Kosmowski Kazimierz
Gdansk University of Technology

Functional safety analysis including human factors

Keywords

hazardous plants, functional safety, human factors, layer of protection analysis, alarm system

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. In such installations the layer of protection analysis (LOPA) methodology is often 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 with regard to 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. Selected issues related to designing the alarm system (AS) with regard to human factors are outlined. Some aspects of human reliability analysis (HRA) as a part of human-machine interface (HMI) assessing and probabilistic modelling of the system are shortly discussed.

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 [22], 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 [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/internal disturbances or 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 & Guttmann [30], Rasmussen [24] Reason [27] and Embrey [6].

Traditionally, potential human and organisational deteriorating 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 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 categorised usually as a set of performance shaping factors (PSFs) relevant to the situation under consideration [6], [18], [19], [20], [26]. The PFSs are divided into internal, stressor and external ones [30].

Lately some new approaches have been proposed by Carey [2], Hickling et al. [10], Froome & Jones [7] and Kosmowski [20], [21] how to deal with the issues of human factors in the functional safety 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 the human-operator interventions include the 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 using the alarm system (AS) and decision support system (DSS) [7], [5], [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 the control and protection systems the functional safety solutions [15] are more and more widely of interest or already implemented in various industrial sectors, e.g. the process industry [16]. However, there are still methodological challenges concerning the functional safety management in life cycle related among other things to human and organisational factors [20].

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 to be implemented using the programmable control and protection systems. 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), known also as BPCS (basic process control system), and SIS (safety instrumented system) 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 the highest level, which requires a complex architecture of E/E/PES consisting of redundant subsystems being diagnosed 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

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 using 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 (*Figure 1*) consists of 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 generally KooN architecture, e.g. 1oo1, 1oo2, 1oo3 or 2oo3.

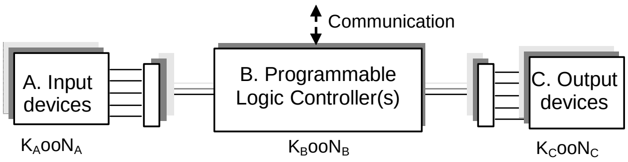


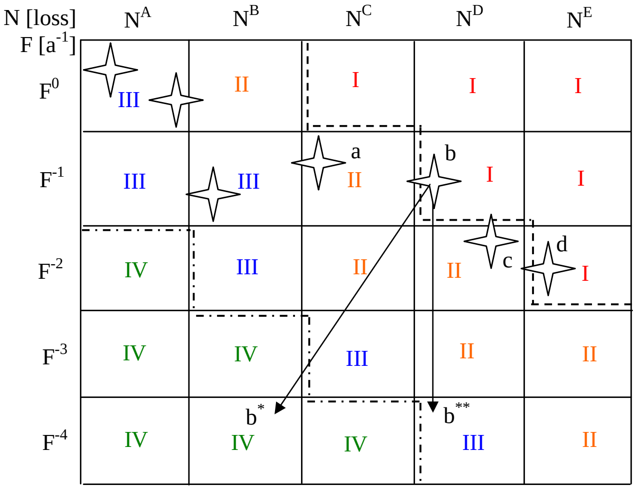
Figure 1. E/E/PE architecture for realization of safety-related functions

Verifying SIL of given safety-related functions to be implemented using the E/E/PES or SIS is usually a challenging task due to scarcity of reliability data and other data used as parameters in probabilistic models of the system in design or operation. In such situation, a qualitative method for crude SIL verifying is suggested in IEC 61508 to assess the architectures considered at the design stage.

2.2. Determining SIL of a safety-related function

The risks associated with accident scenarios are often presented on a risk matrix (*Figure 5*) with distinguishing several categories of consequences (N^A, N^B, …) and frequencies (F^0, F^{-1}, …), defined usually as intervals on logarithmic scales.

The risk control options should be carefully considered during 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.



N [loss] F [a⁻¹]	N^A	N^B	N^C	N^D	N^E
F^0	III	II	I	I	I
F^{-1}	III	III	II	I	I
F^{-2}	IV	III	II	II	I
F^{-3}	IV	IV	III	II	II
F^{-4}	IV	IV	IV	III	II

Figure 2. An example of risk analysis results in relation to categories of frequencies and losses for four classes of risk

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 reduction will move to point b**. It can be seen in *Figure 2* that first of all two accident scenarios - b and d should be analyzed in details, because they contribute to the risks belonging to unaccepted area. The aim is to reduce the frequency at least of three orders of magnitude (decreasing of 1000 times) 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]

$$\Delta R^{x;RCO} = \sum_k F_k^B N_k^{x;B}(1 - r_k^{F;RCO} r_k^{N;RCO}) \qquad (1)$$

where: $F_k^B, N_k^{x;B}$ - the frequency [a^{-1}] and the consequence x [in *units of consequence*] of k-th accident scenario for the basic solution B; $r_k^{F;RCO}$ - the relative reduction of the frequency for k-th accident scenario after implementing given RCO ($r_k^{F;RCO} = F_k^{RCO} / F_k^B$); $r_k^{N;RCO}$ - the relative reduction of the consequence x for k-th accident scenario after implementing given RCO ($r_k^{N;RCO} = N_k^{x;RCO} / N_k^{x;B}$).

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 is to be evaluated as follows

$$r^R = R_t / R_{np} = F_t / F_{np} = r^F \qquad (2)$$

where: F_t is numerical target frequency of potential hazardous event (specified for a tolerable risk level); F_{np} - 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 $R_{nsp} = F_{nsp} N$.

In case of E/E/PES or SIS considered for implementing within the protection layers the value of r^F is equivalent to the average probability of failure on demand PFD_{avg}, i.e. $PFD_{avg}=r^F$. This value is used for determining required SIL of 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 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, in particular accident scenarios. The general aim is to reduce the system vulnerability, which operates in given environment. However, some basic assumptions made in HRA methods used within probabilistic safety analysis of hazardous systems are still the 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. However, there is no doubt that potential human errors should be considered in given context (process dynamic, automation, protection, HMI). Examples of potential human errors in a dynamic system and their consequences are presented in *Figure 3.*

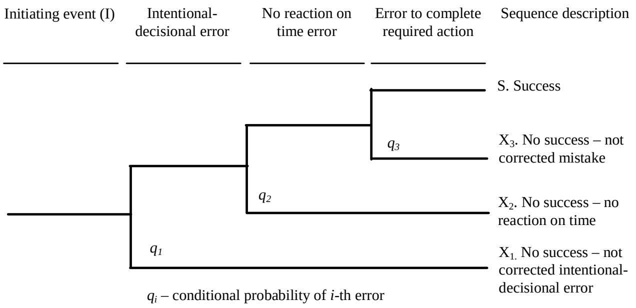

Initiating event (I)
Intentional-decisional error
No reaction on time error
Error to complete required action
Sequence description
S. Success
q_3
X3. No success – not corrected mistake
q_2
X2. No success – no reaction on time
q_1
X1. No success – not corrected intentional-decisional error
q_i – conditional probability of *i*-th error

Figure 3. 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 some HRA methods are shortly characterized that might be applied in the context of functional safety analysis. The rough human reliability assessments based on qualitative information concerning relevant human factors can be useful at the designed stage of safety-related functions and E/E/PESs implementing theses functions [2], [22].

It is justified to emphasise that the functional safety analysis framework, including the safety-related functions to be implemented using the control and protection systems as well as assumptions concerning HMI solution in relation to the alarm system (AS) and decision support system (DSS) gives additional insights in HRA [22].

In performing HRA some knowledge concerning concepts of human behaviour and error types is necessary. Rasmussen [24], [25] proposes the distinction of three categories of human behaviour. His conceptual framework assumes three cognitive levels of human behaviour:

- *skill-based* (highly practiced tasks that can be performed as more or less subconscious routines governed by stored patterns of behaviour),
- *rule-based* (performance of less familiar tasks in which a person follows remembered or written rules), and
- *knowledge-based* (performance of novel actions when familiar patterns and rules can not be applied directly, and actions follow the information processing with the inclusion of diagnosis, planning and decision making).

Figure 4 illustrates this concept, which is useful in analysis of human behaviour and potential errors.

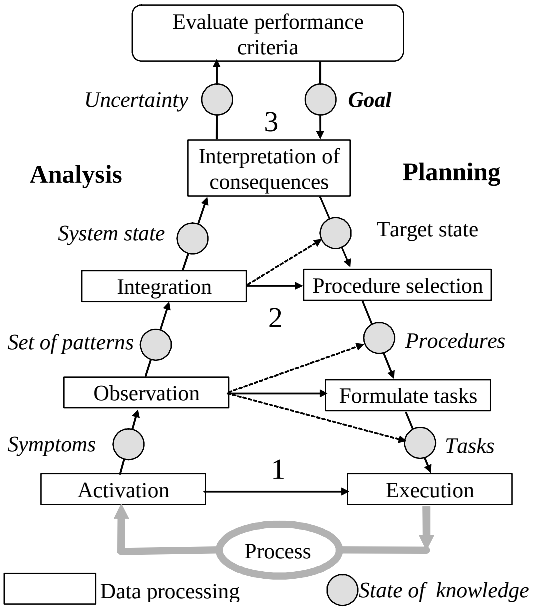


Figure 4. Schematic representation of information processing by operators and human behaviour types (1 - *skill*, 2 - *rules*, 3 – *knowledge*)

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* - is an attention failure (for example, an error in implementing a plan or decision, or an unintended action);
- *a lapse* - is a momentary memory failure (for example, an error to recalling a task step or forgetting intentions);

- *a mistake* - is an error in establishing a course of actions, for example, an error in diagnosis, planning or decision making.

Thus, slips and lapses are unintended actions. They can occur during the execution of skill-based actions. However, mistakes are intended actions. They are committed, e.g. when the knowledge-based actions are planned and executed. Mistakes are associated with more serious error mechanisms as they lead to incorrect understanding of abnormal situation and conceiving an inappropriate plan of actions. Mistakes can also occur in selection and execution of rule-based actions, for example, due to inappropriate selection of a procedure.

A classification of human unsafe acts and error types is presented in *Figure 5*, which combines two frameworks outlined above. 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.

Another category of unsafe acts is violation (exceptional or routine) that includes the acts of sabotage and other malicious acts. These are intentional acts that are very difficult to treat in probabilistic risk analysis, similarly as potential terrorist attacks. They are nowadays included rather in security-oriented analyses [22].

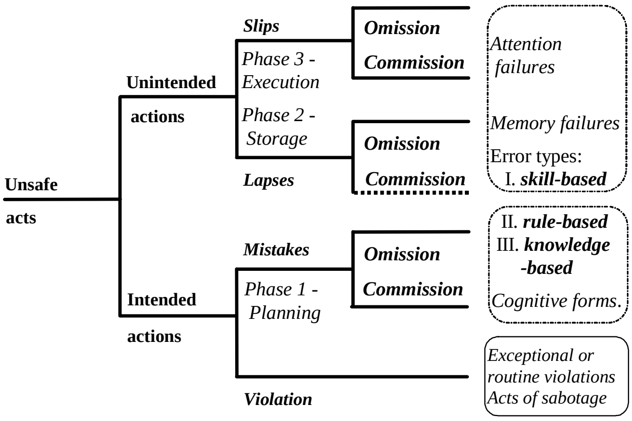


Figure 5. Classification of human unsafe acts and error types

Several traditional HRA methods are used in PSA practice, e.g. THERP method [30], developed for the nuclear industry, but applied also in various 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 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 have been also examined to provide insights concerning the treatment and evaluation of human error probabilities (HEPs) for situations encountered in practice of probabilistic modelling. Comparisons were also made in relation to the SPAR-H method [29]. The final conclusion is that the enhanced SPAR-H methodology is useful as an easy-to-use, broadly applicable, HRA screening tool.

The results of various research indicate that HEP in a dynamic system depend strongly on the time available for the diagnosis, decision making and actions. In *Figure 6* the results of a nominal diagnosis model is presented for evaluating HEP for diagnosis within time T of one abnormal event by the control room personnel.

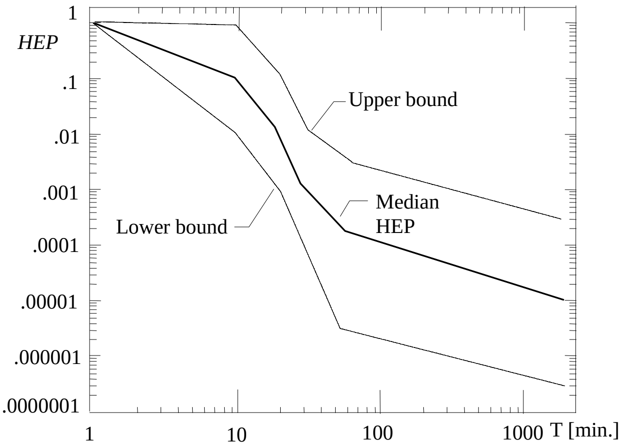


Figure 6. Human error probability for diagnosis within time T of one abnormal event by the control room personnel [30]

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_k and its weight w_k, with constant C for the model calibration

$$HEP = HEP_{no\min al} \sum_k w_k PSF_k + C \tag{3}$$

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

$$HEP = \frac{NHEP \cdot PSF_{composite}}{NHEP(PSF_{composite} - 1) + 1} \tag{4}$$

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

$$\lg HEP_j = c \cdot SI_j + d \tag{5}$$

$$SI_j = \sum_i w_i r_{ij} \tag{6}$$

where: w_i - normalised weight coefficient assigned to *i*-th influence factor ($\sum_i w_i = 1$), r_{ij} - scaled rating of *i*-th factor in *j*-th task (normalised scaling value is $0 \le r_{ij} \le 1$). 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 particular task of interest in probabilistic modeling.

2.4. Human factors in functional safety analysis

Lately, a framework [2] was proposed for addressing human factors in IEC 61508. Consideration is given to a range of applications of 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. Following conclusions were drawn:

- determination of the safety integrity level (SIL) for E/E/PES requires careful consideration of not only the direct risk reduction functions it is providing, but also those risk reduction functions performed by personnel that interact with it; this requires addressing in the hazard and risk analysis some steps of the IEC 61508 lifecycle [16];
- having determined the required safety integrity of the E/E/PE system, it is suggested that the effort that needs to be placed into operations and maintenance in relation to human factors should be greater as the SIL level increases;
- issues of the types of human factors that need to be addressed vary between the classes of systems; therefore, the framework is not specific in terms of the technology or other aspects related to human factors.

A human-operator is involved in performing safety-related functions because:

- he/she is using information from a programmable electronic device within E/E/PES or SIS,
- a human-initiating safety action can be required through a programmable electronic device.

A general framework is proposed for addressing human factors (HFs) within IEC 61508 that include [2]:

- incorporation of human tasks and errors into the hazard and risk assessment process;
- use of the tables to define the human factor requirements for a given safety integrity level.

In the paper [10] publishing Guidance for Users of IEC 61508 was announced, which would be designed to respond to requirements laid down in this standard. They fall into two broad categories:

(1) those associated with hazard and risk analysis,

(2) those concerning the operator interface.

The hazard and risk analysis has to include:

- all relevant human and organizational factors issues,
- procedural actions and human errors,
- abnormal and infrequent modes of operation,
- reasonably foreseeable misuse,
- claims on operational constraints and interventions.

While the operators interface analysis should:

- be covered in safety requirements,
- take account of human capabilities and limitations,
- follow good HF practice,
- be appropriate for the level of training and awareness of potential users,
- be tolerant of mistakes (see classification of

human errors above).

Thus, the scope of analyses should include human and organizational factors with relevant system specific aspects to be traditionally included in HRA methods applied in PSA [4], [8], [9], [14], [17], [29], [30].

It is worth to mention that in the international standard BS EN ISO 13407 (*Human-centered design processes for interactive systems*) the key principles are outlined applied in Usability Engineering [2]. More important characteristics of the human-centered design process are as follows:

- the active involvement of users and a clear understanding of the user and task requirements,
- an appropriate allocation of functions between users and technology,
- the iteration of design solutions,
- multi-disciplinary design.

More important activities described in this standard and their interrelations are shown in *Figure 7*.

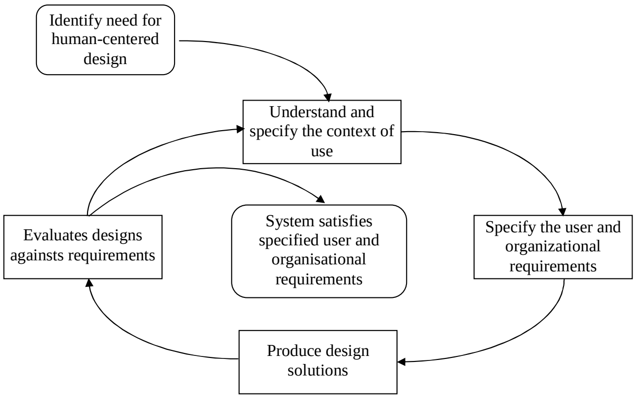

Identify need for human-centered design
Understand and specify the context of use
Evaluates designs againsts requirements
System satisfies specified user and organisational requirements
Specify the user and organizational requirements
Produce design solutions

Figure 7. Human-centered design process according to BS EN ISO 13407

Generally, the requirements concerning the analysis of human factors in functional safety solutions increase in proportion to the integrity level of E/E/PES. Several system categories can be distinguished [2]:

(1) protection system,
(2) supervisory control system,
(3) remote control system,
(4) display and/or communications system, and
(5) offline analysis or support tools.

In this paper only categories 1, 2 and partly 5 are discussed.

As it was mentioned the requirements concerning the human factors increase for higher SIL of safety-related system. For instance for SIL 2 following requirements are suggested:

- 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 for subsystems A, B and C (assuming small values of probabilities) from the formula

$$PFD^{\mathrm{S}}_{\mathrm{avg}} \cong PFD^{\mathrm{A}}_{\mathrm{avg}} + PFD^{\mathrm{B}}_{\mathrm{avg}} + PFD^{\mathrm{C}}_{\mathrm{avg}} \qquad (7)$$

where $PFD^{\mathrm{A}}_{\mathrm{avg}}, PFD^{\mathrm{B}}_{\mathrm{avg}}, PFD^{\mathrm{C}}_{\mathrm{avg}}$ are probabilities of failure on demand for subsystems A, B and C (see *Figure 1*).

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 and/or C) from formula:

$$PFD^{SUB}_{avg} \cong PFD^{FT}_{avg} + PFD^{AT}_{avg} + HEP \qquad (8)$$

where: PFD^{FT}_{avg} is average probability of subsystem failure on demand, detected in periodical functional test (FT); PFD^{AT}_{avg} – the probability of subsystem failure on demand, detected in automatic tests (AT); HEP – the human error probability.

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

For instance, the probability of failure on demand for

1oo2 subsystem including modelling of common cause failures and human error probability (HEP) can be calculated from formula

$$PFD_{avg1oo2} \cong [(1-\beta)\lambda_D]^2 (\frac{T_I^2}{3} + T_I MTTR + MTTR^2) + \beta\lambda_{DU} (\frac{T_I}{2} + MTTR) + HEP \tag{9}$$

where *β*-factor for dependent failures of two channels, λ_D – a dangerous failure rate of one channel; λ_{DU} – a dangerous undetected failure rate, T_I - 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). Designing the safety-related system is based on the risk analysis and assessment to determine their required safety-integrity level (SIL), which should be then verified in the probabilistic modeling. It is important to include in probabilistic model potential dependencies between events representing equipment failures or human errors.

Figure 8 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].

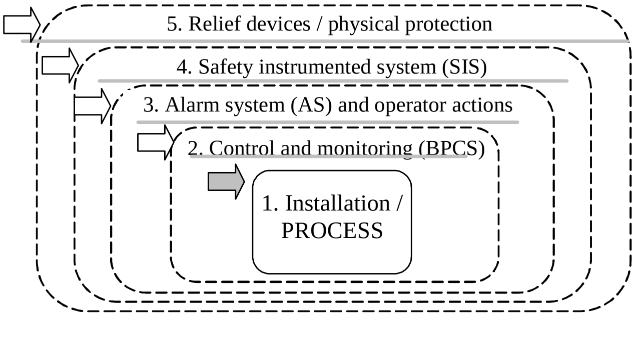

5. Relief devices / physical protection
4. Safety instrumented system (SIS)
3. Alarm system (AS) and operator actions
2. Control and monitoring (BPCS)
1. Installation / PROCESS

Figure 8. Typical protection layers in hazardous industrial installation

An active protection layer generally comprises:

- a sensor of some type (instrument, mechanical, or human),
- a decision-making device (logic solver, relay, spring, human, etc.),
- an action (automatic, mechanical or human).

The protection layers in *Figure 8* include: *basic process control system* (BPCS), alarm system (AS) / *human-operator* interventions and *safety instrumented system* (SIS) as layers: 2, 3 and 4 respectively. These systems should be functionally and physically independent; however, it is not always achievable in practice.

The protection layers shown in *Figure 9* include:

- PL1 – *basic process control system* (BPCS),
- PL2 – *human-operator* (OPERATOR), who supervises the process and intervene in cases of abnormal situations and during emergencies that are indicated by the alarm system,
- PL3 – *safety instrumented system* (SIS), which can perform a function of *emergency shutdown* (ESD).

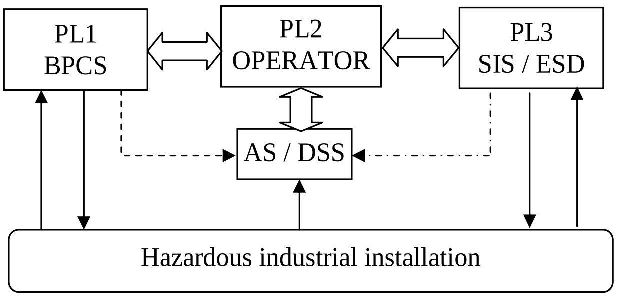


Figure 9. OPERATOR and alarm system (AS) as elements of protection layers

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 using appropriate architectures of their subsystems (see *Figure 1*) taking into account the probabilistic criteria given in *Table 1*, e.g. 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) and 10^{-2} (SIL2), which are values achievable in industrial practice.

There is, however, a considerable problem concerning the layer PL2, i.e. OPERATOR who obtains information through relevant HMI from the alarm system (AS) and/or decision support system (DSS). The independency of this layer, e.g. from BPCS or SIS, can be improved thanks to appropriate designing the alarm system and relevant shaping of performance factors (PSFs) influencing the human-operator reliability.

Only in case of independence of these layers the frequency of *i*-th accident scenario F_i can be calculated form the formula (see formulas in [23])

$$F_i = F_i^I \cdot PFD_{i;PL1} \cdot PFD_{i;PL2} \cdot PFD_{i;PL3} = F_i^I \cdot PFD_i \quad (10)$$

where F_i^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 8*. In case of the second layer $PFD_{i;PL2} = HEP_{i;PL2}$, relevant HEP (*human error probability*) is evaluated using appropriate HRA method.

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

$$F_i^Z = F_i^I \cdot P(X_{i;PL1} \mid I) \cdot P(X_{i;PL2} \mid I \cdot X_{i;PL1}) \cdot P(X_{i;PL3} \mid I \cdot X_{i;PL1} X_{i;PL2}) = F_i^I \cdot PFD_i^Z \quad (11)$$

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

4. Requirements and criteria concerning the alarm system and operator interface

In international standards [15] and [16] there is not clear guidance how to include the human and organizational factors in functional safety analysis. They should be, however, included in designing the human - machine interface (HMI) as a part of the alarm system (AS) and decision support system (DSS). Some suggestions are given in a report [2], guide [5] and 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 the threshold value or discrete state of a process variable that triggers the alarm. The alarm flood (or 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 reliability required of each 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 required.

After making a decision during abnormal situation the operator must execute required 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 a sequence in *Figure 3*) during 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 defined functions to mitigate consequences.

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

(1) whether the AS should be classified as safety related according to the definitions given in the international functional safety standard [15],

(2) whether it should be implemented in 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 an industrial sector. Alarms which are safety-related according to definition in the standard [15] should be given special consideration in terms of designing HMI and operator DSS. If any alarm system is safety-related then 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 only a starting point in the design process of DSS including alarms. The risk reduction achieved by an alarm system will depend on:

- the reliability of the 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 group 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 every alarm system:

- the operator should not be overloaded with alarms presented by the chosen display arrangement, either in normal operation or upsets,
- AS performance should be regularly checked to ensure that alarm overload is not occurring,
- alarms presented by the chosen display arrangement should be operationally useful with few spurious annunciations,
- alarms should be properly prioritized,
- the operator should be trained in using the AS.

Figure 10 presents an example of a qualitative approach for deciding about a basic solution of the alarm system which could be implemented within the basic process control system or to use stand-alone safety-related AS.

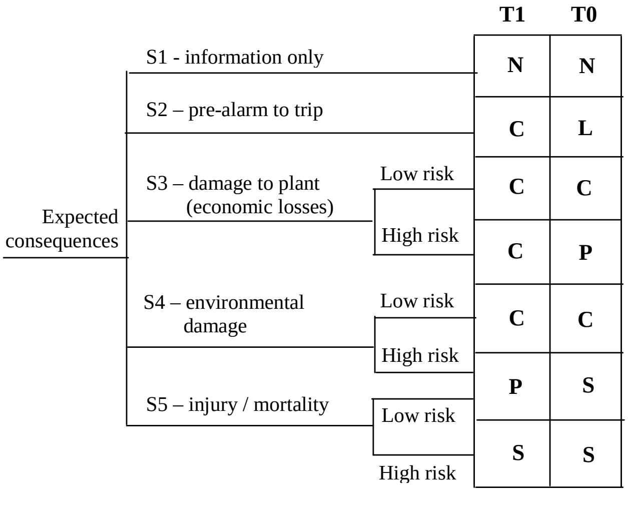


Figure 10. The risk related parameters and their influence on the alarm system design assumptions (adapted from [5])

Depending on the parameters of risk and expected diagnosis difficulties of hazardous installation in a short time TO or T1 (TO – quick response essential ≤ 3 min.; T1 – slow response adequate > 3 min.) an alarm system solution is selected from appropriate column: N – not suitable as alarm, L – limited benefit, C – alarm within basic control system recommended, P – alarm either in stand-alone or control system acceptable, S – alarm within stand-alone system recommended.

It is worth to mention that the threshold value of 3 minutes assumed in defining T0 and T1 is related to difficulties to diagnose abnormal situation in a dynamic system in short time and relatively high probability to commit an error (see *Figure 6*). The risk assessment process may include hazard and operability studies (HAZOPs).

For the safety-related alarm more stringent reliability requirements should be imposed on both equipment and human performance summarized in *Table 2*.

Table 2. Reliability requirements concerning human operator and equipment of safety-related alarm system (adapted from [5])

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

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 a 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 very likely to lead to the operator abandoning use of the system,
- between 20 and 100 – it is hard to cope with,
- under 20 – should be manageable, but may be difficult if several of the alarms require a complex operator response.

From *Figure 10* and *Table 2* some basic assumptions for designing the AS might be derived. In case of hazardous installations of high risk and a quick response required the AS is safety-related and should be stand-alone. Designing of such system according to functional safety principles is described in international standard IEC 61508 [15]. Some suggestions for 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 9*). The AS, if carefully designed with good HMI and DSS functions, will certainly contribute to reduction of human error probability [5], [8], [22].

As it was mentioned in assessment of 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 active failures and in cases of multiple failures. Such challenging problems require further research that would be valuable to develop intelligent alarming.

Another issue that require further research is developing or assessing advisory software for supporting safety-related decision making, which will comply with international standard IEC 61508 [7]. The basic principle concerning the safety-related functions of advisory software can be generally stated as follows: this software must not mislead the user into a dangerous decision.

5. Conclusion

In the paper an integrated approach is outlined that includes selected aspects of the functional safety analysis in hazardous installations including the protection layer analysis. In particular the role of alarm system is emphasized, which requires appropriate designing with regard to careful treating of human and organizational factors.

Nowadays issues concerning the functional safety management in industrial complex hazardous plants with regard to the human and organizational factors becomes very 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 separate from the basic process control system.

It is required to manage the functional safety in entire safety lifecycle keeping the risks 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 systems including the alarm system and decision support system.

The safety management is to be carried out in the life cycle based on 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 industrial hazardous plants.

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 solutions to be implemented by means of the basic process control system, the alarm and decision support system and the safety instrumented systems. Their 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 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) 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

[1] Byers, J. C., Gertman, D. I., Hill, S. G., Blackman H. S., Gentillon, C. D., Hallbert, B. P. & Haney, L. N. (2000). Simplified Plant Analysis Risk (SPAR) Human Reliability Analysis (HRA) methodology: comparison with other HRA

methods. International Ergonomics Association and Human Factors & Ergonomics Society Annual Meeting (July 31– August 4).

[2] Carey, M. (2001). *Proposed Framework for Addressing Human Factors in IEC 61508*. Prepared by Amey VECTRA Ltd. for Health and Safety Executive (HSE), U.K. Contract Research Report 373.

[3] COA (1998). Critical Operator Actions – Human Reliability Modeling and Data Issues. Nuclear Safety, NEA/CSNI/R(98)1. OECD Nuclear Energy Agency.

[4] Dougherty, E.M. & Fragola, J.R. (1988). *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*. A Wiley-Interscience Publication, New York: John Wiley & Sons Inc.

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

[6] Embrey, D. E. (1992). Incorporating Management and Organisational Factors into Probabilistic Safety Assessment. *Reliability Engineering and System Safety* 38, 199-208.

[7] Froome, P. & Jones, C. (2002). *Developing advisory software to comply with IEC 61508*. Contract Research Report 419. HSE Books.

[8] Gertman, I.D. & Blackman, H.S. (1994). *Human Reliability and Safety Analysis Data Handbook*. New York: A Wiley-Interscience Publication.

[9] HERA (2002). Short Report on Human Performance Models and Taxonomies of Human Error in ATM. European Organisation for the Safety of Air Navigation. Brussels: EATMP Infocentre, Eurocontrol Headquarters.

[10] Hickling, E.M., King, A.G. & Bell, R. (2006). *Human Factors in Electrical, Electronic and Programmable Electronic Safety-Related Systems.* A work supported by Health and Safety Executive (HSE) U.K.

[11] Hollnagel, E. (1987). Information and reasoning in intelligent decision support systems. *Int. J. Man-Machine Studies* 27 ,665-678.

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

[13] Hollnagel, E. (2005). Human reliability assessment in context. *Nuclear Engineering and Technology*, Vol.37, No.2, 159-166.

[14] Humphreys, P. (ed.) (1988). Human Reliability Assessor Guide. RTS 88/95Q, Safety and Reliability Directorate, U.K.

[15] IEC 61508:2000. Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems, Parts 1-7. International Electrotechnical Commission, Geneva.

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

[17] Kosmowski, K.T., Degen, G., Mertens, J. & Reer, B. (1994). *Development of Advanced Methods and Related Software for Human Reliability Evaluation within Probabilistic Safety Analyses*. Jülich: Berichte des Forschunszentrum 2928.

[18] Kosmowski, K. T. (1995). Issues of the human reliability analysis in the context of probabilistic studies. *International Journal of Occupational Safety and Ergonomics*, Vol. 1:3, 276-293.

[19] Kosmowski, K.T., Kwiesielewicz, M. (2002). Hierarchical influence diagrams for incorporating human and organisational factors in risk assessment of hazardous industrial systems. *Risk Decision and Policy* Vol. 7, 25-34.

[20] Kosmowski, K.T. (2004). 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), Berlin: Springer, 2048-2053.

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

[22] Kosmowski, K.T. (2007). *Functional Safety Management in Critical Systems*. Gdansk University of Technology. Wydawnictwo: Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdansk.

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

[24] 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.

[25] Rasmussen, J. & Goodstein, L.P. (1985). *Decision support in supervisory control*. IFAC man-Machine Systems. Varsese, Italy.

[26] Rasmussen, J. & Svedung, I. (2000). *Proactive Risk Management in a Dynamic Society.* Swedish Rescue Services Agency, Karlstad.

[27] Reason, J. (1990). *Human Error*. Cambridge University Press.

[28] Richei, A., Koch, M.K. & Unger, H. (1999). Application of the procedure HEROS fort he evaluation and optimization of a man-machine-system within the PSA for NPP. Safety and Reliability, Schuëller & Kafka (eds), Balkema,

Rotterdam.

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

[30] Swain, A.D. & Guttmann, H.E. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application.* NUREG/CR-1278.