Functional Safety Analysis including Human Factors

KAZIMIERZ T. KOSMOWSKI

Gdansk University of Technology, G. Narutowicza 11/12, 80-233 Gdansk, Poland.

(Received on November 18, 2009, revised on July 29, 2010)

Abstract: In this paper selected aspects of human factors are discussed that should be taken into account during the design of safety-related functions for a complex hazardous installation and its protections. The layer of protection analysis (LOPA) methodology is used for simplified risk analysis based on defined accident scenarios. To control the risk the safety instrumented functions (SIFs) are identified and their safety integrity levels (SILs) determined based on results of risk assessment. Given SIF is to be realised by the electric/ electronic/ programmable electronic system (E/E/PES) or safety instrumented system (SIS) and the human-operator. The SIL is to be verified according to requirements and criteria given in international standards IEC 61508 and IEC 61511. Some issues concerning the alarm system (AS) designing with regard to human factors and related human reliability analysis (HRA) are outlined.

Keywords: Hazardous plants, functional safety, human factors, human reliability analysis, layer of protection analysis, alarm system.

1. Introduction

The research on the causes of industrial accidents indicate that broadly understood human errors, resulting often from organizational inadequacies, are the main determining factors in 70-90% of cases [22], depending on industrial sector and the plant category. Because several defences against potential accidents are used in hazardous plants 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. They are to be committed during the design, operation and maintenance [6, 22]. 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 or internal disturbances and active human errors, can contribute to major accident with serious consequences. Some categorizations of human actions and related errors have been proposed, e.g., by Swain and Guttmann [30], Rasmussen [24] Reason [27] and Embrey [6].

Traditionally, potential human and organisational influences in industrial plant are to be incorporated into the probabilistic models through the failure events with relevant probabilities evaluated using selected method of human reliability analysis (HRA) [1, 3, 4, 8, 9, 14, 17, 28, 29, 30]. Careful analysis of expected human behaviour (including context oriented diagnosis, decision making and intentional actions) and potential errors is an essential prerequisite of correct risk assessment and rational safety-related decision making, particularly in dynamic situations [11, 12, 13, 17]. The probabilities of the failure...
events depend significantly on various human, organisational, environmental and technical factors being categorised as a set of performance shaping factors (PSFs) relevant to the situation under consideration [6, 18, 19, 20, 26]. The PSFs are divided into internal, stressor and external ones [30].

Lately some new approaches have been proposed by Carey [2], Hickling et al. [10], Froome and Jones [7], and Kosmowski [20, 21] how to deal with the issues of human factors in the functional safety analysis and management [15, 16]. The human errors can be committed in entire life cycle of the plant, from its design stage, installation, commissioning, and operation to decommissioning. During operation phase the human-operator interventions include the supervision and control actions in cases of transients, disturbances and faults as well as the diagnostic activities, the functionality and safety integrity tests, planned maintenance actions and repairs after faults [2, 5, 22].

Nowadays the operators supervise the process and make decisions based on information from the alarm system (AS) and decision support system (DSS) [5, 7, 11, 25], which should be designed especially carefully for abnormal situations and potential accidents, also for cases of partial faults and dangerous failures within the electric, electronic and programmable electronic systems (E/E/PESs) [15] or the safety instrumented systems (SISs) [16]. The AS and DSS, when properly designed, will contribute to decreasing the human error probability in various plant states and reducing the risk of potential accidents with serious consequences.

2. Functional Safety and Human Factors

2.1 Principles of functional safety

Modern industrial installations are extensively computerised and equipped with complex programmable control and protection systems. In designing of the control and protection systems the functional safety solutions [15] are more and more widely of interest and implemented in various industrial sectors, e.g. the process industry [16]. However, there are still methodological challenges concerning the functional safety management in the life cycle. They related also to issues of human and organisational factors [20, 21].

The aim of functional safety management is to reduce the risk associated with operation of hazardous installation to an acceptable or tolerable level introducing a set of safety-related functions (SRFs) that are implemented using the programmable control and protection systems. The human-operator contributes to realization of given SRF through relevant HMI (human machine interface) in relation to the SCADA (supervisory control and data acquisition) system or DCS (digital control system). In the standard [16] 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 [11, 22, 30].

An important term related to the functional safety concept is the safety integrity [15], understood as the probability that given safety-related system will satisfactorily perform required SRF under all stated conditions within given period of time. The safety integrity level (SIL) is a discrete level (1÷4) for specifying the safety integrity requirements of given safety-related function to be allocated using the electrical/ electronic/ programmable electronic system (E/E/PES) [15] or safety instrumented system (SIS) [16]. The safety integrity level of 4 (SIL4) is a highest level, which requires - when
implemented in industrial practice - a complex architecture of E/E/PES consisting of redundant subsystems being diagnosed on-line and periodically tested.

For the E/E/PES or SIS performing SRF two probabilistic criteria are defined for consecutive SILs (Table 1), namely [15]:
- 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.

Table 1: Probabilistic Criteria for Safety-related Functions

<table>
<thead>
<tr>
<th>SIL</th>
<th>( PFD_{avg} )</th>
<th>( PFH ) [h(^{-1})]</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>([10^{-5}, 10^{-4}])</td>
<td>([10^{-9}, 10^{-8}])</td>
</tr>
<tr>
<td>3</td>
<td>([10^{-4}, 10^{-3}])</td>
<td>([10^{-8}, 10^{-7}])</td>
</tr>
<tr>
<td>2</td>
<td>([10^{-3}, 10^{-2}])</td>
<td>([10^{-7}, 10^{-6}])</td>
</tr>
<tr>
<td>1</td>
<td>([10^{-2}, 10^{-1}])</td>
<td>([10^{-6}, 10^{-5}])</td>
</tr>
</tbody>
</table>

The SIL for given SRF is determined in the risk assessment process using a defined risk matrix, which includes areas for several risk classes, e.g., unacceptable, moderate and acceptable or a risk graph [15, 22].

The E/E/PE safety-related system (see Figure 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) [15]. 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.

Figure 1: E/E/PE Architecture for Realization of Safety-related Functions

2.2 Determining SIL of a safety-related function

The risks associated with accident scenarios can be presented on a risk matrix (Fig. 2) with distinguishing several categories of consequences (\( N^A, N^B, \ldots \)) and frequencies (\( F^0, F^1, \ldots \)), defined as intervals with decreasing exponent of the upper and lower limits on logarithmic scales.

The risk control options should be carefully considered during the design or operation of hazardous industrial systems [22]. Given risk control option (RCO) includes a technical and/or organisational solution, which differs from a basis (B) solution fulfilling some basic requirements. It can be in particular a safety-related function (SRF) to be implemented using E/E/PES or SIS.
As it can be seen in Figure 2 in an area of unaccepted risk (class I) and undesired risk (class II) there are four stars denoted a, b, c and d in order of increasing losses. The risk reduction will be considered on example of point b. Implementing a protection measure, e.g., SIS within protection layers [16] moves the risk coordinates in arrow direction to point b* with relevant reduction of the frequency and consequence of given scenario. If we assume that introducing additional protection will not reduce the losses, but only the frequency of this accident scenario, then the risk coordinates will move to point b**.

The aim is to reduce the frequency at least of two orders of magnitude (to decrease 100 times) or better three orders of magnitude thanks to introducing, for instance, additional safety-related function to be implemented using relevant protection layers (see chapter 3). The implementation of given RCO results in the risk reduction, evaluated for the period of one year, as follows [22]

$$
\Delta R^{RCO} = \sum F^{p} N^{x, R} (1 - r^{f, RCO} r^{x, RCO})
$$

where: $F^{p}, N^{x, R}$ - the frequency [a$^{-1}$] and the consequence $x$ [in units of consequence] of $k$-th accident scenario for the basic solution $B$; $r^{f, RCO}$ - the relative reduction of the frequency for $k$-th accident scenario after implementing given RCO ($r^{f, RCO} = F^{RCO} / F^{p}$); $r^{x, RCO}$ - the relative reduction of the consequence $x$ for $k$-th accident scenario after implementing given RCO ($r^{x, RCO} = N^{RCO} / N^{x, p}$). As consequence $x$ the mortality or economic losses due to given accident scenario can be considered.

Assuming that the risk reduction to a tolerable level can be achieved implementing E/E/PES or SIS for the constant consequences ($N = const$), the relative risk reduction can be evaluated as follows:

$$
r^{R} = R_{t} / R_{op} = F_{t} / F_{op} = r^{R}
$$

where: $F_{t}$ is numerical target frequency of potential hazardous event (specified for a tolerable risk level); $F_{op}$ - the frequency of potential hazardous event that could occur.
without protection; the relevant risk indices for these two cases are: \( R_t = F_t N \) and \( R_{op} = F_{op} N \) \((N = \text{const})\).

In case of E/E/PES or SIS considered for implementing within the protection layer for a low demand mode of operation the value of \( F \) is equivalent to the average probability of failure on demand \( PFD_{avg} \), i.e. \( PFD_{avg} = F \). This value is used for determining required SIL of given safety-related function to be implemented using appropriate architecture of E/E/PES or SIS. In verifying the SIL, usually some architectures of E/E/PES or SIS are considered, and the results of probabilistic modelling are to be compared with interval probabilistic criteria given in Table 1.

2.3 Human Reliability Analysis

The human reliability analysis (HRA) methods are used for assessing the contribution of potential human errors in failure events of given accident scenarios. However, some basic assumptions made in HRA techniques used within probabilistic safety analysis of hazardous systems are still a subject of dispute between researchers [3, 12, 13].

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 concerning human behaviour and potential errors. Hollnagel concludes [13] that some HRA results are of limited value as input for PSA (probabilistic safety analysis), mainly because of oversimplified conception of human performance and human error. On the other hand, it is obvious that it is valuable to consider required human actions and potential errors in given context with regard to the process dynamic, functions of the control and protection systems, quality of HMI (human-machine interface), etc. Examples of potential human errors in a dynamic system and their consequences are presented in Figure 3.

![Figure 3: Examples of Human-operator Errors and their Consequences](image)

In spite of mentioned criticism, waiting for a next generation of HRA methods, the human factor analysts use in PSA some exiting HRA methods. Below some HRA methods are shortly characterized that might be applied in the context of functional safety analysis. The rough human reliability assessments based mainly on qualitative information concerning relevant factors can be useful at the designed stage of safety-related functions and E/E/PES systems implementing these functions [2, 22]. It is justified to emphasise that the functional safety analysis framework gives additional insights in HRA [22, 23].
In performing HRA some basic knowledge concerning concepts of human behaviour and error types is necessary. Rasmussen [24, 25] proposes the distinction of three categories of human behaviour: skill-based, rule-based and knowledge-based. HRA practitioners know that the distinction between a skill-based action and a rule-based action resulting to errors is not always trivial and requires the context oriented analysis by experienced expert. Similar difficulty is also associated with the distinction between a rule-based or knowledge-based behaviour and potential errors [22].

Described above behaviour types seem to involve different error mechanisms, which may mean radically different human reliability characteristics. Reason [27] proposes following classification of human errors: a slip - an attention failure (for example, an error in implementing a plan or decision, or an unintended action); a lapse - a momentary memory failure (for example, an error to recalling a task step or forgetting intentions); and a mistake - an error in establishing a course of actions, for example, an error in diagnosis, planning or decision making. Thus, mistakes are associated with more serious error mechanisms as they lead to incorrect understanding of abnormal situation and conceiving an inappropriate plan of actions.

These two frameworks can be combined as it is shown in Figure 4. Three error types are distinguished: I - skill-based, II – rule-based, and III – knowledge-based. A skill-based error is associated with slips or lapses. Rule- or knowledge-based errors are related to mistakes.

![Figure 4: Classification of Human Unsafe Acts and Error Types](image)

Several HRA techniques are used in PSA practice, e.g. THERP [30], developed for the nuclear industry, but applied also in other industrial sectors. Other HRA methods, more often 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). These HRA methods are characterised in various papers, monographs and reports [1, 3, 8, 14, 17]. In the publication [1] five HRA methods were selected for comparison on the basis of either relatively widespread usage, or recognized as a contemporary technique, e.g. the SPAR-H method [29].

The results of research indicate that the HEP (human error probability) in a dynamic system depend strongly on the time available for the diagnosis, decision making and actions. In Figure 5 the results of a nominal diagnosis model is presented for evaluating HEP of diagnosis within time T by the control room personnel for one abnormal event.
The HEP is evaluated when the human failure event is placed into the probabilistic model structure of the system. In the HRA performed within PSA only more important human failure events are considered [17, 22, 30]. Then, the abnormal situation context and related performance shaping factors (PSFs) are identified and evaluated according to rules of given HRA method. As the result a particular value of HEP is evaluated.

Different approaches are used for evaluating HEP with regard to PSFs, e.g. assuming a linear relationship for each identified \( PSF_j \) and its weight \( w_j \), with constant \( C \) for the model calibration

\[
HEP = HEP_{\text{nominal}} + \sum_{j} w_j PSF_j + C
\]  

(3)

or nonlinear relationship used in the SPAR-H methodology [29],

\[
HEP = \frac{NHEP \cdot PSF_{\text{composite}}}{NHEP(PSF_{\text{composite}} - 1) + 1}
\]  

(4)

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

An appreciated method for performing HRA for a set of PSFs is SLIM [14, 17]. The SLIM is oriented on success probabilities of events to accomplish specified tasks. Probabilistic modelling in the risk analysis is rather failure oriented and it is more convenient to apply a modification of SLIM method named SI-FOM (Success Index - Failure Oriented Method) [19]. The equations including the human failure probabilities \( HEP_j \) and the success indices \( SI_j \) for \( j \)-th task are as follows

\[
\log HEP_j = c \cdot SI_j + d
\]  

(5)

\[
SI_j = \sum_i w_i r_i
\]  

(6)

where: \( w_i \) - normalised weight coefficient assigned to \( i \)-th influence factor (\( \sum w_i = 1 \)), \( r_i \) - scaled rating of \( i \)-th factor in \( j \)-th task (normalised scaling value is \( 0 \leq r_i \leq 1 \)). If for cases considered the success indices \( SI_j \) are evaluated and two probabilities \( HEP_j \) are known (preferably with min and max values of HEP for a category of tasks considered) then coefficients \( c \) and \( d \) can be determined and HEP calculated for a particular task of interest in probabilistic modeling of events.
2.4 Human Factors in Functional Safety Analysis

Lately, a framework [2] was proposed for addressing human factors in IEC 61508. Consideration was given to a range of applications of the E/E/PE systems in safety-related applications. The diversity of ways in which human factors requirements map on to various E/E/PE systems in different industries and contexts has been highlighted in this framework depending on the safety integrity level (SIL) required and functions performed by personnel. Obviously, the effort that needs to be placed into operations including maintenance in relation to human factors should be greater as the SIL increases, but the types of human factors that need to be addressed vary between the classes of systems.

A framework to be developed for addressing human factors (HFs) within IEC 61508 should include:

- incorporating human tasks and potential errors into the hazard and risk assessment,
- defining the human factor requirements for defined safety-related functions to be realized on determined SILs,
- verifying SIL for consecutive safety related functions for solutions proposed with regard to hardware, software and human factors.

The requirements concerning the scope of analyses fall into two broad categories: (1) those associated with hazard and risk analysis (all relevant issues of human and organizational factors, procedural actions and human errors, abnormal and infrequent modes of operation, reasonably foreseeable misuse, claims on operational constraints and interventions, etc.); and (2) those concerning the operator interface (take account of human capabilities and limitations, follow good human factor practice, be appropriate for the level of training and awareness of potential users, be tolerant of mistakes, etc.). Thus, the scope of analyses should include human and organizational factors taking into account relevant context specific aspects.

Generally, the requirements concerning the analysis of human factors in functional safety solutions increase for higher SILs of E/E/PE systems. Several categories of such systems can be distinguished [2, 22]: control and protection, supervisory control, remote control, diagnostics, alarms, communication, and offline analysis and support tools. For instance for SIL 2 following analyses and requirements are suggested [2, 22]:

- key tasks to be performed by operations and maintenance staff have been identified,
- typical operating environments have been identified and described,
- the conceptual design of the user interface is documented as a design deliverable,
- critical tasks and aspects of the human factors have been identified and subjected to systematic, documented review by the design team,
- all staff who operate or maintain the equipment have successfully completed training that covers all relevant aspects of the equipment and its application.

2.5 Probabilistic Modeling of E/E/PES or SIS for verifying SIL

The probability of failure on demand $PFD_{avg}$ of the E/E/PE safety-related system (S) is evaluated taking into account subsystems A, B and C (assuming small values of relevant probabilities) from the formula

$$PFD_{avg}^S = PFD_{avg}^A + PFD_{avg}^B + PFD_{avg}^C$$

(7)

where $PFD_{avg}^A$, $PFD_{avg}^B$, $PFD_{avg}^C$ are probabilities of failure on demand for subsystems A, B and C (see Fig. 1).

The HEP is evaluated when a human failure event is placed into the structure of probabilistic model of the system. Some attributes (factors) of such event are determined
according to rules of given HRA method. Then a particular value of HEP is calculated. In the HRA within PSA only more important human failure events are considered for further context specific analysis [17].

In the case of probabilistic modelling of the E/E/PE safety-related system the human failure event and its probability is an element of subsystem model as explained below. For instance, \( PFD_{avg} \) of a E/E/PE subsystem (SUB), operating in the low demand mode is calculated (for subsystem A, B or C) from formula:

\[
PFD_{avg}^{E/E/PE} = PFD_{avg}^{RT} + PFD_{avg}^{ST} + HEP
\]

where \( PFD_{avg}^{RT} \) is average probability of subsystem failure on demand to be detected in periodical functional test (FT); \( PFD_{avg}^{ST} \) – the probability of subsystem failure on demand, detected in automatic tests (AT); \( HEP \) – the human error probability.

Depending on the subsystem and safety-related function considered the human error can be a design error (hardware or software related) or an operator error for considered activities of the operator in the control room or at site within maintenance group.

For instance, the probability of failure on demand for 1oo2 subsystem, including in probabilistic modelling the common cause failures and/or human error probability (HEP), can be calculated from formula

\[
PFD_{avg_elec} = \left(1 - \beta \right) \left( \frac{1}{3} T + T_{MTTR} + T_{MTTR}^2 \right) + \beta \lambda_{DU} \left( \frac{T_f}{2} + MTTR \right) + HEP
\]

where \( \beta \)-factor for dependent failures of two channels, \( \lambda_{D} \) – a dangerous failure rate of one channel; \( \lambda_{DU} \) – a dangerous undetected failure rate, \( T_f \) - the interval of periodical tests; \( MTTR \) – the mean time to repair.

3. Layer of protection analysis including human factors

Hazardous industrial plants are designed according to a concept of defense in depths using several barriers (protection layers). Figure 6 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 [23]. It is important to include in probabilistic modelling of protection layers potential dependencies between events representing equipment failures and human errors.

![Figure 6: Typical Protection Layers in Hazardous Industrial Installation](image-url)
- PL1 – the basic process control system (BPCS),
- PL2 – the human-operator (OPERATOR), who supervises the process and intervene in cases of abnormal situations and during emergencies that are indicated by the decision support system (DSS) or the alarm system (AS),
- PL3 – the safety instrumented system (SIS), which can perform an emergency shutdown (ESD) function.

![Diagram of Protection Layers]

**Figure 7:** OPERATOR and Alarm System (AS) as elements of Protection Layers

These layers should be independent what requires appropriate technical and organizational solutions. In case of PL1 and PL3 it can be achieved using separate measurement lines (input elements), modules for information processing (PLCs) and actuators (final elements). Required SIL of BPCS and SIS for given safety-related function can be achieved by designing appropriate architectures of their subsystems (see Figure 1) taking into account the probabilistic criteria given in Table 1 for verifying SIL of SIS.

If the risk reduction requirement concerns the protection layers according to formula (2) the required risk reduction should be properly distributed between BPCS, OPERATOR and SIS, e.g. if $10^{-4}$ is for all layers then it should be is distributed as follows: $10^{-1}$ (SIL1), $10^{-1}$ (HEP-SIL1) and $10^{-2}$ (SIL2), which are values achievable without difficulty in industrial practice.

There is, however, a considerable problem in some cases concerning the layer PL2, i.e., OPERATOR who obtains information through relevant HMI from the alarm system (AS) and/or decision support system (DSS). Only in case of independence of these layers the frequency of $i$-th accident scenario $F_i$ can be calculated from the formula

$$F_i = F'_i \cdot PFD_{i,PL1} \cdot PFD_{i,PL2} \cdot PFD_{i,PL3} = F'_i \cdot PFD_{i,j}$$

(10)

where $F'_i$ is the frequency of $i$-th initiating event $I[a^{-1}]$ and $PFD_{i,PLj}$ are probabilities of failure on demand of $j$-th protection layer shown in Figure 7. In case of the second layer $PFD_{i,PL2} = HEP_{i,PL2}$ and relevant HEP is evaluated using appropriate HRA method.

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

$$F^x_i = F'_i \cdot P(X_{i,PL1} | I) \cdot P(X_{i,PL2} | I \cdot X_{i,PL1}) \cdot P(X_{i,PL3} | I \cdot X_{i,PL2}, X_{i,PL1}) = F'_i \cdot PFD^x_i$$

(11)

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

The results of 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 $PFD^x_i >> PFD_i$ - see formulas (10) and (11). Significant meaning in reducing dependencies of mentioned layers has appropriate designing of the
alarm system (AS) and decision support system (DSS) as well as the quality of HMI characterized by relevant factors that are assessed when performing the HRA.

4. Requirements and Criteria concerning the Alarm System and Operator Interface

As it is mentioned in international standards [15] and [16], there is not clear guidance how to include human and organizational factors in functional safety analysis. They should be, however, included in designing the human - machine interface (HMI), e.g., within the decision support system (DSS) and especially the alarm system (AS). Some suggestions are given in a report [2], guide [5] and the HSE book [7].

The alarm system refers to a complete system for generating and handling alarms including field equipment, signal conditioning and transmission, alarm processing and alarm display. It also includes hardware, software and supporting information, e.g., alarm response procedures and management controls. The alarm is defined as an audible or visible means of indicating to the operator the equipment or process malfunction or abnormal condition. The alarm trip point is a threshold value or discrete state of a process variable that triggers the alarm. The alarm flood (overload) is the situation where more alarms are received than can be physically addressed by a single console operator [5].

The attention should be focused on tasks that operator must perform in relation to cope with controlling upset situations according to designed HMI solutions. Depending on complexity of the tasks and required reliability of the protection layers, expressed for instance by the safety integrity level (SIL), requirements for the operator performance can vary and increase for higher SIL.

After making decision during abnormal situation the operator must execute some actions correctly according to prescribed procedures or established practice. All tasks performed or executed by operator can be supported by DSS, which should be an integrated part of HMI related to BPCS, SIS and/or AS. In case of incorrect diagnosis or no reaction on time (see the event sequences in Figure 3) during an abnormal event, e.g. due to complexity or fast dynamic of the process, the ESD (emergency shutdown) system should operate without operator intervention to stop technological process by executing required functions to mitigate the consequences.

The basic issue in designing an alarm system is considering its functionality in relation to identified diagnostic difficulties and characteristics of technical solutions. In particular the answers for two basic questions are of interest [5]:

(1) Whether the AS should be classified as safety related according to the definition given in the functional safety standard [15]? and
(2) Whether it should be implemented as a stand-alone system independent of the basic process control system?

The decision whether AS is safety-related will be influenced by national legislation or by existing practices within given industrial sector. For alarms that are safety-related, according to definition in the standard [15], should be given special consideration in terms of designing HMI and DSS. If the alarm system is safety-related, it should be independent and separate from the process control system, unless the process control system has been itself identified as safety-related and implemented in appropriate manner [15, 16].

The risk assessment provides a starting point in the design process of DSS including alarms. The risk reduction to be achieved by the alarm system solution depends on:
- the reliability of equipment (i.e., field instrumentation and alarm processing system),
- the reliability of the operator responding to the alarm with appropriate action.
The reliability of the human-operator (or a team of operators) performing tasks will in turn depend on such factors as:
- the way in which alarms are presented (technical solution and ergonomics),
- the time available for the operator to diagnose the situation, elaborate decisions and undertake actions,
- the stress level,
- other factors, e.g., distraction, forgetfulness, negligence [14, 27, 29, 30].

The experience shows that majority of AS failures derive from human failures rather than from hardware failures [5]. In practice, the risk reduction benefits are generally more easily derived from improving functionality and usability than from improving hardware integrity. Thus, in the context of alarm system functions:
- the operator should not be overloaded with alarms presented by the chosen display arrangement, either in normal operation or upsets,
- the AS performance should be regularly checked to ensure that alarm overload is not occurring,
- the alarms presented by the chosen display arrangement should be operationally useful with significant limitation of spurious annunciations,
- the alarms should be properly prioritized,
- the operator should be trained in using the AS.

Figure 8 presents an example of qualitative approach for deciding about a basic solution of the alarm system (AS) which might be implemented within the basic process control system (BPCS) or designed as a stand-alone safety-related AS. Depending on the risk parameters: the expected consequences (from S1 to S5) and diagnosis difficulties of hazardous installations in a short time T0 or T1 (T0 – quick response essential \( \leq 5 \) min.; T1 – slow response adequate \( > 5 \) min.) an alarm system suggested solution is selected from appropriate column: N – not suitable as alarm, L – limited benefit, C – an alarm within basic control system recommended, P – the alarm either in stand-alone or control system acceptable, S – the alarm within stand-alone system recommended.

It is worth to mention that a threshold value of 5 minutes assumed in defining T0 and T1 is related to difficulties to diagnose abnormal situation in a dynamic system in relatively short time with a high probability to commit error (see Figure 5).

For the safety-related alarm system more stringent reliability requirements should be imposed on both equipment and expected human performance summarized in Table 2.
Table 2: Reliability Requirements concerning the Safety-related Alarm System and Human Operator (adapted from [5])

<table>
<thead>
<tr>
<th>Claimed $PFD_{avg}$</th>
<th>AS integrity / reliability</th>
<th>Human reliability requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>$&gt; 10^{-1}$</td>
<td>Standard AS, may be integrated into BPCS</td>
<td>No special requirements – the AS should be operated and maintained with regard to good engineering practice [5]</td>
</tr>
<tr>
<td>$(10^{-2}, 10^{-1})$</td>
<td>AS designed as safety-related for SIL1 [15]; it should be independent from BPCS (unless this is designed also as safety-related)</td>
<td>The operator should be well trained for specific expected plant failures that the alarm system indicates. The operator should have clear response procedures for important alarms and claimed operator performance should be audited.</td>
</tr>
<tr>
<td>$\leq 10^{-1}$</td>
<td>AS designed as safety-related for SIL2 [15];</td>
<td>It is not recommended to claim $HEP$ below $10^{-4}$ for any operator action even if it is multiple alarmed and relatively simple to perform.</td>
</tr>
</tbody>
</table>

It is recommended that for all credible accident scenarios the designer should demonstrate that total number of safety-related alarms and their maximum rate of presentation does not overload the operator. It might be interpreted as requirement that no credible accident generates more than a certain number of safety-related alarms within specified period. There is a general guidance on alarm rate following an upset condition of the installation, expressed as a number of alarms displayed in 10 minutes following a major plant upset [5]:
- more than 100 – definitely excessive and it is very likely to lead to the operator abandoning the alarm system,
- between 20 and 100 – it is hard to cope with,
- under 20 – should be manageable, but may be difficult if several alarms require a more complex operator response.

From Figure 8 and Table 2 some basic assumptions for designing the AS might be derived. In case of a high risk and quick response required the AS should be safety-related and stand-alone. Designing of such system according to functional safety principles is generally described in international standard IEC 61508 [15]. Some suggestions for the human reliability analysis in relation to functional safety concept can be found in report [2] and monograph [22].

In the layer of protection analysis using of formula (10) is justified only if the AS was designed as separate and independent from BPCS (see Figure 7). The AS, if carefully designed with good HMI and DSS functions, will certainly contribute to reduction of the human error probability [5, 8, 22].

As it was mentioned in evaluation of the human-operator reliability, various methods have been used in practice, e.g., THERP [30], HEART and SLIM [14, 17]. However, significant problems emerge when cognitive aspects of human-operator behavior and decision making are considered [22], for instance in cases when latent failures contribute to the active failure probability and in cases of potential multiple failures. Such challenging problems require further research to be oriented on developing an intelligent DSS and effective AS contributing to the risk reduction associated with the operation of hazardous industrial plants.

Another issue that requires further research is developing the methodology for designing and assessing the advisory software for supporting on-line safety-related decision making. It should comply with the requirements of functional safety standards [7,
The basic principle concerning the safety-related functions of such software can be stated as follows: it must not mislead the user (human-operator) to undertake decisions that could contribute to deteriorating abnormal plant states. Obviously, relevant advisory system should be intuitive for operators with advanced and safe interactive mechanisms to support effectively diagnosis of abnormal plant states including spurious operation of the control and protection systems. Thus, the functional safety analysis framework for the safety-related control and protection systems provides additional insight for performing human reliability analysis and determining more important factors influencing the risks.

5. Conclusion

In this paper an approach is outlined that includes selected aspects of the functional safety analysis in hazardous installations including the protection layers. In particular the role of alarm system is emphasized, which requires appropriate designing with regard to careful treating of human factors. Nowadays issues concerning the functional safety management in industrial hazardous plants with regard to the human and organizational factors become important due to necessity to design human oriented solutions. They include the human-operator support system and especially the alarm system. If the alarm system is safety-related, it should independent and separated from the basic process control system.

It is required to manage the functional safety in entire safety lifecycle keeping the risk level of potential hazardous events at acceptable levels. Thus, it is essential to improve, when justified, the basic process control system (including SCADA and DCS solutions) and other safety-related solutions including the alarm system and decision support system. The safety management has to be carried out in the life cycle based on reliability data and experience from the plant operation and periodical risk assessments. It is essential to consider carefully the human and organizational factors using relevant HRA methods to maintain adequate risk associated with operation of particular hazardous plant.

The functional safety oriented framework offers additional possibilities for more comprehensive human reliability analysis with emphasis on contextual human-operator behaviour in abnormal situations, also those related to danger failures of the control and protection systems. Such analysis provides understanding how to design the safety-related hardware solutions and functions to be implemented by means of the basic process control system, the alarm and decision support system, and the safety instrumented systems. Their integrated design should be human-centred.

Such design process requires an integrated approach with regard to requirements and criteria related to ergonomics, human factors and functional safety of the control and protection systems. Additional research is needed to obtain more comprehensive insights related to the reliability and safety aspects useful for designing human-centred interactive solutions within hazardous dynamic systems.

Acknowledgements: The author wishes to thank the Ministry for Science and Higher Education in Warsaw for supporting the research and the Central Laboratory for Labour Protection – National Research Institute (CIOP-PIB) in Warsaw for co-operation in the preparation of the research project 5.R.02, concerning the safety management in industrial hazardous plants including functional safety aspects, being carried out within a multiyear research programme.
References


Kazimierz T. Kosmowski is Professor and Head of Automatics Department at the Faculty of Electrical and Control Engineering of the Gdansk University of Technology. His field of interest includes mathematical modeling of safety and reliability of complex technical systems and processes including human factors. He has published over 190 scientific works. He is the vice chairman of Polish Safety and Reliability Association.