIL1	SIL1	SIL2	SIL1	SIL2	SIL3 B	SIL3 B	SIL3 B	SIL3 A
Hazardous event likelihood	*Low*	*Med.*	*High*	*Low*	*Med.*	*High*	*Low*	*Med.*	*High*
	Minor			Serious			Extensive		
	Hazardous event severity rating								

A. One level SIL3 safety instrumented function does not provide sufficient risk reduction at this risk level. Additional modifications are required in order to reduce risk. Combining the BPCS and SIS is not appropriate.
B. One level SIL3 safety instrumented function does not provide sufficient risk reduction at this risk level. Additional review is required. Combining the BPCS and SIS is not appropriate.
C. SIS independent protection layer is probably not needed.

Fig. 7. Example of a safety layer matrix (adapted from [4])
Rys. 7. Przykład matrycy warstw zabezpieczeń (adaptacja [4])

The total number of PLs includes all protection layers including the BPCS and SISs. The estimated likelihood of hazardous events should be reduced by a factor at least of 10 for every PL. In the LOPA methodology [8] an approach is suggested for specifying a number of IPL credits for scenarios of the distinguished consequence levels and their frequencies. Typically, tabular values are provided for the number of independent protection layers (IPLs) required for ranges of initiating event frequency and for credit values for various kinds of protection layers. Tab. 4 illustrates such approach that can be useful in practice, especially during preliminary analyses.

Similar tables could be also developed for other types of consequences, such as the production losses or environmental impact. Expert judgement is needed when specific risk tolerance criteria are not available or not easily established due to the specific process being analysed or hazards involved. Cost-benefit analysis is suggested to be performed in practice for safety-related decision making under uncertainties with regard to functional safety solutions considered [1].

Tab. 4. Example of IPL credit requirements [8]
Tab. 4. Przykład of uznaniowych wymagań dotyczących IPL [8]

Adjusted initiating event frequency **(*f*)	Number of IPL credits required *	
	Consequence Category IV *One fatality*	Consequence Category V *Multiple fatalities*
$10^{-2} \le f$	2	2,5
$10^{-3} \le f < 10^{-2}$	1,5	2
$10^{-4} \le f < 10^{-3}$	1	1,5
$10^{-6} \le f < 10^{-4}$	0,5	1
$f < 10^{-6}$	0	0,5

* Includes adjustments to the initiating event frequency for probabilities of ignition, person present and fatality
** IPL credit is defined as a reduction in hazardous event frequency by a factor of 10^{-2}

3.4. Remarks concerning protection layers and combined systems

Since the issue of IEC 61511 [4] the assessment of risks and appropriate implementation of protection layers are still subjects of discussions in scientific literature and reports. It is worth mentioning that there has been a great deal of misunderstanding related to current requirements for separation of the BPCS from the SIS. There are situations in practice when employing safety-related functionality into the BPCS is justified. Some of existing solutions were specified and named by Marszal & Weil [10] as:

- *Courtesy Action;*
- *Mimic Action;*
- *BPCS - Only Protective Function;*
- *Pre-Emptive Strike;*
- *Additional (Non-Safety Critical) Inputs.*

The benefits of combined systems have been extensively analysed and promoted by some designers and manufactures. The integrity requirements for combined systems are obviously extremely high because there are potential failure modes that would simultaneously generate a hazard and disable multiple protection layers.

Fig. 8 illustrates a diagram of the BPCS and SIS designed to function according to the rules of *Courtesy Action* [10]. The action taken by the BPCS on a final element, controlled by the BPCS, is in similar service as a SIS final element being on command from the SIS. These actions focus on equipment associated functionally with the SIF controlled by the SIS, but are non-safety critical.

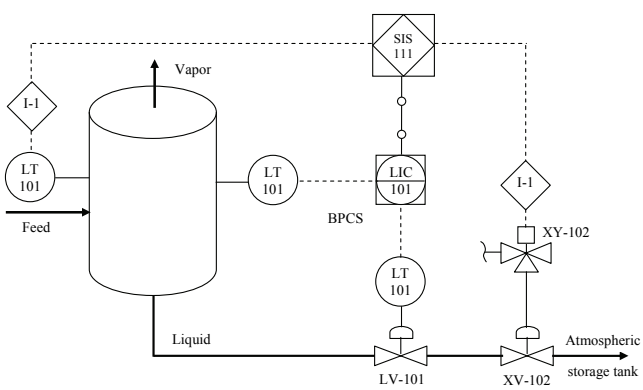

Fig. 8. Example of BPCS and SIS designed to operate as *Courtesy Action*
Rys. 8. Przykład BPCS i SIS zaprojektowanych do działania wspomagającego

The industry guidance concerning separation requirements of these systems is abundant, but not always clear. One can argue that the most recent standards allow the use of combined SIS-BPCS system, if the logic solver used meets the higher requirements of the SIS. While this may seem appropriate, it should not be undertaken without full understanding of the requirements given in the mentioned standards and awareness of the necessity to increase the scope of analyses and assessments for combined functional and structural solutions.

Guidelines [11] define separation as physical and functional isolation of all hardware and software elements. *Physical separation* is defined as the requirement that the BPCS and the SIS functions will be performed using different logic solvers. *Functional separation* is achieved through elimination of CCFs in execution of the BPCS and SIS functions. This may require the separation of BPCS and SIS sensors, final elements, I/O components, and logic solvers, the software operating systems, and the application programs. Some communications may be allowed between separate components as long as no common mode failures can occur.

Thus, there are strict requirements to carry out additional analyses to develop a list of all scenarios under which a combination of SIS and BPCS could result in a single failure that will simultaneously create a demand on the SIS and also prevent it from being able to take action. Such analyses should be performed by completing the following steps [10, 11]:

A. Prepare a list of SIFs to be implemented by the combined control system. The SIF list will contain a description of the action taken by the system along with all inputs and outputs of the function that are safety relevant.
B. Analyze each SIF to determine all of the initiating events that can place a demand on the SIF. When BPCS function failures can place a demand on the SIF, the field equipment (sensors and final elements) are reviewed to ensure that the BPCS field equipment is completely separate from the SIF field equipment (including I/O cards). If any commonality of equipment is identified, recommendations should be prepared and implemented to separate the functions.
C. Determine for each SIF the extent of *shared equipment*, which is expected to include the logic solver CPU, and quantitatively verify that the risk posed by failure of *shared equipment* is tolerable.
D. Review potential impact of systematic programming failures using relevant methods to prevent systematic failures by functionally separating the logic solver application programming.
E. Ensure that the CPU logic solver is designed to the highest SIL of any functionality to be implemented by the logic solver (presumably SIL 3).
F. Ensure that the overall risk of scenarios where the BPCS-SIS failure that will directly lead to a consequence is sufficiently low.

If for example shown in Fig. 8 the hazardous event severity rating would be “Extensive”, then according to Fig. 7 combining the BPCS and SIS would not be appropriate. When the risk reduction requirement concerns three protection layers (as shown in Fig. 4) the required risk reduction should be properly distributed between BPCS, OPERATOR and SIS, e.g. if for *i*-th initiating event $PFD_i = 10^{-4}$ for all layers then it should be distributed respectively as: 10^{-1} (SIL1), 10^{-1} (HEP) and 10^{-2} (SIL2), which are values achievable in industrial practice for not very dynamic process response.

However, only in case of independence of these layers the frequency of *i*-th accident scenario F_i can be calculated from the formula

$$F_i = F_i^I \cdot PFD_{i;PL1} \cdot PFD_{i;PL2} \cdot PFD_{i;PL3} = F_i^I \cdot PFD_i \qquad (1)$$

where F_i^I is the frequency of *i*–th initiating event [a^{-1}] and $PFD_{i;PLj}$ are probabilities of failure on demand of *j*-th protection layer shown in Fig. 4. For the second layer $PFD_{i;PL2} = HEP_{i;PL2}$ and relevant HEP (*human error probability*) is to be evaluated using appropriate HRA method [7].

Generally, the frequency reduction of accident scenarios for the layers considered should be evaluated using relevant formula consisting of conditional probabilities

$$F_i^D = F_i^I \cdot P(X_{i;PL1} \mid I) \cdot P(X_{i;PL2} \mid I \cdot X_{i;PL1}) \cdot P(X_{i;PL3} \mid I \cdot X_{i;PL1} X_{i;PL2}) = F_i^I \cdot PFD_i^D \quad (2)$$

where: $X_{i;PLj}$ denote events that represent failures in performing safety-related functions on demand by consecutive protection layers *PLj* (j = 1, 2, 3) that should be considered for *i*-th initiating event.

The results of several analyses have shown that assuming dependencies of layers in probabilistic modeling significantly increases the failure probability on demand at least an order of magnitude, thus $PFD_i^D >> PFD_i$ - see formulas (1) and (2). In the example above when BPCS and SIS are integrated then due to dependency $PFD_i^D \cong 10^{-3}$ and required risk reduction is not fulfilled.

Significant meaning in reducing dependencies of the mentioned layers has appropriate design of the alarm system and decision support system as well as the quality of HMI characterized by relevant factors that should be assessed when performing the HRA, using e.g. the SPAR-H [15] method. Some proposals concerning solutions of the described above issues were proposed by Kosmowski [7].

4. Conclusions

In this paper selected design issues of protection layers including BPCS and SIS have been outlined. Potential dependencies between these systems are indicated and some warnings concerning the integration of BPCS and SIS as protection layers within an industrial computer network are delivered. The proposals from some hardware and software producers to apply in practice integrated solutions of BPCS and SIS are critically discussed to some extent. It is emphasized that the decision concerning final solution should be based on careful assessments of risks and detailed functional analysis of these systems with regard to requirements and criteria given in relevant standards, especially in the context of CCF (*common cause failure*) analysis and evaluation of potential human errors.

The publication has been worked out on the basis of II stage of a long-term programme "Improvement of safety and work conditions", financed in years 2011 - 2013 in the frame of scientific research and development works from financial resources of the Ministry of Science and Higher Education / National Center for Research and Development.

Programme coordinator: Central Institute for Labour Protection – State Research Institute.

Publikacja opracowana na podstawie wyników II etapu programu wieloletniego „Poprawa bezpieczeństwa i warunków pracy", finansowanego w latach 2011-2013 w zakresie badań naukowych i prac rozwojowych ze środków Ministerstwa Nauki i Szkolnictwa Wyższego / Narodowego Centrum Badań i Rozwoju.

Koordynator programu: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.

5. References

[1] Kosmowski K.T. (Ed.): Functional Safety Management in Critical Systems (Ed). Gdansk University of Technology. Wydawnictwo Fundacji Rozwoju Uniwersytetu Gdańskiego. Gdańsk 2007.

[2] Kosmowski K.T.: Safety management problems of a hazardous industrial plant (in Polish), in: Z. Kowalczuk (Ed.), Diagnosis of Processes and Systems. PWNT, Gdańsk 2009: 181-190.

[3] IEC 61508: Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems, Parts 1-7. International Electrotechnical Commission. Geneva 2010.

[4] IEC 61511: Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva 2003.

[5] Siemens' Process Safety Systems Deliver Modern Features on a Proven Platform. White paper. ARC Advisory Group. ARCweb.com 2005.

[6] Kosmowski K.T.: Functional Safety Concept for Hazardous System and New Challenges. Journal of Loss Prevention in the Process Industries 19(1) 2006: 298-305.

[7] Kosmowski K.T.: Functional Safety Analysis including Human Factors. International Journal of Performability Engineering 7 (1), 2011: 61-76.

[8] Layer of Protection Analysis, Simplified Process Risk Assessment. Center for Chemical Process Safety. American Institute of Chemical Engineers, New York 2001.

[9] Missala T.: The analysis of requirements and conducting methods for the risk assessment and determining required safety integrity level (in Polish). Oficyna Wydawnicza PIAP, Warszawa 2009.

[10] Marszal, E.M., Weil, Ch.P.: Implementing Protective Functions in BPCS and Combined Systems. Kenexis Consult. Corporation, Columbus 2011.

[11] Guidelines for Safe Automation of Chemical Processes. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York 1993.

[12] EEMUA, Publication 191: Alarm Systems, A Guide to Design, Management and Procurement (Edition 2). The Engineering Equipment and Materials Users' Association, London 2007.

[13] Hollnagel E.: The reliability of man-machine interaction. Reliability Engineering and System Safety 38(1-2), 1992: 81-89.

[14] Hollnagel E.: Human reliability assessment in context. Nuclear Engineering and Technology 37(2), 2005: 159-166.

[15] SPAR-H, Human Reliability Analysis (HRA) Method, NUREG/CR-6883, INL/EXT-05-00509, US NRC 2005.

otrzymano / received: 03.09.2011
przyjęto do druku / accepted: 03.10.2011 *artykuł recenzowany*

INFORMACJE

Informacja redakcji dotycząca artykułów współautorskich

W miesięczniku PAK od numeru 06/2010 w nagłówkach artykułów współautorskich wskazywany jest autor korespondujący (Corresponding Author), tj. ten z którym redakcja prowadzi wszelkie uzgodnienia na etapie przygotowania artykułu do publikacji. Jego nazwisko jest wyróżnione drukiem pogrubionym. Takie oznaczenie nie odnosi się do faktycznego udziału współautora w opracowaniu artykułu. Ponadto w nagłówku artykułu podawane są adresy korespondencyjne wszystkich współautorów.

Wprowadzona procedura wynika z międzynarodowych standardów wydawniczych.

Redakcja