Journal of KONBiN 3(6)2008
ISSN 1895-8281

DOI 10.2478/v10040-008-0074-y

HUMAN RELIABILITY ANALYSIS IN THE CONTEXT OF ACCIDENT SCENARIOS

ANALIZA NIEZAWODNOŚCI CZŁOWIEKA W KONTEKŚCIE SCENARIUSZY AWARYJNYCH

Kazimierz T. Kosmowski

Gdansk University of Technology, Faculty of Electrical and Control Engineering
Politechnika Gdańska, Wydział Elektrotechniki i Automatyki
G.Narutowicza 11/12, 80-952 Gdańsk

k.kosmowski@ely.pg.gda.pl

Abstract: This article addresses the issue of human reliability analysis (HRA) in the context of accident scenarios. The need for contextual analysis of human operator behavior with careful treating of errors and dependent failures within given accident scenario is emphasized. The functional safety analysis including the human reliability analysis is illustrated on example of the protection layers of a hazardous industrial system that includes the basic process control system (BPCS), human-operator (HO) and safety instrumented systems (SIS) designed with regard to the functional safety criteria.

Keywords: human reliability analysis, functional safety

Streszczenie: Niniejszy artykuł przedstawia zagadnienie analizy niezawodności człowieka (HRA) w kontekście scenariuszy awaryjnych. Podkreślono potrzebę kontekstowej analizy zachowania człowieka ze starannym traktowaniem błędów i uszkodzeń zależnych w rozważanym scenariuszu awaryjnym. Analizę bezpieczeństwa funkcjonalnego z uwzględnieniem oceny niezawodności człowieka zilustrowano na przykładzie warstw zabezpieczeń przemysłowego systemu podwyższonego ryzyka, który obejmuje główny system sterowania procesu (BPCS), człowieka-operatora (HO) i przyrządowe systemy bezpieczeństwa (SIS) zaprojektowane z uwzględnieniem kryteriów bezpieczeństwa funkcjonalnego.

Słowa kluczowe: analiza niezawodności człowieka, bezpieczeństwo funkcjonalne

HUMAN RELIABILITY ANALYSIS IN THE CONTEXT OF ACCIDENT SCENARIOS

1. Introduction

The research works concerning causes of industrial accidents indicate that broadly understood human errors, resulting from organisational inadequacies, are determining factors in 70-90% of cases, depending on industrial sector and the system category. Because several defences against potential accidents are usually used in hazardous systems to protect people and environment, it is clear that multiple faults have contributed to most of accidents.

It has been emphasized that accidents arose from a combination of latent and active human errors committed during the design, operation and maintenance [5, 14]. The characteristic of latent errors is that they do not immediately degrade the safety-related functions, but in combination with other events, such as random equipment failures, external disturbances or active human errors, can contribute to major accident with serious consequences. Some categorizations of human errors have been proposed, e.g. by Swain & Guttmann [20] and Reason [19].

Traditionally, the human and organisational influences are incorporated into the probabilistic models through the failure events with their probabilities evaluated using relevant method of human reliability analysis (HRA) [3, 4, 6, 11]. Careful evaluation of expected human behaviour (including context oriented diagnosis, intention and action) and potential errors is an essential prerequisite of correct risk assessment and rational safety-related decision making in the safety management process [10, 22]. The probabilities of these failure events significantly depend on various influencing factors including human and organisational factors [3, 15, 16].

Lately some approaches have been proposed by Carey [2], Hickling et al. [9] and Kosmowski [19] how to deal with the issues of human factors in the functional safety management [12, 13]. The human errors can be committed in entire life cycle of the system, from the design stage, installation, commissioning, and its operation to decommissioning. In operation time the human-operator interventions include the control actions during transients, disturbances, faults as well as the diagnostic activities, the functionality and safety integrity tests, maintenance actions and repairs after faults [17, 18].

The operators supervise the process and make decisions using the operator support system (OSS), which should be designed carefully for abnormal situations and accidents, also for cases of partial faults and dangerous failures within the electric, electronic and programmable electronic (E/E/PE) systems [12] or the safety instrumented systems (SIS) [13]. The OSS when properly designed will contribute to reducing the human error probability and the risk of potential accidents. The paper emphasizes the importance of human reliability analysis in the context of functional safety management.

2. Human reliability analysis in the context of functional safety

2.1. Safety integrity levels and probabilistic criteria

Modern industrial systems are extensively computerised and equipped with complex programmable control and protection systems. In designing of the control and protection systems a functional safety concept [12] is more and more widely implemented in various industrial sectors, e.g. the process industry [13].
The aim of functional safety management is to reduce the risk of a hazardous system to the acceptable or tolerable level introducing a set of safety-related functions (SRFs) to be implemented using the programmable control and/or protection systems. Human-operator (HO) contributes to realization of given SRF according to the technical specification. However, there are still methodological challenges concerning the functional safety management in life cycle [17].
An important term related to the functional safety concept is the *safety integrity* [12], understood as the probability that given safety-related system will satisfactorily perform required SRF under all stated conditions within a given period of time. The *safety integrity level* (SIL) is a discrete level (1÷4) for specifying the safety integrity requirements of given safety function to be allocated using the E/E/PE system or SIS. The safety integrity level of 4 (SIL4) is the highest level, which require a redundant architecture of E/E/PE system consisting of subsystems diagnosed and periodically tested.
For consecutive SILs two probabilistic criteria are defined [12], namely:
- the average probability of failure to perform the safety-related function on demand (PFD_{avg}) for the system operating in a low demand mode, and
- the probability of a dangerous failure per hour *PFH* (the frequency) for the system operating in a high demand or continuous mode of operation.

The interval probabilistic criteria for the safety-related functions to be implemented using E/E/PE systems are presented in Table 1. Similar interval criteria also used in assessments of SIS [13].

Table 1. Probabilistic criteria for safety functions [12]

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 given SRF is determined in the risk assessment process for defined risk matrix, which includes areas of several risk categories, e.g. unacceptable, moderate and acceptable [18, 19].
Verifying SIL for given safety-related function to be implemented using the E/E/PE or SIS system is usually a difficult task due to scarcity of reliability data and other data used as parameters in probabilistic models of the system in design. In such situation, a qualitative method for crude verifying of SIL is permitted in IEC 61508 for the system architectures to be considered at the design stage.

2.2. The influence factors in human reliability analysis

The human reliability analysis (HRA) methods are used for assessing the risks resulting from potential *human errors*, and for reducing the system vulnerability, operating in given environment, widely understood. However, some basic assumptions made in HRA methods used within probabilistic safety analysis of hazardous systems are still the subjects of dispute between researchers [10].
Practically all HRA methods assume that it is meaningful to use the concept of human errors and it is justified to estimate their probabilities. Such point of view is sometimes questioned due to not fully verified assumptions about human behaviour and potential errors. Hollnagel [10] concludes that some HRA results are of limited value as an input for PSA, mainly because of oversimplified conception of human performance and human error. There is no doubt, however, that potential human errors should be considered in given context (process dynamic, automation, MMI). Examples of human errors and their consequences are presented in Figure 1.

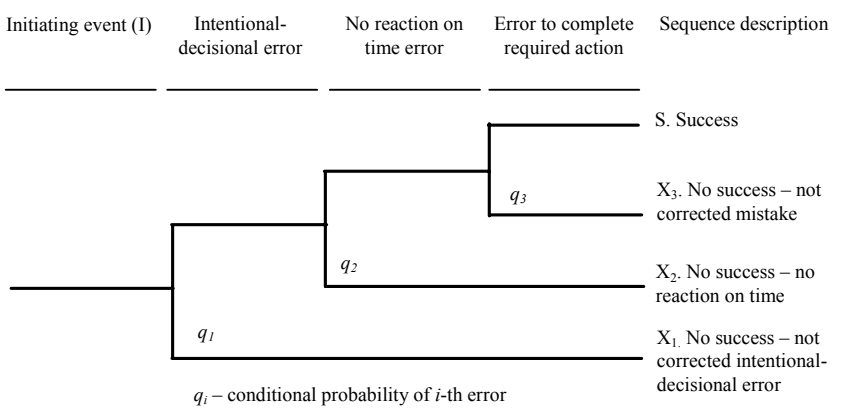


Figure 1. Examples of human-operator errors and their consequences

In spite of mentioned criticism, waiting for a next generation of HRA methods, the human factor analysts use in PSA several exiting HRA methods. Below selected HRA methods are shortly characterized, which can be applied within the functional safety analysis. The rough human reliability assessments based on qualitative information with regard to human factors can be especially useful for initial decision making at the designed stage of the safety-related functions and systems [18]. It will be demonstrated that the functional safety analysis framework, including the control & protection systems and assumed MMI (Man-Machine Interface) solutions, gives additional insights in performing HRA.

Several traditional HRA methods have been often used in PSA practice, particularly the THERP method [20], developed for the nuclear industry, but applied also in various industrial sectors. Other HRA methods, more frequently used in industrial practice are: Accident Sequence Evaluation Procedure-Human Reliability Analysis Procedure (ASEP-HRA), Human Error Assessment and Reduction Technique (HEART), and Success Likelihood Index Method (SLIM) - see the description and characterization of these methods in reports [3, 11].

In the publication [1] five HRA methods were selected for comparison on the basis of either relatively widespread usage, or recognized contribution as a newer contemporary technique:

- Technique for Human Error Rate Prediction (THERP);
- Accident Sequence Evaluation Program (ASEP);
- Cognitive Reliability and Error Analysis Method (CREAM);
- Human Error Assessment and Reduction Technique (HEART);
- Technique for Human Event Analysis (ATHEANA).

In addition to these methods, other sources of information were also examined to provide insights concerning the treatment and evaluation of human errors. Comparisons were made with regard to the SPAR-H method [7]. The final conclusion is that the enhanced SPAR-H methodology is useful as an easy-to-use, broadly applicable, HRA screening tool.
The human error probability (HEP) is evaluated when the human failure event is placed into the probabilistic model structure of the system. In the HRA within PSA only more important human failure events are considered [14, 16]. Then, the context related performance shaping factors (PSFs) are specified and determined according to rules of given HRA method. As the result the particular value of HEP is evaluated.
Different approaches are used for evaluating HEP with regards to PSFs, e.g. assuming a linear relationship for each identified PSF_k and its weight w_k, with constant C for the model calibration

$$HEP = HEP_{nominal} \sum_k w_k PSF_k + C \tag{1}$$

or nonlinear relationship used in the SPAR-H methodology [7]

$$HEP = \frac{NHEP \cdot PSF_{composite}}{NHEP(PSF_{composite} - 1) + 1} \tag{2}$$

where: NHEP is the nominal HEP; the NHEP equals 0.01 for diagnosis, and NHEP equals 0.001 for action.

3. Human factors and layers of protection analysis

Industrial hazardous plants are nowadays designed according to a concept of *defense in depths*, distinguishing several protection layers. The design of safety-related systems is based on the risk assessment for determination of required SIL and its verification in the process of probabilistic modeling [8, 18]. A simplified methodology for preliminary risk analysis and safety-related decision making is the *layer of protection analysis* (LOPA) methodology [20].
An active independent protection layer (IPL) generally comprises following components:
- A - a sensor of some type (instrument or human as sensor),
- B - a decision-making element (logic solver, relay, human, etc.),
- C - an action (automatic, mechanical, or human).

The IPL can be designed as a *basic process control system* (BPCS) or SIS. These systems should be functionally and structurally independent; however, it is not always possible in practice. Figure 2 illustrates the functional relationships of three protection layers: BPCS, *human operator* (HO) and SIS. An important part of such complex system is the *man-machine interface* (MMI) [6, 8]. Its functionality in abnormal system states and design quality are often included as important PSFs in HRA [6, 14].

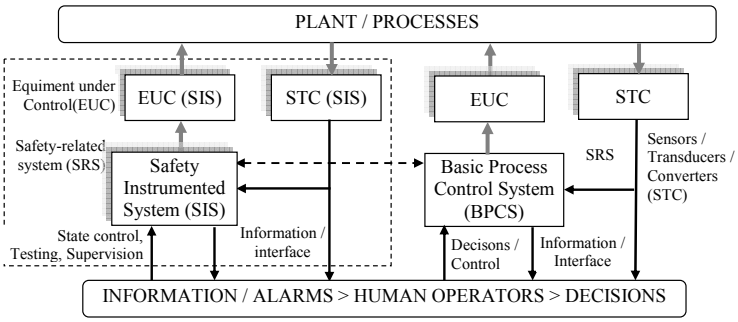


Figure 2. The control and protection systems as layers in hazardous plant

The protection layers from Figure 2 are shown in Figure 3. They include:
- PL1 – basic process control system (BPCS),
- PL2 – human-operator (HO),
- PL3 – safety instrumented system (SIS).

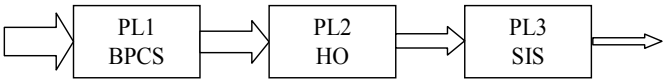


Figure 3. Protection layers for reducing the frequency of accident scenarios

These protection layers should be treated generally as dependent. The frequency of *i*-th accident scenario F_i^{PLs} is calculated taking into account the conditional probabilities of PFD, resulting in a higher value of the frequency then in the case of independency

$$F_I^{PLs} = F_i^I PFD_i^{PL1} PFD_i^{PL2} PFD_i^{PL3} = d \cdot F_i^{IPLs} \tag{3}$$

The value of coefficient d can be much higher than 1 (even an order of magnitude) if independency of protection layers (*IPL*) would be assumed with the frequency F_i^{IPLs} of accident scenario. The value of d is

significantly influenced by assumptions concerning probabilistic modeling of dependent failures due to equipment failures and/or human errors [19].

4. A case study of the layer of protection analysis

Two safety-related systems are considered below: a turbine control system (TCS) and a turbine protection system (TPS). These systems perform an important safety-related function to close the relevant valves and shut down a turbine set of the electrical power unit in situations of disturbances. Failures of these systems can lead to very serious consequences.
The TCS operates in a continuous mode of operation and TPS is the system operating in a low demand mode (see item 2.1). These systems are designed with regard to required SIL, determined in the process of risk assessment. It was evaluated that the risk should be lowered by factor 10^{-4} (equivalent to SIL4) using TCS and TPS, treated as first and third barrier (see Fig. 3). Between these layers there is a second barrier is situated: Human-Operator (HO) (see Fig. 4).

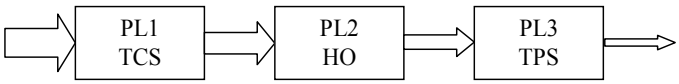


Figure 4. Protection layers reducing the frequency of accident scenario

Preliminary results of the functional safety analysis of TCS indicate that assumed architecture ensures the safety integrity level SIL1. This low level is mainly due to the safety integrity of subsystem C (a control valve V-TCS) evaluated on the level of SIL1 (Fig. 5). The subsystem A (sensor, transducer or converter - STC) contributes less significantly to the result obtained (SIL2) and the contribution to PFD_{avg} of subsystem B (E/E/PES) is low because of SIL3.

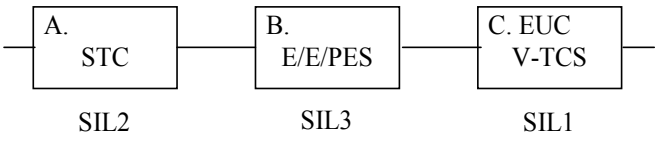


Figure 5. Subsystems of the turbine control system (TCS)

The TPS ensures the safety integrity level 2 (SIL2), as it can be seen in Figure 6. It is mainly due to SIL of subsystem C (a control valve V-TPS) evaluated as SIL2. Subsystem A (sensor, transducer or converter)

contributed less significantly (SIL2) and the contribution of subsystem B (E/E/PES) to the PFD_{avg} is low (SIL3).

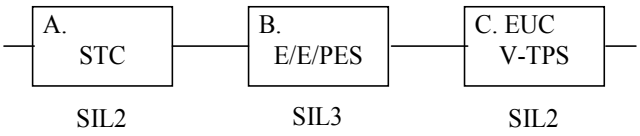


Figure 6. Subsystems of the turbine protection system (TPS)

Resulting safety integrity levels of protection layers are shown in Figure 7. Due to significant dynamic of the system for most initiating events, and a high dependency of human actions, the human error probability was evaluated (with regard to three methods: THERP, HEART and SPAR-H) as high, close to 1 (HEP ≈ 1). Therefore, the risk reduction by TCS and TPS is only on the level of 10^{-3} (SIL1 & SIL2).
Thus, the risk reduction required at level of 10^{-4} is not met and the design improvements have to be considered. The analysis has shown that it is not possible at reasonable costs to make a higher SIL of TCS (from SIL1 to SIL2). Therefore other design option was taken into account to make higher SIL of TPS (from SIL2 to SIL3 – see right block in Fig. 7).

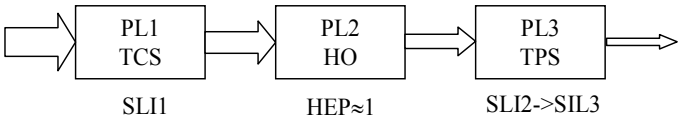


Figure 7. Final safety integrity levels in protection layers of the turbine shut-down system

It is proposed to make higher SIL of TPS by increasing SIL of subsystem A from SIL2 (see Fig. 6) to SIL3 and subsystem C from SIL 2to SIL3. In subsystem A the architecture 2oo3 is proposed to lower PFD_{avg} and to lower frequency of TPS spurious operation. For increasing SIL of subsystem C it is not justified to implement 1oo2 structure due to too high costs of valves. Therefore, relevant organisational aspects (the selection of a high quality valve and proper testing strategy of the shut-down valve) must be considered to meet requirements related to SIL3.

5. Conclusions

The functional safety oriented framework offers additional possibilities for more comprehensive HRA analysis with emphasis on contextual human-operator behaviour in abnormal situations, also those related to the safe and danger failures of the control and protection programmable equipment. Such analysis provides understanding how to design the safety-related functions to be implemented by means of the basic process control system (BPCS), human-operator (HO) and the safety instrumented systems (SISs) with regard to probabilistic criteria defined for distinguished safety integrity levels (SILs). Additional research is needed to obtain more comprehensive insights concerning the influence of human factors in the context of safety-related functions to be designed using the programmable control and protection systems.

References

1. Byers J.C., Gertman D.I., Hill S.G., Blackman H.S., Gentillon C.D., Hallbert, B.P. & Haney, L.N.: *Simplified Plant Risk (SPAR) Human Reliability Analysis (HRA) Methodology: Comparisons with Other HRA Methods*. INEEL/CON-00146. International Ergonomics Association and Human Factors & Ergonomics Society Annual Meeting, 2000.
2. Carey M.: *Proposed Framework for Addressing Human Factors in IEC 61508*. Prepared for Health and Safety Executive (HSE). Contract Research Report 373. Amey Vectra Ltd., Warrington, 2001.
3. *Critical Operator Actions – Human Reliability Modeling and Data Issues*. Nuclear Safety, NEA/CSNI/R(98)1. OECD Nuclear Energy Agency, 1998.
4. Dougherty E.M. & Fragola J.R.: *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*. A Wiley-Interscience Publication, John Wiley & Sons Inc., New York 1988.
5. Embrey D.E.: *Incorporating Management and Organisational Factors into Probabilistic Safety Assessment*. Reliability Engineering and System Safety 38, 1992 (199-208).
6. Gertman I.D. & Blackman H.S.: *Human Reliability and Safety Analysis Data Handbook*. A Wiley-Interscience Publication. New York 1994.
7. Gertman D., Blackman H., Marble J., Byers J. & Smith C.: *The SPAR-H Human Reliability Analysis Method*. NUREG/CR-6883, INL/EXT-05-00509. Idaho National Laboratory, Idaho Falls, 2005.
8. *Guidelines for Safe Automation of Chemical Processes*. American Institute of Chemical Engineers, Center for Chemical Process Safety. New York, 1993.
9. Hickling E.M., King A.G. & Bell R.: *Human Factors in Electrical, Electronic and Programmable Electronic Safety-Related Systems*. Vectra Group Ltd. Warrington, 2006.

10. Hollnagel E.: *Human reliability assessment in context*. Nuclear Engineering and Technology, Vol.37 (2) 2005 (159-166).
11. Humphreys P.: *Human Reliability Assessors Guide*. Safety and Reliability Directorate. Wigshaw Lane,1988.
12. IEC 61508: *Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems*. Parts 1-7. International Electrotechnical Commission. Geneva, 2000.
13. IEC 61511: *Functional safety: Safety Instrumented Systems for the Process Industry Sector*. Parts 1-3. International Electrotechnical Commission. Geneva, 2003.
14. Kosmowski K.T.: *Issues of the human reliability analysis in the context of probabilistic studies*. International Journal of Occupational Safety and Ergonomics. Vol.1(3) 1995 (276-293).
15. Kosmowski K.T., Kwiesielewicz M.: *Hierarchical influence diagrams for incorporating human and organisational factors In risk assessment of hazardous industrial systems.* Risk Decisions and Policy, Vol 7, 2002 (25-34).
16. Kosmowski K.T.: *Incorporation of human and organizational factors into qualitative and quantitative risk analyses*. Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM 7- ESREL'04). Springer, Vol.3 (2048-2053). Berlin, 2004.
17. Kosmowski K.T.: *Functional Safety Concept for Hazardous System and New Challenges*. Journal of Loss Prevention in the Process Industries Vol. 19, 2006 (298-305).
18. Kosmowski K.T., Śliwiński M. & Barnert T.: *Methodological Aspects of Functional Safety Assessment*. Journal of Machines Operation and Maintenance (ZEM, Polish Academy of Science), Vol. 41 (148), 2006 (158-176).
19. Kosmowski K.T. (ed.): *Functional Safety Management in Critical Systems*. Gdansk University of Technology. Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdansk, 2007.
20. *Layer of Protection Analysis, Simplified Process Risk Assessment*. American Institute of Chemical Engineers, Center for Chemical Process Safety. New York, 2001.
21. Reason J.: *Human Error*. Cambridge University Press, 1990.
22. Swain A.D. & Guttmann H.E.: *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application*. NUREG/CR-1278, 1983.

ANALIZA NIEZAWODNOŚCI CZŁOWIEKA W KONTEKŚCIE SCENARIUSZY AWARYJNYCH

1. Wstęp

Badania dotyczące przyczyn awarii przemysłowych wskazują, że szeroko rozumiane czynniki ludzkie, wynikające z niedociągnięć organizacyjnych, są decydującymi czynnikami 70-90% przypadków, zależnie od sektora przemysłowego i kategorii systemu. Ponieważ stosuje się zwykle szereg środków zapobiegania potencjalnym awariom, aby ochraniać ludzi i środowisko, jest bezsporne, że do większości awarii przyczyniły się wielokrotne uszkodzenia i błędy.

Podkreśla się, że awarie powstają w wyniku kombinacji utajonych i aktywnych błędów człowieka popełnionych podczas projektowania, eksploatacji i obsługi [5, 14]. Charakterystyką błędów utajonych jest, że nie powodują one degradacji funkcji związanych z bezpieczeństwem natychmiast, ale w kombinacji z innymi zdarzeniami, takimi jak losowe uszkodzenia wyposażenia, zakłócenia zewnętrzne lub aktywne błędy człowieka, i mogą przyczynić się do powstania dużej awarii z poważnymi skutkami. Klasyfikacje błędów człowieka były proponowane, m.in. przez Swaina i Guttmanna [20] oraz Reasona [19].

Tradycyjnie wpływ czynników ludzkich i organizacyjnych jest włączany do modeli probabilistycznych poprzez zdarzenia związane z uszkodzeniami wraz z ich prawdopodobieństwami wyznaczonymi stosując odpowiednią metodę analizy niezawodności człowieka (HRA) [3, 4, 6, 11]. Staranna ocena przewidywanego zachowania się człowieka (z włączeniem kontekstowo zorientowanego diagnozowania, intencji i działania) oraz potencjalnych błędów jest podstawową przesłanką poprawnej oceny ryzyka i racjonalnego podejmowania decyzji w procesie zarządzania bezpieczeństwem [10, 22]. Prawdopobieństwa tych zdarzeń zależą istotnie od różnych czynników wpływu, w tym czynników ludzkich i organizacyjnych [3, 15, 16].

Ostatnio, Carey [2], Hickling i inni [9] oraz Kosmowski [19] proponują nowe podejścia, w jaki sposób uwzględniać czynniki ludzkie w zarządzaniu bezpieczeństwem funkcjonalnym [12, 13]. Błędy ludzkie mogą być popełniane w całym cyklu życia systemu, począwszy od etapu projektowania, instalowania, oddawania do eksploatacji i samej eksploatacji, aż do likwidacji. Podczas eksploatacji interwencje człowieka-

operatora obejmują działania sterujące podczas stanów przejściowych, zakłóceń i uszkodzeń, jak również czynności diagnostyczne, testy funkcjonalności i integralności bezpieczeństwa, działania obsługi profilaktycznej i napraw po uszkodzeniach [17, 18].
Operatorzy nadzorują proces i podejmują decyzje przy użyciu systemu wspomagania operatora (OSS), który powinien być starannie zaprojektowany na sytuacje nienormalne i awaryjne, również na przypadki częściowych uszkodzeń i uszkodzeń niebezpiecznych w obrębie systemów elektrycznych, elektronicznych i programowalnych elektronicznych (E/E/PE) [12] lub przyrządowych systemów bezpieczeństwa (SIS) [13]. OSS, kiedy jest odpowiedni zaprojektowany, przyczynia się do zmniejszenia prawdopobieństwa błędu człowieka i ryzyka potencjalnych awarii. W artykule podkreśla się znaczenie analizy niezawodności człowieka w kontekście zarządzania bezpieczeństwem funkcjonalnym.

2. Analiza niezawodności człowieka w kontekście bezpieczeństwa funkcjonalnego

2.1. Poziomy nienaruszalności bezpieczeństwa i kryteria probabilistyczne

Współczesne systemy przemysłowe są w znacznym stopniu skomputeryzowane i wyposażone w złożone programowalne systemy sterowania i zabezpieczeń. W projektowaniu systemów sterowania i zabezpieczeń ma zastosowanie, w różnych sektorach przemysłowych, koncepcja bezpieczeństwa funkcjonalnego [12], na przykład w przemyśle procesowym [13].
Celem zarządzania bezpieczeństwem funkcjonalnym jest redukcja ryzyka w systemie systemu podwyższonego ryzyka do poziomu akceptowanego lub tolerowanego wprowadzając zestaw funkcji związanych z bezpieczeństwem (SRS) stosując systemy programowalne sterowania i/lub zabezpieczeń. Człowiek-operator (HO) wpływa na realizację danej SRF zgodnie ze specyfikacją techniczną. Jednakże, występują nadal wyzwania metodyczne dotyczące zarządzania bezpieczeństwem funkcjonalnym w cyklu życia [17].
Ważnym terminem związanym z koncepcją bezpieczeństwa funkcjonalnego jest nienaruszalność bezpieczeństwa [12], rozumiana jako prawdopodobieństwo zdarzenia, że dany system związany z bezpieczeństwem wypełni właściwie wymaganą SRF we wszystkich podanych warunkach w określonym przedziale czasu. Poziom nienaruszalności bezpieczeństwa (SIL) jest poziomem dyskretnym (1÷4) i służy do specyfikowania wymagań nienaruszalności danej funkcji bezpieczeństwa, która będzie alokowana za pomocą systemu E/E/PE lub SIS. Czwarty poziom nienaruszalności bezpieczeństwa (SIL4) jest

poziomem najwyższym, który wymaga zastosowania architektury redundancyjnej systemu E/E/PE, zawierającego podsystemy diagnozowane i okresowo testowane.
Dla kolejnych SIL-ów definiowane są dwa kryteria probabilistyczne, a mianowicie:

- przeciętne prawdopodobieństwo wypełnienia funkcji związanej z bezpieczeństwem na przywołanie (PFD_{avg}) w przypadku systemu działającego w trybie rzadkiego przywoływania, oraz
- prawdopodobieństwo niebezpiecznego uszkodzenia na godzinę *PFH* (częstość) w przypadku systemu działającego w trybie częstego przywoływania lub ciągłym.

Przedziałowe kryteria probabilistyczne dla funkcji związanych z bezpieczeństwem zaimplementowanych za pomocą systemów E/E/PE podano w Tablicy 1. Podobne kryteria przedziałowe są również stosowane w ocenach SIS [13].

Tablica 1. Kryteria probabilistyczne dla funkcji bezpieczeństwa [12]

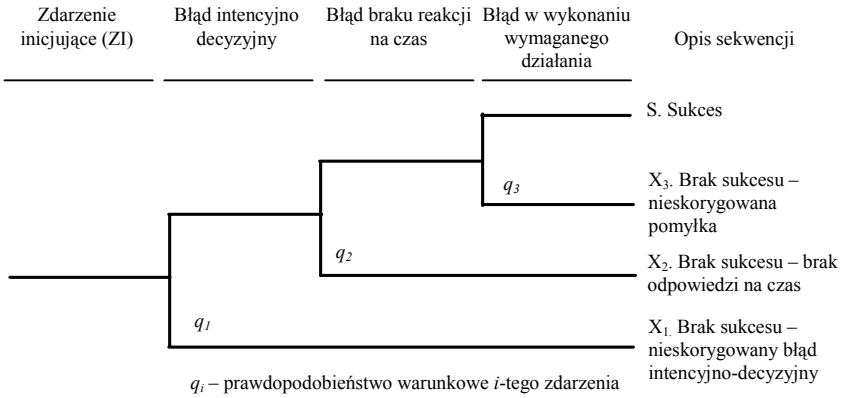
SIL	PFD_{avg}	PFH [h^{-1}]
4	[10^{-5}, 10^{-4})	[10^{-9}, 10^{-8})
3	[10^{-4}, 10^{-3})	[10^{-8}, 10^{-7})
2	[10^{-3}, 10^{-2})	[10^{-7}, 10^{-6})
1	[10^{-2}, 10^{-1})	[10^{-6}, 10^{-5})

SIL danej funkcji związanej z bezpieczeństwem (SRF) jest określony w procesie analizy i oceny ryzyka na podstawie zdefiniowanej matrycy ryzyka, która zawiera obszary kilku kategorii ryzyka, na przykład nieakceptowanego, umiarkowanego i akceptowanego [18, 19].
Weryfikowanie SIL danej funkcji związanej z bezpieczeństwem do zaimplementowania za pomocą systemu E/E/PE lub SIS jest trudnym zadaniem z powodu niedoboru danych niezawodnościowych i innych danych stosowanych jako parametry w modelach probabilistycznych systemów w projektowaniu. W takiej sytuacji przyzwala się w IEC 61508 stosować metodę jakościową do zgrubnego weryfikowania SIL dla rozważanych architektur systemu, rozważanych na etapie projektowania.

2.2. Czynniki wpływu w analizie niezawodności człowieka

Metody analizy niezawodności człowieka (HRA) są stosowane do oceniania ryzyka, wynikającego z potencjalnych błędów człowieka, w celu redukowania podatności systemu na uszkodzenia, który jest eksploatowany w danym, szeroko rozumianym środowisku. Jednakże, niektóre podstawowe założenia dotyczące metod HRA, które są stosowane w ramach

probabilistycznych analiz bezpieczeństwa systemów podwyższonego ryzyka, są nadal tematami sporu pomiędzy badaczami [10].
Praktycznie wszystkie metody HRA zakładają, że jest sensowne stosowanie pojęcia błędów człowieka i jest uzasadnione szacowanie ich prawdopodobieństw. Taki punkt widzenia jest niekiedy kwestionowany z powodu nie w pełni zweryfikowanych założeń dotyczących postępowania człowieka i potencjalnych błędów. Hollnagel [10] konkluduje, że niektóre wyniki HRA mają ograniczoną przydatność jako wejście do analizy probabilistycznej PSA, głównie z powodu zbyt uproszczonej koncepcji działania i błędu człowieka. Nie ma wątpliwości, jednakże, że potencjalne błędy człowieka powinny być rozpatrywane w danym kontekście (dynamika procesu, automatyzacja, interfejs człowiek-maszyna MMI). Przykładowe błędy człowieka i ich konsekwencje przedstawiono na rys. 1.



Rys. 1. Przykładowe błędy człowieka-operatora i ich konsekwencje

Mimo wspomnianej krytyki, w oczekiwaniu na następną generację metod HRA, analitycy czynników ludzkich stosują w ramach PSA kilka dostępnych metod HRA. Poniżej krótko scharakteryzowano kilka wybranych metod HRA, które mogą być stosowane w analizie bezpieczeństwa funkcjonalnego. Zgrubne oceny niezawodności człowieka bazujące na informacji jakościowej mogą być szczególnie użyteczne we wstępnym podejmowaniu decyzji na etapie projektowania funkcji związanych z bezpieczeństwem i systemów je realizujących [18]. Zostanie wykazane, że struktura analizy bezpieczeństwa funkcjonalnego, obejmująca systemy sterowania i zabezpieczeń oraz przyjęte rozwiązania interfejsu MMI (Man-Machine Interface), daje dodatkowe spostrzeżenia przydatne w przeprowadzaniu HRA.
Kilka konwencjonalnych metod HRA było częściej stosowanych w praktyce PSA, szczególnie metoda THERP [20], opracowana dla przemysłu jądrowego, ale stosowana również w różnych sektorach przemysłowych.

Innymi metodami HRA, częściej stosowanymi w praktyce przemysłowej są: *Accident Sequence Evaluation Procedure-Human Reliability Analysis Procedure* (ASEP-HRA), *Human Error Assessment and Reduction Technique* (HEART), and *Success Likelihood Index Method (SLIM)* – zobacz opis i charakterystykę tych metod w raportach [3, 11].

W publikacji [1] dokonano selekcji pięciu metod w celu ich porównania na podstawie, zarówno stosunkowo szerokiego stosowania, jak i rozpoznanego wkładu jako aktualnej współczesnej techniki:

- *Technique for Human Error Rate Prediction* (THERP);
- *Accident Sequence Evaluation Program* (ASEP);
- *Cognitive Reliability and Error Analysis Method* (CREAM);
- *Human Error Assessment and Reduction Technique* (HEART);
- *Technique for Human Event Analysis* (ATHEANA).

W uzupełnieniu do tych metod były badane również inne źródła informacji, w celu zgłębienia zagadnień dotyczących traktowania i oceny błędów człowieka. Zostały przeprowadzone porównania względem metody SPAR-H [7]. Finalną konkluzją jest, że uaktualniona metodyka SPAR-H jest użytecznym i łatwym w użyciu narzędziem przesiewowym HRA do szerokiego stosowania.

Prawdopodobieństwo błędu człowieka (HEP) szacuje się, kiedy zdarzenie błędu człowieka umieszczono w strukturze modelu probabilistycznego systemu. Podczas przeprowadzania HRA wykonywanej w ramach PSA rozpatruje się tylko ważniejsze zdarzenia błędów człowieka [14, 16]. Specyfikuje się wówczas odpowiednie czynniki kształtujące działanie (PSF), określane zgodnie z zasadami danej metody HRA. W wyniku uzyskuje się określoną wartość HEP.

Do wyznaczania HEP z uwzględnieniem PSF stosowane są różne podejścia, na przykład przy założeniu liniowej zależności dla każdego zidentyfikowanego PSF_k i jego współczynnika wagowego w_k, ze stałą C do kalibracji modelu

$$HEP = HEP_{no\min al} \sum_k w_k PSF_k + C \tag{1}$$

lub nieliniowej zależności stosowanej w metodzie SPAR-H [7]

$$HEP = \frac{NHEP \cdot PSF_{composite}}{NHEP(PSF_{composite} - 1) + 1} \tag{2}$$

gdzie: NHEP jest nominalnym prawdopodobieństwem HEP; NHEP równa się 0.01 dla diagnozowania, a NHEP równa się 0.001 dla błędu działania.

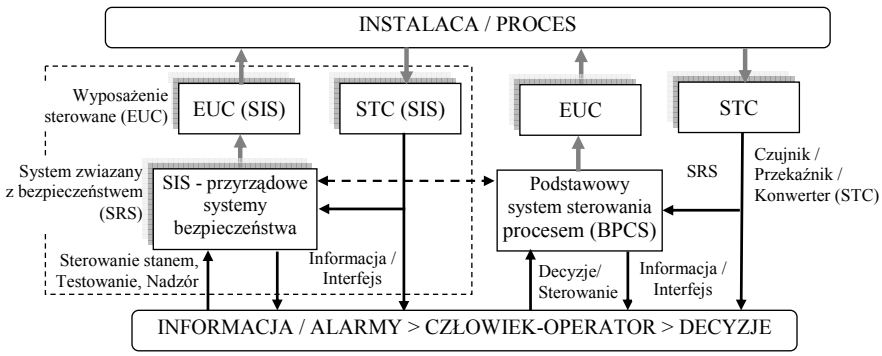
3. Czynniki ludzkie i analiza warstw zabezpieczeń

Instalacje przemysłowe podwyższonego ryzyka są obecnie projektowane zgodnie z *zasadą obrony w głąb*, z wyróżnieniem kilku warstw zabezpieczeń. Projektowanie systemów związanych z bezpieczeństwem jest oparte na ocenie ryzyka z określeniem wymaganego poziomu SIL i jego weryfikacji w procesie modelowania probabilistycznego [8, 18]. Uproszczoną metodą do wstępnej analizy ryzyka i podejmowania decyzji związanych z bezpieczeństwem jest metodyka analizy warstw zabezpieczeń (LOPA) [20].

Aktywna niezależna warstwa zabezpieczeń (IPL) zawiera ogólnie następujące elementy:

- A – czujnik określonego typu (przyrząd lub człowiek jako sensor),
- B – element decyzyjny (układ logiczny, przekaźnik, człowiek itd.),
- C – działanie (automatyczne, mechaniczne lub człowieka).

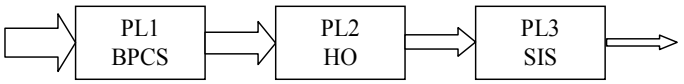
Warstwy IPL mogą być zaprojektowane jako podstawowy system sterowania (BPCS) lub SIS. Systemy te powinny być funkcjonalnie i strukturalnie niezależne; jednakże, nie jest to zawsze możliwe w praktyce. Rys. 2 przedstawia zależności funkcjonalne trzech warstw zabezpieczeń: BPCS, człowieka-operatora (HO) i SIS. Ważną częścią takiego złożonego systemu jest interfejs człowiek- maszyna (MMI) [6, 8]. Jego funkcjonalność w stanach nienormalnych systemu i jakość projektu są często przyjmowane jako ważne czynniki PSF w analizie HRA [6, 14].



Rys. 2. Systemy sterowania i zabezpieczeń jako warstwy w obiekcie podwyższonego ryzyka

Warstwy zabezpieczeniowe z rys. 2 są przedstawione na rys. 3. Obejmują one:

- PL1 – podstawowy system sterowania procesu (BPCS),
- PL2 – człowieka - operatora (HO),
- PL3 – przyrządowy system bezpieczeństwa (SIS).



Rys. 3. Warstwy zabezpieczeń redukujące częstość scenariuszy awaryjnych

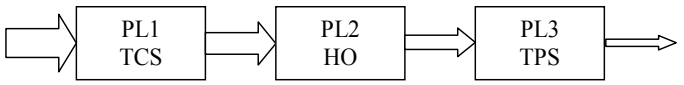
Te warstwy zabezpieczeń powinny być traktowane ogólnie jako zależne. Częstość *i*-tego scenariusza awaryjnego F_i^{PLs} jest obliczana biorąc pod uwagę prawdopobieństwa warunkowe *PFD*, skutkujące wyższą wartością częstości niż w przypadku niezależności

$$F_I^{PLs} = F_i^I PFD_i^{PL1} PFD_i^{PL2} PFD_i^{PL3} = d \cdot F_i^{IPLs} \tag{3}$$

Wartość współczynnika d może być znacznie większa niż 1 (nawet o rząd wielkości) jeśli byłaby przyjęta niezależność warstw zabezpieczeń (*IPL*) z częstością scenariusza awaryjnego F_i^{IPLs}. Na wartość *d* znacząco wpływają założenia dotyczące modelowania probabilistycznego uszkodzeń i błędów zależnych spowodowanych uszkodzeniami wyposażenia i/lub błędami człowieka [19].

4. Studium przypadku analizy warstw zabezpieczeń

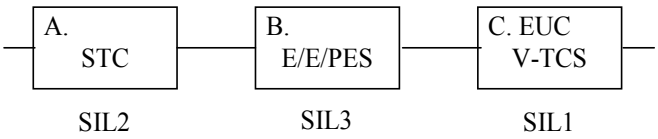
Rozważa się poniżej dwa systemy związane z bezpieczeństwem: system sterowania turbiną (TCS) i system zabezpieczeń turbiny (TPS). Systemy te pełnią ważną funkcję zamknięcia odpowiedniego zaworu i wyłączenia turbiny zespołu elektroenergetycznego w sytuacjach zakłóceń. Uszkodzenia tych systemów mogą doprowadzić do bardzo poważnych skutków.
TCS działa w trybie ciągłym, a TPS jest systemem działającym w trybie rzadkiego przywołania do działania (zob. podrozdz. 2.1). Systemy te są projektowane z uwzględnieniem wymaganego poziomu SIL, określonym w procesie oceny ryzyka. Oceniono, że ryzyko powinno być obniżone ze współczynnikiem 10^{-4} (ekwiwalentnie do poziomu SIL4), stosując systemy TCS i TPS traktowane jako pierwsza i trzecia bariera (zob. rys. 3). Pomiędzy tymi warstwami usytuowana jest druga bariera: człowiek-operator (HO) (zob. rys. 4).



Rys. 4. Warstwy zabezpieczeń redukujące częstość scenariusza awaryjnego

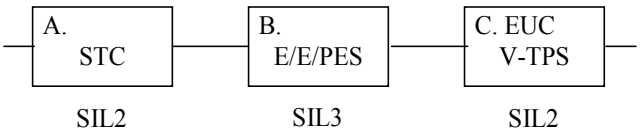
Wstępne wyniki analizy bezpieczeństwa funkcjonalnego TCS wskazują, że przyjęta konfiguracja zapewnia poziom nienaruszalności bezpieczeństwa SIL1. Taki niski poziom SIL wynika głównie z poziomu nienaruszalności bezpieczeństwa podsystemu C (zawór sterowany V-TCS) ocenionego na

poziomie SIL1 (rys. 5). Podsystem A (czujnik, przetwornik lub konwertor) wpływa mniej znacząco na uzyskany wynik (SIL2), a udział w PFD_{avg} podsystemu B (E/E/PES) jest nieznaczny z powodu SIL3.



Rys. 5. Podsystemy w systemie sterowania turbiny (TCS)

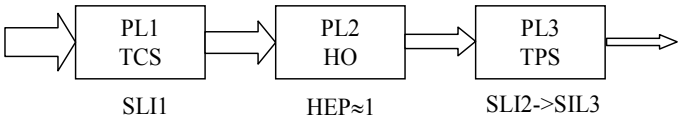
TPS zapewnia poziom nienaruszalności bezpieczeństwa 2 (SIL2), jak można zauważyć na rys. 6. Wynika to z SIL podsystemu C (zawór V-TPS) wyznaczony jako SIL2. Podsystem A (czujnik, przetwornik lub konwertor) wpływa mniej znacząco na uzyskany wynik (SIL2), a udział w PFD_{avg} podsystemu B (E/E/PES) jest nieznaczny (SIL3).



Rys. 6. Podsystemy w systemie zabezpieczeń turbiny (TPS)

Wynikowe poziomy nienaruszalności bezpieczeństwa pokazano na rys.7. Z powodu znacznej dynamiki systemu dla większości rozpatrywanych zdarzeń inicjujących oraz dużej zależności działań człowieka, prawdopodobieństwo błędu człowieka zostało wyznaczone (na podstawie trzech metod: THERP, HEART i SPAR-H) jako wysokie, bliskie 1 (HEP ≈ 1). Dlatego, redukcja ryzyka przez TCS i TPS jest tylko na poziomie 10^{-3} (SIL1 i SIL2).

Wymagana redukcja ryzyka na poziomie 10^{-4} nie została, więc, osiągnięta i należy rozpatrzyć modyfikację projektu. Analiza wykazała, że nie jest możliwe na uzasadnionym poziomie kosztów spowodowanie wzrostu SIL w systemie sterowania TCS (z SIL1 do SIL2). Dlatego wzięto pod uwagę inną opcję projektu ze wzrostem SIL systemu zabezpieczeń TPS (z SIL2 na SIL3 – zob. blok z prawej strony na rys. 7).



Rys. 7. Finalne poziomy nienaruszalności bezpieczeństwa w warstwach zabezpieczeń systemu wyłączania turbiny

Zaproponowano osiągnąć wyższy poziom SIL systemy TPS przez wzrost SIL podsystemu A z SIL2 (zob. rys. 6) do SIL3 oraz podsystemu C z SIL2

do SIL3. W podsystemie A zaproponowano architekturę 2oo3 w celu obniżenia PFD_{avg} i obniżenia częstości niepotrzebnego zadziałania TPS. Aby zwiększyć SIL podsystemu C nie jest uzasadnione zaimplementowanie struktury 1oo2 z powodu zbyt wysokich kosztów zaworów. Dlatego w celu osiągnięcia wymagań związanych z SIL3 należy rozpatrzyć stosowne aspekty organizacyjne (selekcja zaworu wysokiej jakości i odpowiednia strategia testowania zaworu wyłączającego).

5. Wnioski

Schemat zorientowany na bezpieczeństwo funkcjonalne stwarza dodatkowe możliwości pełniejszej analizy niezawodności człowieka (HRA) z podkreśleniem kontekstowego zachowania się człowieka w sytuacjach nienormalnych, również tych związanych z bezpiecznymi i niebezpiecznymi uszkodzeniami programowalnego wyposażenia sterującego i zabezpieczającego. Taka analiza umożliwi zrozumienie jak projektować funkcje związane z bezpieczeństwem za pomocą podstawowego systemu sterowania procesem (BPCS), człowieka-operatora (HO) i przyrządowych systemów bezpieczeństwa (SIS) z uwzględnieniem kryteriów probabilistycznych dla wyróżnionych poziomów nienaruszalności bezpieczeństwa (SIL). Potrzebne są dalsze badania w celu dokonania bardziej wyczerpujących obserwacji dotyczących wpływu czynników ludzkich w kontekście funkcji związanych z bezpieczeństwem projektowanych za pomocą programowalnych systemów sterowania i zabezpieczeń.

Prof. **Kazimierz Kosmowski,** received Ph.D. in 1981 and D.Sc. in 2003 from Gdansk University of Technology (GUT). Since 2006 the manager of Division of Control Eng. at Faculty of Electrical and Control Eng. and since 2007 a vice-chairman of Polish Safety and Reliability Association (PSRA).
Specialization: reliability and safety of technical systems, human reliability, functional safety of programmable control and protection systems.