*Advances in Reliability, Safety and Security, Part 5 – Kołowrocki, Kosmowski (eds.)*
*© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-17-3 (printed), ISBN 978-83-68136-04-3 (electronic)*

**Advances in Reliability, Safety and Security**

ESREL 2024
Monograph Book Series

# Human Factors And Reliability In Functional Safety Analysis

Kazimierz T. Kosmowski

*Polish Safety and Reliability Association, Gdańsk, Poland*

**Abstract**

This paper addresses the state of the art and current research challenges concerning human factors, in particular the human reliability analysis (HRA) as a part of probabilistic modelling of hazardous industrial plant. Important role in the safety management of such plant plays nowadays the design and operation of a safety-related control system (SRCS), being a part of the industrial automation and control system (IACS). It is emphasized that the automation and safety-related control system should be designed as human centered. It is presented how to apply a methodological framework for dealing with evaluating and reducing risks in life cycle regarding human factors. Such framework includes the functional safety analysis concept and an appropriate human reliability analysis technique supported by contextual task analysis. Safety-related tasks in abnormal or accident situation execute a team of human operators who use a human system interface (HSI) and an alarm system (AS). The time widow for diagnosis of abnormal situation and performing required actions is usually limited, depending on dynamic properties of the plant. Some safety functions are initiated automatically, but the probability of the SRCS failure depends on its architecture, quality of software, and a strategy of inspections including periodical testing of components with recovering of faulty ones. The approach is illustrated on the case studies using an event tree and probabilistic modelling of events. The label of such event tree consists of protections, in particular safety related systems, and human actions that can be correct in given situation or erroneous.

*Keywords*: industrial installation, hazards, risk reduction, industrial automation and control system, functional safety, alarm system, human factors, human cognitive reliability

## 1. Introduction

The functional safety a part of general safety, which depends on the proper functioning in time of the programmable control and protection systems. General concept of the functional safety was formulated in the international standard IEC 61508 (2010). It includes defining, for given hazardous installation, a set of safety functions (SF) that are implemented in properly designed the electric, electronic, and programmable electronic (E/E/PE) systems, or so-called safety instrumented systems (SIS) (IEC 61511, 2016) in the process industry sector. The safety-related control systems (SRCS) are designed using the functional safety concept (IEC 61508, 2010; Kosmowski, 2006, 2016). It includes defined categories of the safety integrity level (SIL). Determined SIL of given safety function to be implemented in the basic process control system (BPCS) and/or the safety instrumented system (SIS) must be then verified regarding the SRCS architecture proposed.

It is emphasized that the automation and safety-related control system should be designed as human centered. It will be discussed during the workshop how to apply a methodological framework for dealing with evaluating and reducing risks in life cycle regarding human factors. Such framework includes the functional safety analysis concept and an appropriate human reliability analysis technique supported by contextual task analysis. Safety-related tasks in abnormal or accident situation execute a team of human operators who use a human system interface (HSI) and an alarm system (AS).

More frequently used in engineering practice HRA techniques will be characterized with their pros and cons. It will be outlined how to evaluate the human error probability (HEP) using selected HRA methods, such as THERP, SPAR-H and CREAM (Bell & Holroyd, 2009). The HEP for relevant human operator behavior type: skill (S), rule (R), and knowledge (K). The SRK concept of human activity was applied in the human cognitive reliability (HCR) model. The graph-based method called hierarchical influence diagram (HID) will be also presented and discussed on example of the Formal Safety Assessment (FSA) methodology of IMO. Usefulness of other HRA methods are also discussed for using in the context specific situation, especially when the cognitive aspects is not crucial. The concept of the hierarchical influence diagrams will be also presented similar to that proposed by IMO in the formal safety analysis (FSA) methodology.

In final part of the paper some proposals are formulated how to shape the human factors in the context of the functional safety and cybersecurity evaluations. As regards functional safety concept, the contribution of human and organizational factors are usually included defining the dependent failures in probabilistic modelling to verify the safety integrity levels of safety-related systems in which the safety functions are implemented. In cybersecurity evaluation the human and environmental factors should be evaluated in the context of fundamental requirements (FR) for the control system domain including converged IT and OT networks.

A concept of knowledge-based system is also discussed for supporting the human factors analysis in the integrated functional safety and cybersecurity analysis. The human and organizational factors are also of interest, in particular in the light of shaping safety and security culture of the technical and organizational solutions of Industry 4.0 and 5.0. These cultures influence significantly the resilience of hazardous installations and critical infrastructure. The resilience issue requires further research due to its importance for reliable and safe system operation in uncertain conditions. Some topics to undertake such research will be proposed. Applying the AI-based algorithms for that purpose will be also discussed regarding legal and engineering aspects in designing the safety and security related decision support systems.

## 2. Typical architecture of ICT including converged IT-OT systems and categories of human activities

A typical ICT architecture including converged technologies OT-IT-CT, IACS components and categories of human activity is shown in Figure 1. Some concepts for integrating functional safety and cyber security analyses are described in publications (Kanamaru, 2020; Kosmowski, 2021a; 2022; Kosmowski et al., 2019, 2022).

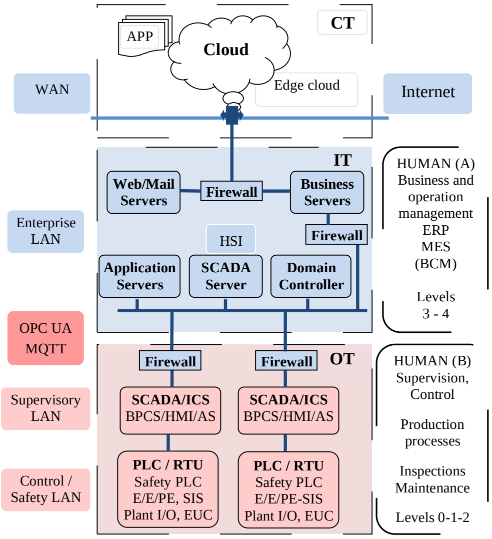

Fig. 1. Typical ICT architecture including converged OT-IT and categories of human activity

At the bottom of OT area following elements and systems are located: the control / safety local area network (LAN), input/output (I/O) elements, the electrical / electronic / programmable electronic (E/E/PE) system, safety instrumented system (SIS), safety programmable logic controllers (PLC), basic process control system (BPCS), human machine interface (HMI), alarm system (AS), remote terminal units (RTU), supervisory control and data acquisition (SCADA) system.

At a higher system level, a human system interface (HSI) is placed that enables human operators to monitor and control the subsystems of OT. More details about such complex architecture including basic functional, safety and security requirements specified in selected international standards can be found in a publication (Kosmowski et al., 2019).

In the right side of this figure two blocks represent distinguished categories of human activities within an industrial company. The upper block (A) concerns the business and a long-term operation management. It includes, for instance, the business continuity management (BCM) activities in relation to functionality of the enterprise resource planning (ERP) system and manufacturing execution system (MES). It corresponds to the levels 3 and 4 distinguished in the ISA 95 reference model (Kosmowski et al., 2019).

The lower block (B) concerns the supervision and control of production processes that include periodical inspections and maintenance according to a strategy developed regarding equipment current states and predictive models. It corresponds to the levels 0, 1 and 2 distinguished in the ISA 95 reference model (Kosmowski et al., 2019). These two blocks represent cognitive realm of human behaviors at relevant levels of the system model. The time window for human reaction in abnormal situation is an important factor influencing correct diagnosis and action. If this time is too short then the human error probability (HEP) can be high, even close to 1 (Kosmowski, 2022). Such situation can deteriorate the system resilience depending on the design solution of the safety-related control system designed, for instance to fulfil requirements of the functional safety standards (IEC 61508, 2010; IEC 61511, 2016). Selected issues of human reliability analysis (HRA) including cognitive aspects will be discussed later in context of functional safety analysis and SCADA interface.

The lower block (B) concerns the supervision and control of production processes that include periodical inspections and maintenance according to a strategy developed regarding equipment current states and predictive models. It corresponds to the levels 0, 1 and 2 distinguished in the ISA 95 reference model (Kosmowski et al., 2019). These two blocks represent cognitive realm of human behaviors at relevant levels of the system model. The time window for human reaction in abnormal situation is an important factor influencing correct diagnosis and action. If this time is too short then the human error probability (HEP) can be high, even close to 1 (Kosmowski, 2022). Such situation can deteriorate the system resilience depending on the design solution of the safety-related control system designed, for instance to fulfil requirements of the functional safety standards (IEC 61508, 2010; IEC 61511, 2016). Selected issues of human reliability analysis (HRA) including cognitive aspects will be discussed later in context of functional safety analysis and SCADA interface.

## 3. Defining safety functions and layer of protection analysis

### 3.1. Defining safety functions for reducing risks

The functional safety a part of general safety, which depends on the proper functioning in time of the programmable control and protection systems. General concept of the functional safety was formulated in the international standard IEC 61508 (2010). It includes defining, for given hazardous installation, a set of safety functions (SF) that are implemented in properly designed the electric, electronic, and programmable electronic (E/E/PE) systems, or so-called safety instrumented systems (SIS) (IEC 61511, 2016) in the process industry sector.

Two different requirements have to be specified to ensure required safety level:

- the requirements imposed on performance of the safety function considered,
- the safety integrity requirements, understood as the probability that given safety function will be performed in a satisfactory manner within a specified time.

These requirements are specified regarding hazards identified and potential accident scenarios defined. The safety integrity level (SIL) requirements stem from the results of the risk assessment considering the risk criteria to be specified (IEC 61508, 2010; IEC 61511, 2016). Two categories of operation modes are to be considered in the functional safety analysis, namely: (1) low, and (2) high or continuous. A low demand mode is typical for the process industry protection systems, e.g., within protection layers. A high or continuous demand mode is encountered in many systems for monitoring and control, for instance in the production or transportation sectors.

The E/E/PE systems or SIS should be appropriately designed to perform specified functions to ensure that relevant risks are reduced to fulfil specified risk criteria at the plant design stage. The risk assessment should be verified periodically during the operation of installation, because the operating conditions and hazards can change in time. However, the risk criteria are not defined generally in mentioned above standards. Only some examples of risk graphs are presented, but with remarks, that specific criteria should be defined for given process installation. It is suggested to consider three types of losses, namely health, environmental, and material.

Allocation of requirements for the safety functions and safety-related systems implementing these functions is illustrated in Figure 2 (Kosmowski, 2013). It starts with the hazard identification and risk evaluation to determine required safety-integrity level (SIL) of the safety function (SF) to be implemented for the risk reduction. The risk acceptance criteria are to be defined for the individual risk and/or societal risk depending on the objective of safety management.

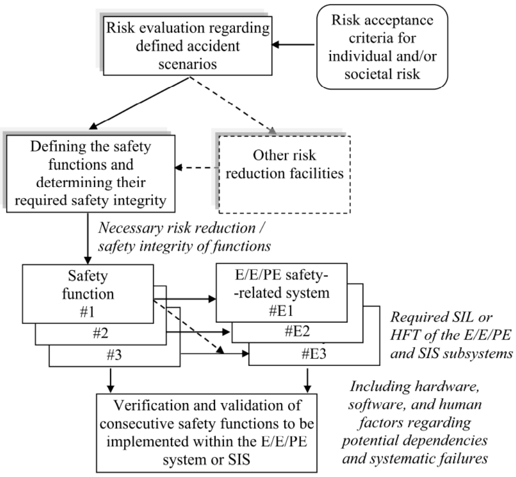
Risk evaluation regarding defined accident scenarios
Risk acceptance criteria for individual and/or societal risk
Defining the safety functions and determining their required safety integrity
Other risk reduction facilities
Necessary risk reduction / safety integrity of functions
Safety function #1
#2
#3
E/E/PE safety--related system #E1
#E2
#E3
Required SIL or HFT of the E/E/PE and SIS subsystems
Verification and validation of consecutive safety functions to be implemented within the E/E/PE system or SIS
Including hardware, software, and human factors regarding potential dependencies and systematic failures

Fig. 2. Allocation of requirements for safety functions to be implemented in safety-related systems.

Identified safety functions are to be implemented in the SRCS, e.g., E/E/PE or SIS. The SIL goal to be achieved by designed architecture of SRCS is verified using probabilistic models developed (Kosmowski, 2013). It is important to include in probabilistic models potential dependencies between failure events, in particular potential common cause failures (CCF) in cases when SRCS comprises the redundant subsystems. The architecture of SRCS (hardware and software) must be then verified as regards potential systematic failures and the influence of human factors resulting due to potential human errors of relevant types (Kosmowski, 2011, 2022, 2023).

### 3.2. Layer of protection analysis

In some hazardous plants a single SRCS can be not sufficient to reduce the risk as required. In such case the safety-related system has to be designed according to a concept of defense in depths (D-in-D) using two or more protection layers. In Figure 3 typical protection layers in a process plant (IEC 61511, 2016) are presented. An appreciated approach for the preliminary risk analysis and safety-related decision making in industrial process installations is the layer of protection analysis (LOPA) methodology (LOPA, 2001).

For instance, the protection layers can include: a basic process control system (BPCS), an alarm system (AS) with human-operator interactions, and the safety instrumented system (SIS) performing an emergency shutdown (ESD) function, numbered in Figure 3 respectively as layers: 2, 3 and 4. These protection layers should be physically and functionally independent, however, it is not always achievable in industrial practice. They are denoted in Figure 4 respectively as protection layer (PL): $PL_2$, $PL_3$ and $PL_4$.

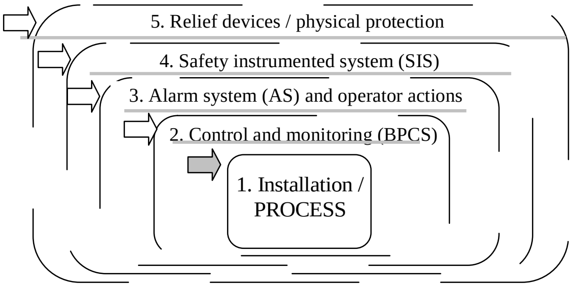
5. Relief devices / physical protection
4. Safety instrumented system (SIS)
3. Alarm system (AS) and operator actions
2. Control and monitoring (BPCS)
1. Installation / PROCESS

Fig. 3. Typical protection layers in hazardous industrial installation (Kosmowski, 2013).

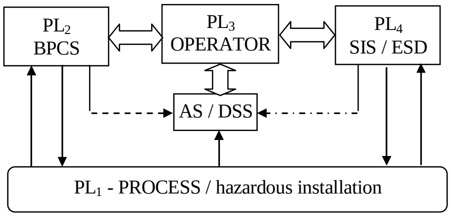

Fig. 4. Human operator and alarm system (AS) as elements of the protection layers.

Achieving independency of protection layers requires appropriate technical and organizational solutions. In case of $PL_2$ and $PL_4$ it can be achieved using separate sensors and input elements, input modules for information processing in PLCs and actuators (final elements). Required safety integrity levels (SIL) of BPCS and SIS for given safety function is to be achieved using appropriate architectures of subsystems considering the probabilistic criteria for verifying the SIL to be achieved, from SIL1 to SIL4 (Kosmowski, 2013, 2023b). The safety function implemented in BPCS is characterised usually by low safety integrity level (SIL1) due to high complexity of such system, and when it can be treated as safety-related.

## 4. Incorporating cognitive aspects in human reliability analysis

### 4.1. Human factors and systems cognitive engineering

The domain of systems engineering (SE) is traditionally focused on the technological aspects of the system design, such as hardware, software, and automation, while ignoring sometimes the fact that these systems will ultimately be used, operated, and maintained by humans to meet the mission and production goals (IAEA, 2021). It is known that human factors influence significantly the operation, reliability, safety, and security of technical systems. Therefore, they should be properly treated in industrial practice applying, for instance, the systems engineering (SE) general concept (SE, 2001) for effective management of installations including the control systems and communication networks in life cycle of industrial plant (Rasmussen et al., 1990; Whaley et al., 2016). Interesting proposals to deal with human factors regarding the functional safety functional safety concept have been published (Cray, 2001; Froome & Jones, 2002).

The goal of cognitive engineering (CE), or more generally cognitive systems engineering (CSE), is to develop advanced systems, training programs, and other products that support cognitive functions in decision-making, abnormal situation management, course-of-action selection, resource allocation and other information processing tasks (Bonaceto et al., 2005; Gersh et al., 2005).

The CE approaches are classified regarding their focus and application purpose. Following categories of the CE research areas may be distinguished that concern (Kosmowski, 2017): (1) Analysis of system oriented human interactions, (2) Task analysis and identification of critical tasks, (3) Behavioural processes, (4) Cognitive processes, and (5) Identification of erroneous diagnosis and following actions. Each of these areas can be divided into several subareas. An approach outlined below is focused on area (5).

For the purpose of a case study an event tree (ET) method is used for defining accident scenarios including human related events for identified actions and potential errors, similarly as in an operator action event tree (OAET) (Gertman et al., 1994; Kirwan, 1994; Embrey, 2000). The failure events and success events in the ET are also defined for the safety-related control system and human operator actions that are evaluated using selected methods of the human reliability analysis (HRA). Human actions and potential errors are considered in the context of safety functions implemented using relevant systems: BPCS, AS, and/or SIS. Cognitive aspects of human operator behaviour are incorporated into probabilistic model using the Rasmussen's skill-rule-knowledge (SRK) conceptual framework (Rasmussen, 1983).

### 4.2. Human behaviour types

Some HRA methods are based on conceptual frameworks that include the human behaviour types and distinguished categories of human unsafe acts (Reason, 1990). Rasmussen (1983) proposes the distinction of three types of human behaviour. His known frame-work assumes following cognitive levels of human behaviour:

- skill-based (S), highly practiced tasks that can be performed as more or less sub-conscious routines governed by stored patterns of behaviour,

- rule-based (R), performance of less familiar tasks in which a person follows some common-sense rules and previously developed procedures, and
- knowledge-based (K), rough analysing a system state in unknown situation when familiar patterns and rules cannot be applied directly, and actions that follow include information processing with the inclusion of diagnosis, planning and decision making directed towards reducing losses.

Figure 5 illustrates this concept that is useful in the analysis of human behaviour during abnormal situations and accidents to identify potential human errors.

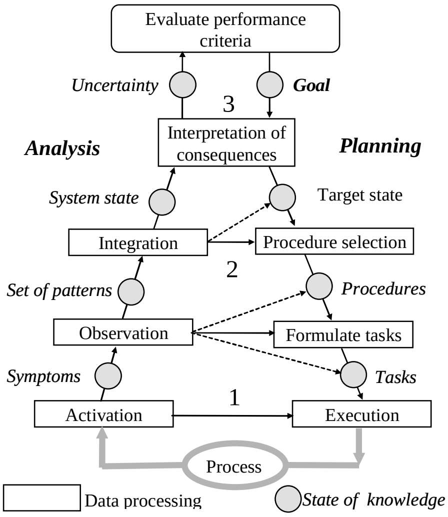

Fig. 5. Schematic representation of information processing by operators in context of behaviour types (1 - skill, 2 - rules, 3 – knowledge).

### 4.3. Including cognitive aspects in human reliability analysis

Appreciated HRA method, developed for dealing with cognitive aspects in evaluating human error probability (HEP) for defined activity, is a HCR (human cognitive reliability) technique based on a probabilistic model developed by Hannaman et al. (1984). HEP is treated in analysis as the probability of an event to be assigned within an event tree developed for defining potential accident scenarios (Kosmowski, 2023).

Three types of human behaviour types are distinguished (Kosmowski, 2022), according to Rasmussen’s conceptual model:

- Skill-based (S),
- Rule-based (R), and
- Knowledge-based (K).

Time-dependent HEP, treated as an event of non-response or human error in the situation considered, is calculated from the Weibull distribution from following formula:

$$HEP^{\mathrm{X}}(t) = \exp\left\{-\left[\frac{t/t_{0.5} - a}{c}\right]^{b}\right\} \tag{1}$$

where: *a, b, c* – are behaviour type coefficients specified below for behaviour type X (S, R, K) in given situation as explained below, and $t_{0.5}$ is the median value of time required to perform required task by human operators. If median value $t_{0.5}$ is short, e.g., below 1 min., then HEP is high, and is close to 1.

Different HRA method can be applied for evaluating HEP regarding a set of PSFs, e.g., using a nonlinear relationship proposed in the SPAR-H (2005) method:

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

where: NHEP is a nominal HEP; the value of NHEP is suggested to be assumed as equal 0.01 for diagnosis (D), and 0.001 for action (A).

In the method SPAR-H eight performance shaping factors ($PSF_i$) are to be evaluated by the HRA analysts/experts:

(1) available time (for diagnosis and/or action),
(2) stressors,
(3) complexity,
(4) experience/training,
(5) procedures,
(6) ergonomics/HMI/HSI,
(7) fitness for duty, and
(8) work processes,

according to relevant tables developed for tasks of diagnosis (D) and/or action (A) in specified situations to be evaluated in given technical system.

Described above models can be applied in analyses of operational resilience of the OT and IT networks when reactions of persons, responsible for functioning of these networks, are required, to diagnose correctly abnormal situation and to undertake action to shorten outage time of industrial installation. Similar models could be also used within the business continuity management (BCM) as suggested in the publication (Kosmowski et. al., 2022).

### 4.4. Human reliability analysis in context of accident scenarios

Potential human errors should be considered in given context, i.e., the installation complexity, dynamic of technological process, time limitation for reaction, solutions of control and protection systems, quality of the HMI / HSI, availability and quality of procedures, etc. Some categories of potential human errors and their consequences are presented in Figure 6.

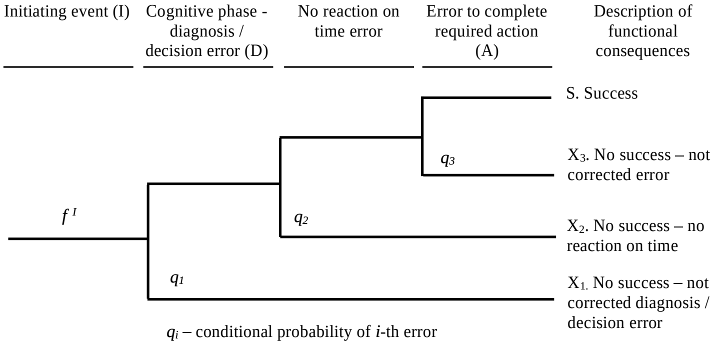
Initiating event (I)
Cognitive phase - diagnosis / decision error (D)
No reaction on time error
Error to complete required action (A)
Description of functional consequences
S. Success
$q_3$
X3. No success – not corrected error
$f^I$
$q_2$
X2. No success – no reaction on time
$q_1$
X1. No success – not corrected diagnosis / decision error
$q_i$ – conditional probability of $i$-th error

Fig. 6. Typical human-operator errors and their consequences.

Several traditional HRA methods are appreciated for using in PSA practice, e.g., Technique for Human Error Rate Prediction (THERP) method (Swain & Gutman, 1983), developed for the nuclear industry, applied also in various industrial sectors. Other HRA methods more often used in practice are as follows: Accident Sequence Evaluation Procedure (ASEP), Human Error Assessment and Reduction Technique (HEART), and Success Likelihood Index Method (SLIM). These conventional HRA methods are characterized and evaluated in various papers, monographs, and reports (Adhikari et al., 2009; Bell & Holroyd, 2009).

A considerable interest has been lately noticed to apply in industrial practice the Cognitive Reliability and Error Analysis Method (CREAM) developed by Hollnagel (1998), and lately also simplified, but easy to apply the SPAR-H (2005) method. However, the SPAR-H method is a second-generation method, not suitable for dealing with cognitive aspects of human operators' behaviour during diagnosis of abnormal or emergency situation. In a case study below the human cognitive reliability (HCR) model was applied that prove to be useful for the layered protection analysis.

## 5. Case study

### 5.1. Defining accident scenarios in layered protection system

An industrial installation and process is considered according to the author's publication [19] denoted as variant B. It comprises of a pressurized vessel containing a mixture of gas and volatile flammable liquid with necessary instrumentation. Process control is handled using a basic process control system (BPCS) that monitors the signal from the flow transmitters and makes the flow control to operate a control valve. Additional layers of protection are also considered: an alarm system (AS) with relevant interface to human operators, a safety instrumented system (SIS) performing the emergency shutdown (ESD) of the installation, and a pressure relief valve certified for SIL 2.

Relevant event tree including the operator action (response is required when the flow control loop fails) as it is shown in Figure 7. The results of the safety related analyses and calculations of the frequency for consecutive scenarios are presented in Table 1. The frequency of an initiating event was evaluated for a danger failure of the BPCS (SIL1), approximately at the level of $f^I = 10^{-5}$ h$^{-1}$ = 0.0876 a$^{-1}$ ~ 0.1 a$^{-1}$ (per year).

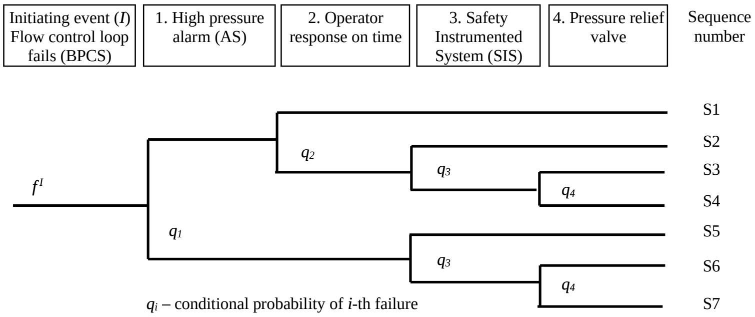
Initiating event (*I*)
Flow control loop fails (BPCS)
1. High pressure alarm (AS)
2. Operator response on time
3. Safety Instrumented System (SIS)
4. Pressure relief valve
Sequence number
$f^I$
$q_1$
$q_2$
$q_3$
$q_4$
$q_3$
$q_4$
S1
S2
S3
S4
S5
S6
S7
$q_i$ – conditional probability of *i*-th failure

Fig. 7. An event tree for the pressure vessel with protection layers.

In the case considered the human error probability was evaluated as equal $q_2$ = HEP$^R$ = 0.5, i.e., for the rule-based behaviour (R) due to a greater complexity of that process installation and performing tasks according to procedures of moderate quality. Relevant probabilistic model of the HCR method for the rule-based behaviour was applied as described in the section 4.3. It is worth to mention that if AS would be implemented within BPCS, the danger failure of BPCS (DCS/SCADA) could cause a danger situation due to unavailability of alarms and therefore human error probability would be close to 1.

Table 1. Description of the event tree sequences.

| Sequence | Frequency | Data: $q_1$ = 0.1; $q_2$ = HEP$^R$ = 0.5; $q_3$ = 0.01; $q_4$ = 0.01 |
|---|---|---|
| number | [a$^{-1}$] | Consequences and remarks |
| S1 | $0.45 \cdot 10^{-1}$ | No release to the flare |
| S2 | $0.45 \cdot 10^{-1}$ | No release to the flare |
| S3 | $0.45 \cdot 10^{-3}$ | Release to the flare |
| S4 | $0.45 \cdot 10^{-5}$ | Release to the environment (a failure of the vessel) |
| S5 | $0.99 \cdot 10^{-2}$ | No release to the flare |
| S6 | $0.99 \cdot 10^{-4}$ | Release to the flare |
| S7 | $1.00 \cdot 10^{-6}$ | Release to the environment (a failure of the vessel) |

The cumulative frequency of release to the environment (sequence S4 and S7) is equal $0.55 \cdot 10^{-5}$ [a$^{-1}$], i.e., 36 times lower than for the case A evaluated in publication (Kosmowski, 2017). If conditional probability $q_2$ = HEP$^X$ = 1 (e.g., for knowledge-based behaviour X = K in complex situation of multiple failures), then the release frequency to the environment would be $1.0 \cdot 10^{-5}$ [a$^{-1}$], i.e., approximately 2 times higher. It shows the importance of careful evaluation of HEPX in probabilistic modelling of physically and functionally dependent systems. It should be emphasised that potential dependent failures in probabilistic modelling of complex architecture systems is challenging and require multidisciplinary research including current achievements of the systems engineering and human factors engineering (IAEA, 2021).

### 5.2. Alarm system design issues to meet functional safety criteria in context of human reliability analysis

Probabilistic models described above enable to effectively perform the functional safety analyses and evaluations during the safety-related control system design regarding protection layers to verify the risk criteria defined by the regulatory institutions in consultation with safety experts. It shows the importance of defence in depth (D-in-D) solutions using, e.g., BPCS, the human operators interacting with AS, and SIS for the risk reduction to meet criteria defined.

Expected reaction time of human operators cannot be too short, i.e., less than 2 - 5 minutes depending on the system complexity and dynamic of processes during transients, abnormalities occurring or major accidents. In such situations the human error probability HEPX, for X = R or K can be high (close to 1), especially for knowledge-based behaviour (X = K). In addition, if the risk reduction required is high, a separate alarm system (AS), physically and functionally independent from the BPCS, is suggested to be considered at the design stage of a layered protection system. Basic safety integrity requirements for the alarm systems are presented in Table 2.

Table 2. Safety integrity requirements for the alarm system (EEMUA, 2007).

| Claimed $PFD_{\text{avg}}$ | AS safety integrity requirements | Human operators' reliability and organizational requirements |
|---|---|---|
| $\geq 10^{-1}$ | Standard AS, may be integrated into BPCS. | No special requirements, however, AS should be designed, operated, and maintained according to a good engineering practice. |
| $[10^{-2}, 10^{-1})$ | AS is designated as safety-related, SIL1, it should be independent from BPCS (unless BPCS is also designed as safety-related). | The alarm presentation arrangement should make the claimed alarm obvious to the operator. The operator must be trained for specific plant failures that the alarm system indicates. The operator should have written clear procedure to support responding correctly and on time to alarms. The required operator response should be simple, obvious, and invariant. The claimed operator performance should be audited and verified in time. |
| $< 10^{-2}$ | AS designated as safety related for SIL2 or higher. | It is not recommended to assume HEP below $10^{-2}$ for any operator action even if there is multiple alarming and task is relatively simple. |

Thus, a correct reaction of operators in abnormal situation or emergency depends on the alarm system (AS) design. Three cases can be considered:

(1) AS is designed as not safety-related (within BPCS treated as not safety-related),

(2) AS is designed as safety-related for the safe-ty integrity level SIL1,

(3) AS is designed as safety-related for the safe-ty integrity level SIL2 or higher.

If the risk evaluated for given industrial installation is high, then AS must be designed as separated from BPCS. To obtain high operational resilience of such system the human factors and human reliability should be adequately shaped. In case (3) of the AS solution it is not recommended to assume in analysis the HEP below $10^{-2}$ for any operator action, even if multiple alarming is applied and the operator task is relatively simple.

## 6. Conclusion

The human factors engineering, and cognitive engineering are important interdisciplinary domains that offer methodological support and new possibilities to deal more systematically with issues of integrated analyses of interactions between humans and complex systems. The safety-related control systems perform nowadays crucial safety functions in industrial hazardous plants. They are usually designed and operated according to the functional safety concept. The objective is to maintain high performance and productivity of industrial installations, and to reduce risks due to existing or emerging hazards and threats.

In the second edition of the functional safety standards IEC 61508 and IEC 61511 the importance of human factors and the human reliability analysis (HRA) is emphasized. These issues should be carefully considered at the design stage of industrial installations and during operation, regarding functions and architectures of the safety-related control systems. However, there are no clear indications in these standards how to support the functional safety analysis and management in this respect. Some characteristic HEP range values are given in the IEC 61511 standard to be assumed by the HRA analysts at low level, e.g., from $10^{-4}$ to $10^{-2}$ for trained operators in no stress conditions, and from 0.5 to 1.0 under stress. Typical HEP for the operator response to alarms was often evaluated in these standards as equal $10^{-1}$. The rationale for these values was not sufficiently explained in mentioned above standards.

The approach has been outlined how to apply the human cognitive reliability (HCR) method for evaluating HEP in the layered protection systems regarding the functional safety requirements. These issues are considered in the context of the SRCS architecture and the alarm system (AS) solution. The HCR method for HEP evaluation for selected behaviour types of human operators (X = S, R or K) seems to be well suited for dealing with probabilistic modelling of the layered protection systems.

Modern alarm system should designed intelligent and effective support of human operators during abnormal events and accidents. It concerns, for instance, presenting of most important, preferably root failure messages, and ranking them regarding importance for safety. An important issue is to avoid confusions with predefined procedures (symptom or root failure oriented) to be followed by human operators during diagnosis and recovery actions. Such support system should cover the operational situations with multiple failures and/or errors.

These issues cannot be satisfactorily solved without applying theoretical findings of system oriented cognitive engineering and human cognitive reliability. Applying the HRA cognitive method, such as HCR or CREAM, is undoubtedly a valuable step in this direction. Some new methods to be developed should be directed towards integrating theoretical findings of the systems engineering (SE), human factors engineering (HFE), cognitive engineering (CE), cognitive reliability (CR), and cyber physical systems (CPS). Thus, it requires further interdisciplinary research.

## References

Adhikari, S. et al. 2009. Human Reliability Analysis: A Review and Critique, Final report of the EPSRC funded project “Rethinking Human Reliability Analysis Methodologies”, Manchester Business School Working Paper No 589.

Bonaceto, C., Burns, K. 2005. Using Cognitive Engineering to Improve Systems Engineering. MITRE Corporation, Bedford.

Bell, J., Holroyd, J. 2009. Review of human reliability assessment methods, Prepared by the Health and Safety Laboratory for the Health and Safety Executive.

Carey, M. 2001. Proposed Framework for Addressing Human Factors in IEC 61508. A Study prepared by Amey VECTRA Ltd. for Health and Safety Executive (HSE), U.K., Research Report 373.

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

Embrey, D. 2000. Task analysis techniques. Human Reliability Associates Ltd.

Froome, P., Jones, C. 2002. Developing Advisory Software to comply with IEC 61508. Contract Research Report 419. HSE Books.

Gersh, J.R., McKneely, J.A., Remington, R.W. 2005. Cognitive Engineering: Understanding Human Interaction with Complex Systems. John Hopkins Technical Digest, Vol. 26, No. 4.

Gertman, I.D., Blackman, H.S. 1994. Human Reliability and Safety Analysis Data Handbook. New York: A Wiley-Interscience Publication.

Hannaman, G.W., Spurgin, A.J. & Lukic, Y.D. 1984. Human cognitive reliability model for PRA analysis. Report NUS-4531, EPRI Project RP2170-3.

Hollnagel, E. 1998. Cognitive Reliability and Error Analysis Method. Elsevier.

IAEA. 2021. Human Factors Engineering Aspects of Instrumentation and Control System Design. Nuclear Energy Series No. NR-T-2.12.

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

IEC 61511. 2016. Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva.

Kirwan, B.: A Guide to Practical Human Reliability Assessment. CRC Press, London (1994)

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

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

Kosmowski, K.T. 2013. Functional safety and reliability analysis methodology for hazardous industrial plants. Gdańsk University of Technology Publishers.

Kosmowski, K.T. 2017. Human Factors and Cognitive Engineering in Functional Safety Analysis. In: Advanced Solutions in Diagnostics and Fault Tolerant Control (Eds. Kościelny, J.M., Syfert, M., Sztyber, A.), Springer.

Kosmowski, K.T. 2023a. Functional safety management in hazardous process installations regarding the role of human operators interacting with the control and alarm systems. In: Intelligent and Safe Computer Systems in Control and Diagnostics (Ed. Z. Kowalczuk). Springer, Lecture Notes in Networks and Systems, Vol. 545, 85–99.

Kosmowski, K.T. 2023b. Operational resilience regarding safety and security aspects of industrial automation and control systems. In Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar, 99-116.

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

Rasmussen, J. 1983. Skills, rules, knowledge; signals, signs and symbols and other distinctions on human performance models. IEEE Transaction on Systems, Man and Cybernetics, SMC-13/3.

Rasmussen, J., Svedung, I. 2000. Proactive Risk Management in a Dynamic Society. Swedish Rescue Services Agency, Karlstad.

Reason, J. 1990. Human Error. Cambridge University Press.

SPAR-H. 2005. Human Reliability Analysis Method, NUREG/CR-6883, INL/EXT-05-00509, US NRC.

SE. 2001. Systems Engineering Fundamentals. defense acquisition university press, Fort Belvoir, Virginia 22060-5565.

Swain, A.D., Guttmann, H.E. 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278. Washington: US Nuclear Regulatory Commission.

Whaley, A.M., et al. 2016. Cognitive Basis for Human Reliability Analysis. NUREG-2114, US NRC.