Kosmowski Kazimierz T.
Gdańsk University of Technology, Gdańsk, Poland

Designing issues of the alarm system in context of functional safety and human factors

Keywords

hazardous plants, protection layers, functional safety, alarm system, human factors

Abstract

This article addresses selected aspects of the alarm system and human factors that should be evaluated during the design and operation of an industrial hazardous installation. In such installations the layer of protection analysis (LOPA) methodology is often applied for simplified risk analysis based on defined accident scenarios. To reduce and control the risks the safety instrumented functions (SIFs) are identified and their safety integrity levels (SILs) determined taking into account defined criteria the risk evaluation results. Given SIF is implemented using the basic process control system (BPCS), the alarm system (AS) and the safety instrumented system (SIS). Nevertheless a crucial role plays the human-operator undertaking safety-related decisions during potential abnormal situations and accidents. Below some issues concerning requirements for the alarm system design in context of human factors are outlined and discussed.

1. Introduction

Many research works concerning causes of industrial accidents indicate that broadly understood human failures, resulting often from organisational neglects, are determining factors in 70-90% of cases [21], [26], depending on industrial sector and plant category. Because several defences against potential accidents are usually used in hazardous plants to protect people and environment, it is obvious that multiple faults have contributed to major industrial accidents.

It has been emphasized that such accidents arose from a combination of latent and active human errors committed during the design, operation and maintenance [18], [26], [27]. 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 and internal disturbances or active human errors, can contribute to major accident. Some categorizations of human actions and related errors have been proposed, e.g. by Swain & Guttmann [29], Rasmussen [24], and Reason [27].

Traditionally, potential human and organisational deteriorating influences in industrial plant are to be incorporated into the probabilistic models as failure events with relevant probabilities evaluated using selected method of human reliability analysis (HRA) [8], [22]-[23], [28]-[29]. Careful analysis of expected human behaviour (including context oriented diagnosis, decision making and actions) and potential errors is prerequisite of correct risk assessment and rational safety-related decision making.

The probabilities of failure events depend significantly on various human and organisational factors, categorised usually as a set of performance shaping factors (PSFs) relevant to the situation or scenario under consideration [8], [28]. The PFSs are divided into internal, stressor and external ones and are evaluated applying various methods [29].

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, faults as well as the diagnostic activities, the functionality and safety integrity tests, planned maintenance actions and repairs after faults [19], [21]-[22].

A human operator can be a part of a safety-related function, therefore *human factors* (HFs) should be properly included in the *functional safety analysis* [19], [20]. It includes the *human reliability analysis* (HRA) [8] taking into account the results of *task analysis* (TA) [17]. When in hazardous plant the

layers of protections have to be applied due to a high risk, then the *layer of protection analysis* (LOPA) method is of interest [23].

Nowadays the operators supervise the process and make decisions using the *decision support system* (DSS) [13], [21], [22] and the *alarm system* (AS) [1], [4], [6]. They 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 (E/E/PE) systems [14] or the safety instrumented systems (SIS) [15].

The DSS and AS when are properly designed will contribute to decreasing the human error probability in various plant states and reducing the risk of potential accidents with serious consequences [9]. Thus, in hazardous plants the *alarm system* (AS) should be carefully designed within relevant *human-system interface* (HSI) [16].

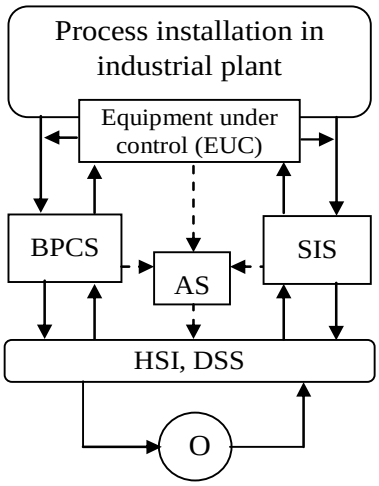
An important issue is to design safety-related *decision support system* (DSS) and advisory software [8], [10], [25]. Theoretical aspects of human factors are nowadays of interest of such research domains as: *cognitive human factors engineering* (CHFE), *cognitive tasks analysis* (CTA), and *cognitive human reliability analysis* (CHRA) [11], [12].

To reduce and control the risks the *safety instrumented functions* (SIF) are identified and their *safety integrity levels* (SIL) determined taking into account the risk assessment results [14], [15]. Given SIF is to be implemented using the *basic process control system* (BPCS), the *alarm system* (AS) and the *safety instrumented system* (SIS). Nevertheless a crucial role plays the human-operator undertaking safety-related decision in abnormal situations and potential accidents. Below some selected issues concerning the design requirements and evaluation of the alarm system (AS) in context of human factors are outlined and discussed.

2. Designing protection layers in industrial hazardous installation

Typical system for implementing the protection layers in hazardous installation is shown in *Figure 1*. The *equipment under control* EUC [14] is to be controlled by the basic process control system and the safety instrumented system. These systems and entire process installation is supervised by human operators (O) through relevant *human-system interface* (HSI).

The operators undertake operational or safety-related decisions based on indications of computerized HSI and information from a *decision support system* (DSS). In cases of abnormalities and accidents an important role play the *alarm system* (AS) that should be designed to avoid alarm flood and to support effectively operators in time of stressful situations [1], [4], [6].



BPCS – *basic process control system*, AS - alarm system, SIS – *safety instrumented system*, HSI – *human-system interface*, DSS – *decision support system*, O – *human operators*

Figure 1. Typical system for implementing protection layers in the process installation

The identification of accident scenarios is one of most important part of the LOPA analysis, which can be performed using the event tree (ET) method as shown in *Figure 2*. In the LOPA method each barrier has certain contribution in reducing risk to defined tolerable level. For consecutive layers the risk reduction is made applying the safety functions that are implemented using the BPCS, AS and human-operator interventions (in reaction to signals representing the installation state), and the SIS.

The failure probabilities on demand (PFD_i) of these consecutive layers can be characterised as follows: (1) PFD_1 of the BPCS if it is safety-related, but only of SIL1 due to its complexity, (2) the *human error probability* $HEP = PFD_2$ depending on the *alarm system* (AS) properties, and PFD_3 for SIS (safety-related of SIL1 or higher) performing *emergency shutdown* (ESD) function.

In the *Figure* 2 it was assumed that these layers are independent and therefore there is simple multiplication of PFD_i in consecutive formulas placed after consecutive layers. However, in real systems these layers are more or less dependent and therefore modified formulas have to applied [20]-[21]. Thus, the human operator interventions should be effectively supported by the alarm system (AS) and the computerised decision support system (DSS) if available, but these actions will be successful if the process dynamic is not too fast and the time window required for his reaction is not too short (below 3 or 5 minutes depending on hazardous situation) [4].

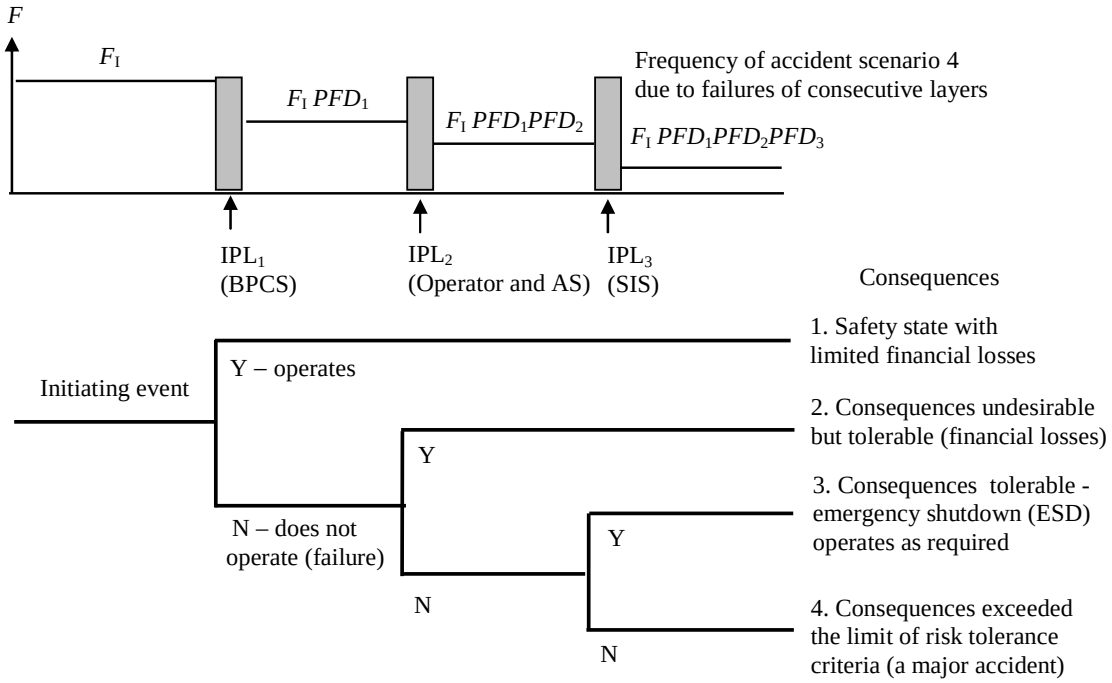


Figure 2. Event tree for defining the accident scenarios in layer of protection analysis

It should be emphasised that spurious operation of the AS or not selective alarming of abnormal situations combined with flood of alarms, can contribute to increase significantly the HEP, and therefore higher frequency of hazardous events.

The AS design is currently one of the most important issue requiring additional research effort to support the human operators of hazardous installations and it can be treated in the context functional safety [2], [4]. For the safety-related alarm more stringent reliability requirements should be imposed on both equipment and human performance as summarised in *Table 1*.

As it can be seen in *Table 1* the functional safety related requirements for designing the alarm system (AS) are strict when AS is treated as safety-related, i.e. for SIL1. More challenging is to design AS for SIL2 or higher, also in the context of preparing written procedures to support operators in responding correctly to various alarms.

In terms of the *safe failure fraction* S_{FF} of a subsystem or channel, treated as the serial reliability configuration of elements, this fraction is to be evaluated from the following formula [14]:

$$S_{FF} = \frac{\sum \lambda_S + \sum \lambda_{Dd}}{\sum \lambda_S + \sum \lambda_{Dd} + \sum \lambda_{Du}} \quad (1)$$

where: λ_S is the rate of safe failures of all elements in such configuration, λ_{Dd} is the rate of dangerous failures that are detected by the diagnostic tests, and λ_{Du} the rate of dangerous undetected failures.

Table 1. Reliability requirements concerning alarms

Claimed PFD_{avg}	AS integrity / reliability requirements	Human reliability requirements
$\geq 10^{-1}$	Standard AS, may be integrated into BPCS.	No special requirements, however the AS should be operated and maintained according to *good engineering practice* characterized in [4].
$[10^{-2}, 10^{-1})$	The AS is to be designated as safety-related of SIL1; it should be independent from BPCS (unless BPCS is also designed as safety-related).	The alarm presentation arrangement should make the claimed alarm obvious to the operator of the highest priority in the system. The operator should be trained for specific plant failures that the alarm system indicate. The operator should have clear written procedure to support responding correctly to alarms. The required operator response should be simple, obvious and invariant. The claimed operator performance should be audited.
$< 10^{-2}$	The AS designated as safety-related, at least SIL2.	It is not recommended that claims for $PFD_{avg} = HEP$ below 10^{-2} are made for any operator action even if it is multiple alarmed and task is simple.

The standard IEC 61508 introduces two types of elements: A and B in the E/E/PE safety-related systems. An element can be regarded as type A if, for

the components required to achieve the safety function, can be characterized as follows [14]:

a) the failure modes of all constituent components are well defined; and
b) the behaviour of the element under fault conditions can be completely determined; and
c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met.

An element shall be regarded as type B if, for the components required to achieve the safety function, can be characterized as follows:

a) the failure mode of at least one constituent component is not well defined; or
b) the behaviour of the element under fault conditions cannot be completely determined; or
c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures.

If at least one of the components satisfies the conditions for a type B element then that element must be regarded as type B rather than type A.

The *hardware fault tolerance* (HFT) requirements apply to the subsystem architecture that is used under normal operating conditions. The HFT requirements may be relaxed while the E/E/PE safety-related system can be repaired on-line. However, the key parameters relating to any such relaxation should be previously evaluated, taking into account the *mean time to restoration* (*MTTR)*, to demonstrate that the system unavailability due to a channel failure and restoration is low compared to the probability of failure on demand [14].

If all the elements have achieved safe failure fractions S_{FF} that are in the same range specified in *Table 2* the following procedure is to be followed:

a) determine the safe failure fraction S_{FF} of an element/channel;
b) determine the hardware fault tolerance of the subsystem;
c) determine the maximum SIL that can be claimed for the subsystem if the elements are of type A from *Table 2*;
d) determine the maximum safety integrity level that can be claimed for the subsystem if the elements are of Type B from *Table 2* (in parentheses).

Taking into account rules concerning architectural constrains [14] (see *Table 2*) for system that consists of subsystems of type B (complex programmable) to achieve SIL2 for the AS without redundancy, the value of S_{FF} should be higher than 90% (99% for AS of SIL3). These are strict design assumptions for the AS implementing more complex diagnostics methods, especially when are taking into account the requirements for testing, verifying and validating of software according to part 3 of IEC 61508 [14] depending on the level of SIL assigned.

Table 2. Maximum allowable safety integrity level for a subsystem carried out safety function using elements of type A (type B)

Safe failure fraction S_{FF}	Hardware fault tolerance *M*		
	0	1	2
<60%	SIL1 (- - -)	SIL2 (SIL1)	SIL3 (SIL2)
[60%, 90%)	SIL2 (SIL1)	SIL3 (SIL2)	SIL4 (SIL3)
[90%, 99%)	SIL3 (SIL2)	SIL4 (SIL3)	SIL4 (SIL4)
≥99%	SIL3 (SIL3)	SIL4 (SIL4)	SIL4 (SIL4)
A hardware fault tolerance of *M* means that *M* + 1 faults could cause a loss of the safety function.			

3. Basic requirements concerning human factors in designing human-system interaction

An interesting framework was proposed for addressing human factors in functional safety analysis [2]. 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 of 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 [14];
- 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 outlined 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 factors requirements for a given safety integrity level.

In the standard IEC 61508 there is not sufficient guidelines to deal systematically with the human and organizational factors. Two broad categories of issues have been distinguished, namely:
(1) those associated with hazard and risk analysis,
(2) those concerning the operator interface.
The hazard and risk analysis should 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 operator interface analysis should be characterized as follows:

- 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 [21], [27].

Thus, the scope of analyses should include human and organizational factors with relevant system specific aspects to be traditionally included in the HRA methods applied in probabilistic safety analysis (PSA) [8], [22], [28], [29].
In the international standard EN ISO 9241-2010 [5] the key principles are outlined and more important characteristics of the human-centered design process are given as follows:

- the active involvement of users and a clear understanding of 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* 3.
Human-centred design teams do not have to be large, but the team should be sufficiently diverse to collaborate over design and implementation trade-off decisions at appropriate times. The following skill areas and viewpoints could be needed in the design and development team [5]:

a) human factors and ergonomics, usability, accessibility, human-computer interaction, user research;
b) users and other stakeholder groups (or those that can represent their perspectives);
c) application domain expertise, subject matter expertise;
d) marketing, branding, sales, technical support and maintenance, health and safety;
e) user interface, visual and product design;
f) technical writing, training, user support;
g) user management, service management and corporate governance;
h) business analysis, systems analysis;
i) systems engineering, hardware and software engineering, programming, manufacturing and maintenance;
j) human resources, sustainability and other stakeholders.

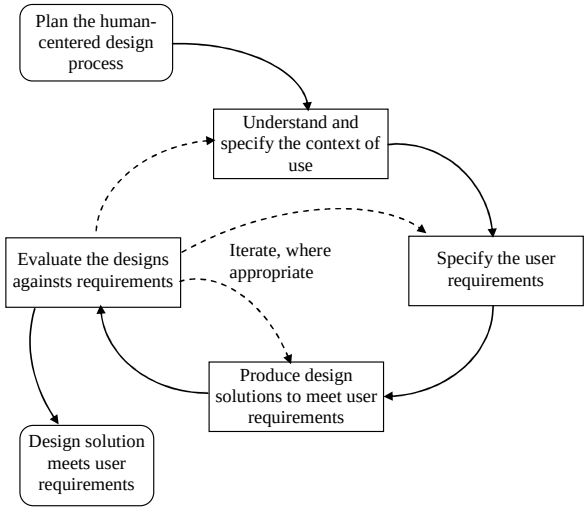


Figure 3. Interdependence of human-centred design activities [5]

Projects benefit from additional creativity and ideas from the interaction and collaboration of team members who, collectively, have an extensive skill base. An additional benefit of a multidisciplinary and multi-perspective approach is that team members become more aware of the constraints and realities of the other disciplines. For example, technical experts can become more sensitized to user issues and users can become more aware of technical constraints.
Thus, the issue is to make the design solutions more concrete and transparent. It can be done by developing scenarios, simulations, models and mock-ups or other forms of prototype that enables designers to communicate the proposed design to users and other stakeholders to obtain feedback. The benefits include [5]:

a) making design proposals more explicit (this enables members of the design team to communicate with each other and with users early in the development process);
b) allowing designers to explore several design concepts before they settle on one;
c) making it possible to incorporate user feedback

into the design early in the development process;
d) making it possible to evaluate several iterations of a design and alternative designs;
e) improving the quality and completeness of the functional design specification.

Simple prototypes are valuable at early stage to explore alternative design solutions. While there can be substantial benefit in making the design solutions as realistic as possible, the level of detail and realism should be appropriate to the issues that need to be investigated. Investing too much time or money in producing a detailed working prototype can lead to a reluctance to change the design.

The requirements concerning the human factors in designing the functional safety increase in proportion to the integrity of E/E/PE system. 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 tool.

In this article mainly categories 2 and 4 are of interest. As it was mentioned the requirements concerning human factors increase for higher SIL of safety-related system. For instance for the level of SIL2 following requirements are suggested [2], [19]:

- 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.

4. Basic alarm system design issues with emphasis on human factors

The operator's main task in modern control systems in chemical production plants is that of monitoring a largely automated process. Operator action is required only when the status of either the process or the equipment necessitates adjustment, compensatory action or fault rectification. The design of the human-process interface must, therefore, be resolutely dictated by operator needs, and it must take into account human limitations.

There are remarks concerning operator capability to response depending on alarming rate following an upset condition of the installation, expressed as a number of alarms displayed in 10 minutes following a major plant upset [4]:

- 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;
- less than 20 – might be manageable, but with difficulties if several of alarms require more complex operator response.

Several categories of alarms are to be distinguished:

- *Absolute alarm* - alarm when a set limit is exceeded or undershot, high / high-high / low / low-low;
- *Deviation alarm* - alarm triggered by a deviation from standard that exceeds a set tolerance;
- *Adaptive alarm* - automatic adaptation of limit values e.g. boiler temperature depending on steam pressure in heating elements.

Generally, an *alarm* is understood as indication requiring immediate response by the operator. The response may be, for example, manual intervention, increased watchfulness or initiation of further investigation. Alarm management system supports the operator in avoiding and controlling abnormal conditions.

The objective to assign an *alarm priority* is to *c*lassify the alarms according to their importance (e.g. seriousness of consequences) and urgency. The a*larm rate is a n*umber of alarms that occur per unit of time, e.g. 10 minutes or a half hour. *Alarm suppression* is temporary suppression of alarm functions.

PCS (process control system) alarm is a message from the PCS requiring an immediate response from the operator e.g. to initiate maintenance. The *alarm system* is an entire system designed for the management of messages and alarms in the PCS. Allowable *response time* means the time available to the operator to take preventive action against the undesired state of the process.

Alarms signal process and/or plant deviations from normal set status requiring immediate response by the operator to prevent [6]:

- *Hazardous situations* (early warning system to avoid emergency trips)
- *Economic losses* (product quality and quantity).

A message differs from an alarm in that it signals the occurrence of an event that does not require immediate action by the operator.

According to EEUMA [4], an alarm should have the following characteristics, it should be:

- *relevant* - i.e. justified and not insignificant in the operator's priorities,
- *unique* - i.e. not merely a repetition of information from another alarm,

- *timely* - it comes up neither long before intervention is necessary nor too late for action to be taken,
- *prioritized* - it indicates the urgency of the problem requiring operator action,
- *understandable* - it contains a clear message that is easily understood,
- *diagnostic* - it helps with the identification of the problem,
- *advisory* - it helps to find the correct action,
- *focusing* - it directs attention to the important.

Alarms and message signals are generated in close association with the process in a process control instrument (e.g. sensor, actuator, PCS) with a synchronous time stamp. Signal generation can be linked with certain conditions, e.g. hysteresis.

The following distinct alarm types are given by analogy with EEMUA [4]:

- Absolute alarms,
- Deviation alarms,
- Rate of change alarms,
- Deviation status alarm,
- Delayed alarms i.e. the alarm is not generated until the alarm criterion has been met over a predetermined period of time.
- Recipe-dependent alarms,
- Bit pattern alarms,
- Process control system alarms,
- Flexible alarms,
- Operator-set alarms,
- Adaptive alarms,
- Alarms capable of reactivation.

Requirements concerning the plant designers, constructors, operators and operating companies include using of alarm type most suited to the purpose with involvement of the interdisciplinary team that defines the alarms (supervision of what?, what kind of response is possible, and set the limit values).

From the process control system characteristics point of view the system requirements include such aspects as: *time windows* for alarms capable of reactivation, hysteresis, triggering of alarm suppression by a lead alarm/master alarm in order to avoid cascade alarms, clock synchronization, configurable alarm generation functions such as process and/or plant status dependent inhibition, e.g. for startup, shutdown, offline.

Alarm processing supports the operator in the efficient exercise of duties. Its purpose is to reduce the burden on the operator by compressing information and giving interpretation support. In addition, it provides support tools for activating or deactivating alarms depending on a combination of plant status and active alarms (dynamic alarm processing).

The *prioritization of alarms* suggests to the operator a sequence in which to process the alarms if several accumulate at the same time. It must take account both of the potential effects of not responding and of the available response times. *Alarm priorities* should be colour-coded.

Alarms are indicated to the operator by a visual or audible signal (e.g. audible or visible indicators or loudspeaker). With the acknowledgment of an alarm or a message signal, the operator documents knowledge of the change of status.

The operator must be given the support he/she needs to obtain a total view of the process and plant status, enabling correct decision making on the response to any alarm. The operator must be adequately supported in selecting the relevant graphic screen and responding appropriately to one or more alarms as the situation requires.

It is necessary to assess the *operator workload.* Anything that might impair the operator's ability to act (e.g. too many alarms rushing in at once) is to be avoided in order to assure sufficient scope for operating and monitoring. The alarm rate per operator workplace is suggested in EEMUA [4]. For instance, the long-term average alarm rate in normal operations should not exceed one alarm every ten minutes.

The system management should provide tools for optimizing, updating and managing the *alarm management system*.

5. Human reliability analysis in context of protection layers including alarm system

The *human reliability analysis* (HRA) methods are used for assessing the contribution to risks the events resulting from potential *human errors*. The general aim is to reduce the system vulnerability operating in given environment. However, some basic assumptions made in HRA methods used within probabilistic safety analysis of hazardous systems are still the subjects 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 [11] that some HRA results are of limited value as an input for *probabilistic safety analysis* (PSA), 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).

In performing HRA a knowledge concerning some concepts of human behaviour types and error types is necessary. Rasmussen [24]-[25] proposed the distinction of three categories of human behaviour (see *Figure* 4).

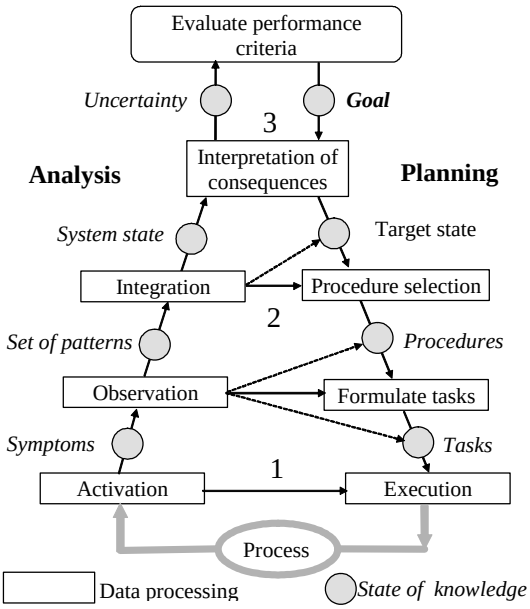


Figure 4. Schematic representation of information processing scope by operators and human behaviour types (1 - *skill*, 2 - *rules*, 3 – *knowledge*)

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).

This concept is useful in analysis of human behaviour and potential errors. However, the HRA practitioners know that the distinction between a skill-based action and a rule-based action and potential errors is not always trivial and require the context oriented analysis by experienced expert. Similar difficulty is also associated with the distinction between a rule-based and knowledge-based behaviour and related potential errors.

It is worth to mention that Hollnagel in his methodology named CREAM (*Cognitive Reliability and Error Analysis Method*) proposes different quantification of operator control modes and relevant interval assessment of *HEP* [11]:

a) strategic [0.00005, 0.01];
b) tactical [0.001, 0.1];
c) opportunistic [0.01, 0.5];
d) scrambled [0.1, 1].

The HRA methodologies are still not fully mature and most of them is categorised as I generation HRA methods. The CREAM methodology, although with some aspirations to a II generation HRA method, requires still improvements and simplification to be of wider interest in HRA practice. Therefore below two other methods will be described, named SI-FOM and SPAR-H for *HEP* evaluations with regard to a set of *performance shaping factors* (PSFs) evaluated with support by analyses of cognitive behaviour of operators in defined accident scenario. These methods will be described further.

An appreciated method for performing HRA for a set of PSFs, from the point of view of scientific formalism, is SLIM [8]. The SLIM method is oriented on success probabilities of events to accomplish specified tasks. However, the probabilistic modelling for the risk assessment is rather failure oriented and it is more justified to apply a modification of SLIM method named SI-FOM (*Success Index-Failure Oriented Method*) [18]. The equations for the human failure probabilities HEP_j and the success indices SI_j for j^{th} task are as follows:

$$\lg HEP_j = c \cdot SI_j + d \tag{2}$$

$$SI_j = \sum_i w_i r_{ij} \tag{3}$$

where: w_i is normalised weight coefficient assigned to i^{th} influence factor $\left(\sum_i w_i = 1\right)$; r_{ij} - scaled rating of i^{th} influence factor in j^{th} task (normalised scaling values are from the interval $0 \le r_{ij} \le 1$).

If for a category of human actions being considered the minimum and maximum values of HEP are known (taken from the range: $0 < HEP \le 1$): $[HEP_{\min}, HEP_{\max}]$, e.g. from the experiments on a full scale simulator and/or with using expert opinions, and relevant $SI_{\max}$ and $SI_{\min}$ were evaluated for such extreme situations from equation (3), the coefficients c and d can be calculated from relevant two equations (2).

Knowing the coefficients c and d the value of SI_j for a j-task characterised by a set of values w_i and r_{ij} the value of SI_j is calculated from (3) and the value of interest HEP_j from (2) or from following equivalent equation [18] is evaluated:

$$HEP_j = 10^{cSI_j + d} \tag{4}$$

For instance, if it would be assumed that $HEP_{\min} = 0.01$, $HEP_{\max} = 0.1$, respectively for $SI_{\max} = 1$ and $SI_{\min} = 0$, then from two equations (2) following values of coefficients c and d are obtained: $c = -1$ and $d = -1$. If for a situation 1 considered $SI_1 = 0.5$, then using formula (4) the value of human error probability is equal $HEP_1 \cong 0.03$.

Various approaches are used for evaluating human error probability (*HEP*) with regard to a set of *performance shaping factors* (PSFs). For instance, in the SPAR-H method [28] it is proposed to distinguish two cases of human error probability: for a diagnosis HEP_D and HEP_A for action that follows diagnosis. The following formulas are used for calculation of HEP_{Dj} for diagnosis of j^{th} abnormal situation

$$HEP_{Dj} = NHEP_D \cdot S_{Dj} \tag{5}$$

where: $NHEP_D$ is the nominal HEP for diagnosis, in SPAR-H method suggested to be equal 0.01; S_{Dj} is the composite PSF of j^{th} situation.

These composite PSFs are evaluated from following formulas:

$$S_{Dj} = \prod_i S_{Dij} \tag{6}$$

When three or more values of S_{Dij} are greater than 1 (some of them can reach values up to 50), to keep the probability values of HEP_{Dj} below or equal 1, other formulas have to be used [21]:

$$HEP_{Dj} = \frac{NHEP_D \cdot S_{Dj}}{NHEP_D (S_{Dj} - 1) + 1} \tag{7}$$

In a similar way *HEP*s are evaluated in the HEART method, although in that method the human error includes both diagnosis and action resulting in one failure event with relevant *HEP*.

Thus, the *human error probability* (*HEP*) can be evaluated using one of the HRA methods, e.g. THERP [29] or SPAR-H [28]. In the method SPAR-H eight factors are to be evaluated by HRA analyst: *(1) Available time; (2) Stress/stressors; (3) Complexity; (4) Experience/training; (5) Procedures; (6) Ergonomics/HSI; (7) Fitness for duty, and (8) Work processes.* Factors (1), (5) and (6) have highest influence on the HEP evaluations [28].

The HEP is to be calculated using selected method and then it can be evaluated in context of protection layers (PL) as shown in *Figure* 5:

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

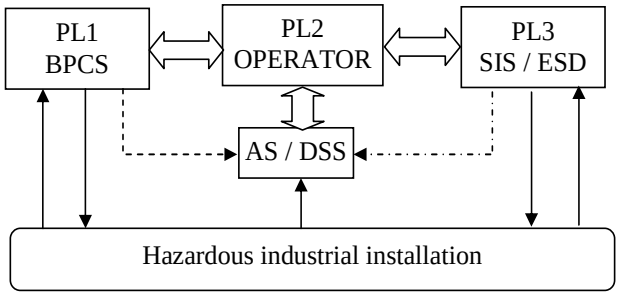


Figure 5. OPERATOR and alarm system (AS) as elements of protection layers

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 taking into account the probabilistic criteria for verifying SIL of SIS.

If the risk reduction can be 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 practicably achievable.

However, there is often a 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) that are not properly designed.

For two cases considered, namely (A) *existing* and (B) *improved*, that differed mainly as regards quality of: *Procedures* and *Ergonomics*/*HSI*, relevant values of human error probability have been obtained using the SPAR-H method: $HEP_A = 0.5$ and $HEP_B = 0.05$.

The analyses undertaken show importance of appropriate design of the alarm system (AS). In many cases the quality, reliability and independency of this layer, e.g. from BPCS or SIS, can be improved thanks to appropriate designing the alarm system and diligent shaping of factors (PSFs) influencing significantly the operator reliability.

It should be noted that significant problems emerge when cognitive aspects of human-operator behaviour and potential errors are considered. For instance in cases of latent failures that can contribute significantly to committing active failures and in

cases of multiple and dependent failures when advanced diagnostic tools are not applied, based on *artificial intelligence* (AI) methods.
Such issues require further research aimed at developing advanced *cognitive human reliability analysis* (CHRA) method in the context of using computers to enhance plant diagnosis and operator response, especially from the perspective of functional safety analysis and management. Interesting methods to be considered in such research include publications [3], [11], [30].

6. Conclusions

Human operator actions can be a part of safety-related function, therefore human factors should be properly included in the functional safety analysis. It includes the human reliability analysis taking into account the results of task analysis. When in hazardous plant the layers of protection have to be applied due to a high risk, then the layer of protection analysis (LOPA) is of interest. In such plant the alarm system (AS) should be properly designed including relevant human-system interface.
An important issue is to design safety-related decision support system (DSS). Theoretical aspects of human factors are nowadays of interest of such research domains as: cognitive human factors engineering, cognitive tasks analysis, and cognitive human reliability analysis.
When the decision support system and alarm system will be properly designed, they would contribute to decreasing the human error probability in various plant states and reducing the risk of potential major accidents with serious consequences.

References

[1] ANSI/ISA-18.2 (2009). Management of Alarm Systems for the Process Industries.
[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] EEMUA (2007). Publication 191: Alarm Systems, A Guide to Design, Management and Procurement (Edition 2). The Engineering Equipment and Materials Users' Association. London.
[5] EN ISO 9241-210 (2010). Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems.
[6] EN 62682 (2015). Management of alarms systems for the process industries.
[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] Guidelines (2008) for Hazard Evaluation Procedures. New York: Center for Chemical Process Safety. Wiley-Interscience, A John Wiley & Sons.
[10] Hollnagel, E. (1987). Information and reasoning in intelligent decision support systems. Int. J. Man-Machine Studies 27, p. 665-678.
[11] Hollnagel, E. (1998). Cognitive Reliability and Error Analysis Method, CREAM. Elsevier Science Ltd, Oxford.
[12] Hollnagel, E. (1999). Cognitive Systems Engineering: New wine in new bottles. Int. J. Human-Computer Studies, 51, p. 339-356.
[13] IAEA (1998).TECDOC-1019. Use of computers to enhance nuclear power plant diagnosis and operator response. International Atomic Energy Agency, Vienna.
[14] IEC 61508 (2010). Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems. Parts 1–7. Geneva: International Electrotechnical Commission.
[15] IEC 61511 (2014). Functional safety: Safety Instrumented Systems for the process industry sector. Parts 1–3. Geneva: International Electrotechnical Commission.
[16] IEC 61513 (2011). Nuclear power plants, Instrumentation and control for systems important to safety, General requirements for systems. International Electrotechnical Commission, Geneva.
[17] Kirwan, B. (1994). A Guide to Practical Human Reliability Assessment. CRC Press, London.
[18] Kosmowski, K.T. (2003). Risk analysis methodology for reliability and safety management of nuclear power plants (*in Polish*). Monografie 33. Gdańsk University of Technology Publishers.
[19] Kosmowski, K.T. (Ed.) (2007). Functional Safety Management in Critical Systems. Gdansk University of Technology. Publishing House OF Gdansk University (Wydawnictwo Fundacji Rozwoju Uniwersytetu Gdańskiego).
[20] Kosmowski, K.T. (2013). Functional safety and reliability analysis methodology for hazardous industrial plants. Gdańsk University of Technology Publishers.
[21] Kosmowski, K.T. (2013). Problems in designing and operating the functional safety solutions of

higher integrity levels**.** Journal of Polish Safety and Reliability Association, 4, 1, 83-99.

[22] Kosmowski, K.T. (2014). Human factors in designing the instrumentation and control systems important to safety. International Journal of Performability Engineering 10, 7, 741-754.

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

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

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

[30] Woods D. D., Pople H. E. & Roth, E.M. (1990). The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability. NUREG/CR-5213. Westinghouse Science and Technology Center, Pittsburgh.