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

Cognitive engineering and functional safety technology for reducing risks in hazardous plants

Keywords

cognitive science, cognitive systems engineering, human factors, human reliability, functional safety

Abstract

Cognitive engineering is considered nowadays as interesting multidisciplinary domain that focuses on improving the relations between humans and the systems that are supervised and operated. The industrial automation and control systems (IACS) in hazardous plants are increasingly computerized and perform various safety functions. These are designed and implemented according to the functional safety concept. The objective is to maintain high performance / productivity and reduce various risks related to identified hazards and threats. An approach is proposed to apply selected cognitive engineering methods for verifying the design of the functional safety technology implemented in given hazardous plant in context of defined safety functions, operator interfaces, communication means and procedures. The methodology developed might be applied for functional safety management in life cycle of industrial hazardous plants and oil port terminals.

Introduction

The *cognitive engineering* is considered nowadays as interesting multidisciplinary domain that focuses on improving the relations between humans and the systems that are supervised and operated. Lately it proposes some applications, including intelligence analysis as well as command and control [7].

The discipline of cognitive engineering combines knowledge and experience from cognitive science, human factors, human-computer interaction design, and systems engineering. *Cognitive science* is the interdisciplinary study of mind and intelligence, embracing philosophy, psychology, artificial intelligence, neuroscience, linguistics, and anthropology [29].

Cognitive systems engineering (CSE), called often shortly *cognitive engineering*, has been identified as an important activity in the early 1980s [2], [7]. The CSE is rooted in the domains of *human factors* and *ergonomics*.

The *industrial automation and control systems* (IACS) in industrial plants are increasingly computerized and perform various safety functions, designed and operated according to the *functional safety* concept [10], [11], [19]. The objective is to maintain high performance / productivity and reduce various risks related to identified hazards and threats.

The staff and operators play a key role supervising and managing the plant and are responsible for safety-related decision making in entire life cycle. Research results concerning causes of accidents in industrial plants indicate that *human failures* resulting from organisational deficiencies are determining factors of 70-90% cases depending on industrial sector and plant category [19].

In second edition of *functional safety* standards [10], [11] the meaning of *human factors* and *human reliability analysis* (HRA) is emphasized. However, there are no clear indication about the HRA methodology that might support functional safety analysis and management.

In this article an approach is outlined how to deal with the *task analysis* and the *human reliability analysis* (HRA) in context of functional safety analysis using selected methods of the CSE.

Careful analysis of expected human behaviour (including contextual diagnosis, decision making and actions) and potential human errors is a prerequisite of correct evaluation of risks and rational safety-related decision making in life cycle. An approach is proposed to apply selected CSE methods for verifying

the design of functional safety systems to be implemented in an industrial hazardous plant in context of defined safety functions for risk reducing, operator interfaces, communication means and procedures.

2. Cognitive science and cognitive engineering

2.1. Cognitive systems engineering

According to Stanford Encyclopedia of Philosophy *Cognitive science* is the interdisciplinary study of mind and intelligence, embracing philosophy, psychology, artificial intelligence, neuroscience, linguistics, and anthropology [29]. Its intellectual origins are in the mid-1950s when researchers in several fields began to develop theories of mind based on complex representations and computational procedures. Its organizational origins are in the mid-1970s when the *Cognitive Science Society* was formed and the journal *Cognitive Science* began.

Cognitive systems engineering (CSE), called also shortly *cognitive engineering*, has been identified as an important activity in the early 1980s [2], [7]. CSE is rooted in the domains of *human factors and ergonomics*. It arose in response to transformations in the workplace spurred by two major sources:

(1) wide application in practice of computer systems and necessity to develop design principles to ensure that ordinary people, not only informatics' specialists, would be able to interact with them effectively,

(2) safety-critical systems were becoming more complex and increasingly computer controlled, so, design principles were needed to ensure that teams of skilled technicians and less prepared personnel could operate them safely and efficiently.

The discipline of cognitive engineering combines knowledge and experience from *cognitive science*, *human factors*, *human-computer interaction* design, and *systems engineering*. It is distinguished from these applied research disciplines in two primary ways [2], [7], [21]:

- specific focus on the cognitive demands imposed by the external (surroundings) and internal (workplace) environments, and
- concern with complex socio-technical domains in which long term activities and current actions must be conditioned on the expected behavior of other agents, both human and autonomous.

Thus, the CSE is relatively new discipline aimed at development of advanced systems, also those called as the *socio-technical systems*. In socio-technical systems the humans provide essential functionality related to deciding, planning, collaborating and generally managing [2].

Drawing on insights from cognitive, social and organizational psychology, a *cognitive systems engineer* seeks to design particular system that is effective, robust, reliable and safe. The focus is on amplifying the human capability to perform cognitive work by effective and reliable integrating required *technical functions* with *human cognitive processes* [24].

Cognitive systems engineers may assist with the design of human interfaces, communication systems, training systems, teams, and management systems that co-ordinate various activities within identified processes [7]. In particular they employ principles and methods that enable high quality development and design of required processes / procedures and training for more and more advanced technology. Examples of systems that can benefit from CSE are the air traffic control, transportation, communication, process control, power generation, power distribution, health-care, and critical infrastructure.

Cognitive systems engineers identify the *cognitive states*, the *cognitive processes*, and the *cognitive strategies* used by knowledgeable practitioners performing various activities and develop advanced design solutions and new tools for planning and decision making that support subsequently human cognition [7].

Within the development of any large-scale socio-technical system, the CSE has an important role to play thanks to systematic gathering of data and knowledge acquisition for decision making in life cycle. The CSE helps in developing strategies and tools that can be used to identify human-relevant operational requirements and operational demands, to generate human-compatible solution descriptions, and also to design *cognitive decision support systems* (CDSS). It proposes also tools for verifying and validating *cognitive performance* and for monitoring and enhancing *system safety performance* [2],[7].

2.2. Cognitive engineering and hazardous plants

As it was mentioned the *cognitive engineering* is considered as a multidisciplinary domain that focuses on improving the relations between humans and the systems that are supervised and operated. Lately it proposes some applications, including intelligence analysis as well as command and control [7]. Obviously, it is of increasing interest not only for the safety and security domain specialists and experts.

The challenge is to recognize better limitations and strengths of humans and complex systems to develop and then to implement advanced solutions in the organization. They include means for supporting management and operation of technical systems

through making changes in culture, engineering policy, implementing advanced technologies and good engineering practices in the entire life cycle.
For instance, some analysts have showed that team organization and the displays and controls in the plant control room did not support operators' rapid (on time required) recognition of an abnormal state of the plant and undertaking appropriate actions to achieve a safe condition of industrial installation. Also, the conclusions from analyses of commercial aircraft accidents indicated increasing potential for pilot errors due to faulty use of complex automated flight deck systems. Even if the flight deck automation decreased number of some accidents, a new pattern of accidents emerged [7].
Various theories and approaches to the cognitive engineering have been developed. They all tend to involve a few key concepts [2], [7]: the design of complex interactive systems involves an ecological stance, and the design must simultaneously consider people, system, human goals, and the environment in which specified goals or assumed ad hoc goals during major accidents could be achieved. That is, the design must be based on the observation and understanding of system users taking sometimes actions in unfriendly conditions. It emphasizes observation and understanding directed toward developing and using a *cognitive task analysis* (CTA) to solve real problems that captures people's tasks and goals within their work domain.
Methods for systematically investigating users' tasks, organizing the results of observations, and using this information to drive system design and evaluation have become foundations for the emerging engineering discipline of *human-systems integration* [7]. The use of an approach based on cognitive engineering means that the human user (e.g. operator) must be understood in the context of tasks, tools, and work environment.
This gain impetus to the emerging field of *cognitive modeling*, which seeks to capture both the contribution of the domain and the computational characteristics of human cognition that constrain how humans respond to their environment states. In recent years, these approaches and methods have been applied to prevalent issues of *information overload* and *sense making* [7], [29].
Goal-based performance requires that information be transmitted possibly seamlessly as knowledge to the decision maker. To achieve this, the human must be actively involved in information transformation by synthesizing his/her own experience with available information to generate useful knowledge for the decision maker [7].
System complexity is moving the role of systems engineering away from a single individual being a forcing function of hardware and software decisions to that of an *interdisciplinary team* collaboratively integrating hardware, software, and human considerations in system design trade-off analyses and decisions. This enables the systems engineering process to be more robust and responsive to the *mission requirements* [7].
If hardware, software, and human interaction requirements are not integrated during design, it will cause necessity for the human user/operator/decision maker to do that integration in addition to the work demands of the job at hand. Thus, the system design deficiencies become operations problems and require highly skilled users to overcome these deficiencies. These skill requirements drive increased training demands and potential user error problems [7], [29].
The application of cognitive engineering approaches to such areas as intelligence analysis, command and control has received lately increasing attention. Below some safety and security-related issues of industrial plants will be discussed in context of *human system interface* (HSI). The role of human operators in supervising and/or performing various functions in relation to functions of the *industrial automation and control systems* (IACS) [12], operating in a computer network, will be discussed.

3. Functional safety of industrial automation and control system

3.1. Reference model

A reference model of IACS describes a generic view of an integrated manufacturing or production system, expressed as several logical levels [12]. Such model, based on the ISA99 series of standards, is shown in *Figure 1*. This model is derived from a general model used in ANSI/ISA-95.00.01-2000: *Enterprise-Control System Integration* in which following levels are distinguished:

Level 0 – *Technological processes*. It includes the physical process and basic equipment: sensors and actuators directly connected to the process and process equipment, named as equipment under control (EUC).

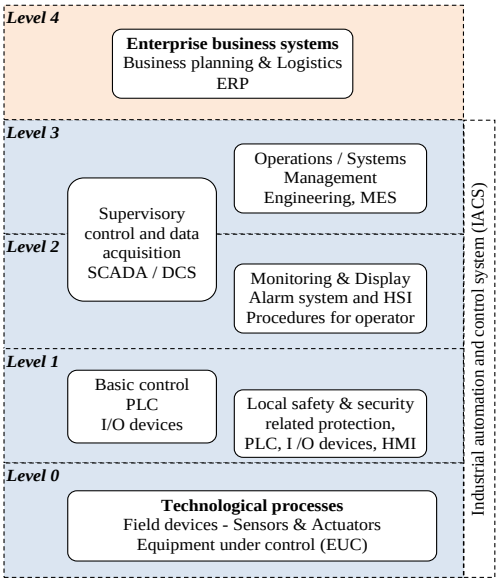

Figure 1. A reference model for the operational management and control of production system

Level 1 – *Basic control and local safety & security related protections.* This level includes continuous control, sequence control, batch control, and discrete control. The protections are implemented using *programmable logic controllers* (PLCs) that monitor the process and are designed to return the process to a safe state if defined limits will be exceeded. This category includes also systems that diagnose the processes and devices, and alert operators through a *human-machine interface* (HMI) about impending unsafe conditions to undertake actions according to elaborated procedure(s).

Level 2 – *Supervisory control*. This level includes the functions of monitoring and controlling the physical process using *distributed control system* (DCS) and *supervisory control and data acquisition* (SCADA) software. There are typically multiple production areas in industrial plants and this level include: operator *human-system interface* (HSI), operator alarms, supervisory control functions and data of the process history.

Level 3 – *Management of operations*. This level includes engineering aspects of operation using a *manufacturing execution system* (MES).

Level 4 – *Enterprise business systems*. This level is characterized by business planning and related activities, including logistics, using an *enterprise resource planning* (ERP) system to manage and coordinate effectively business and engineering processes.

There are essential reliability, safety and security related problems to be considered at all these levels, both during design of the IACS and in the plant operation. It is necessary to begin with identification of hazards and designing safety functions to be implemented in safety-related systems [19]. Below basic issues to be considered relevant to the design of functional safety systems are outlined. These systems are placed mainly at levels 0 and 1 of the reference model (see *Figure 1*).

When the *defense-in-depth* (D-in-D) concept has to be implemented due to a high risk, the *layer of protection analysis* (LOPA) methodology [22] is usually applied. In such analysis the human operator activities are of prime importance including relevant tasks and available functions of the alarm system. In such cases the levels 2 and 3 of the reference model have to be also considered together with lower levels characterized above.

3.2. Functional safety systems for reducing risk

Figure 2 illustrates a basic concept of the risk reduction in hazardous industrial plant. It assumes that [10], [19]:

– there is certain configuration of *equipment under control* (EUC) and its control/protection system;
– there are associated human factor issues;
– the protection system comprises a *electrical / electronic / programmable electronic* (E/E/PE) system [10] or a *safety instrumented system* (SIS) [11], and there are other safety measures reducing risk.

Thus, a risk model for a specific application has to be developed taking into account the specific manner in which the necessary risk reduction is being achieved by the E/E/PE implementing defined *safety functions* (SF) regarding other risk reduction measures [17].

The risk measures shown in *Figure 2* for a *low demand mode of operation* [10] are as follows:

– the *EUC risk* R_{np} - the risk existing for specified hazardous event (no designated safety protective features are considered);
– the *tolerable risk* R_t - the risk which can be presumably accepted taking into account current societal values or opinions of experts;
– the *residual risk* R_r - remaining risk for the specified hazardous events after risk reduction.

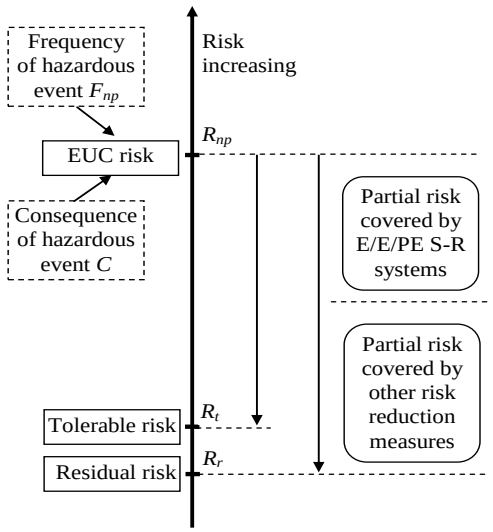

Figure 2. Risk reduction for low demand mode of operation

The risk measure R_{np} can be evaluated using the formula as follows

$$R_{np} = F_{np}C \tag{1}$$

where: F_{np} is the frequency of a hazardous event (without considering protection), i.e. the demand rate on the safety-related system per year [a^{-1}]; and C denotes a consequence of this hazardous event (in units of a consequence).
The tolerable risk is determined as follows

$$R_t = F_t C_x \tag{2}$$

where: F_t is the tolerable frequency of hazardous event (with protection) [a^{-1}]; C_x is the consequence of hazardous event (in units of consequences) usually reduced, i.e. $C_x < C$.
For the operation mode considered the *average probability failure on demand* (PFD_{avg}) of the *protection function* is calculated, assuming $C_x = C$, from the formula

$$PFD_{avg}^{r} \le F_t / F_{np} \tag{3}$$

Knowing the value of PFD_{avg}^{r} the required *safety integrity level* (SIL) [10] for given SF implemented in the E/E/PE system, is to be determined regarding defined *criteria intervals* [10], [20]. For instance if $PFD_{avg} = 3 \cdot 10^{-4}$, then SIL3 is determined [10]. Requirements concerning the SIL for software of the E/E/PE system or SIS, implementing given SF, are specified in part 3 of IEC 61508 [10].
Having required SIL for given SF, some architectures of the E/E/PE system or SIS are considered. For given system architecture the *average probability failure on demand* PFD_{avg}^{Sys} of this *protection system* is calculated using probabilistic model developed, to meet relevant interval criterion (preferably $PFD_{avg}^{Sys} \le PFD_{avg}^{r}$).
The average probability of failure on demand of the E/E/E system can be calculated from formula [19]

$$PFD_{avg}^{Sys} \cong PFD_{avg}^{A} + PFD_{avg}^{B} + PFD_{avg}^{C} \tag{4}$$

where: A, B, and C are subsystems respectively of sensors, logic devices, and actuators generally of KooN configuration.
The probabilistic model for consecutive subsystems is to be built with regard to the reliability data for hardware elements and parameters characterizing potential *common cause failures* (CCF). Probabilities of potential *human errors* are also considered applying appropriate method of the *human reliability analysis* (HRA) [9] to calculate human error probability (HEP) [8], [26], [27].
In case of finding alternative architectures that meet the probabilistic criterion for PFD_{avg}^{Sys} and software related requirements [10], additional aspects may be considered to determine final architecture, for instance: costs, diagnostics, quality related requirements, experience in operation similar solution, testing requirements, training issues, etc.

3.3. Protection layers

Industrial hazardous 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 required *safety-integrity level* (SIL), which should be then verified in the probabilistic modeling process. It is important to include in probabilistic models to be developed potential dependencies between failure events.
In *Figure 3* typical layers of protection of in a hazardous plant are presented. An interesting methodology for preliminary risk analysis and safety-related decision making is the layer of protection analysis (LOPA) [22].

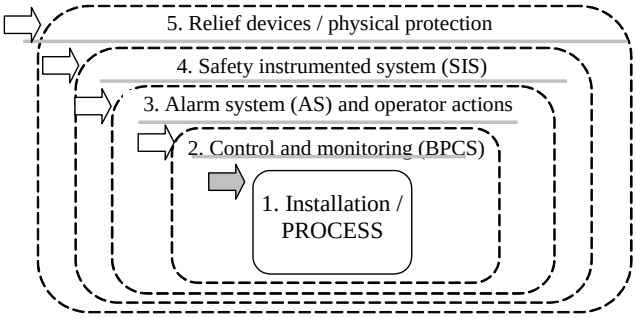

Figure 3. Typical protection layers in hazardous industrial installation

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

Protection layers (LPs) shown in *Figure 4* include:

- PL1 – the *basic process control system* (BPCS),
- PL2 – OPERATOR supervising the process and intervening in cases of abnormal situations or accidents that using the alarm system (AS),
- PL3 – the *safety instrumented system* (SIS) to perform *emergency shutdown* (ESD) function.

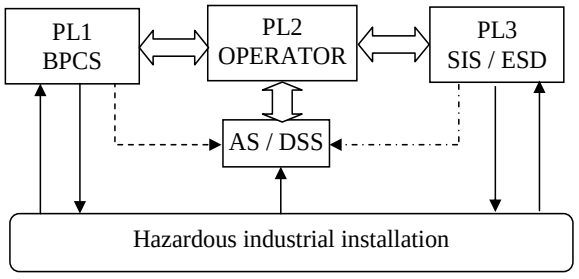

Figure 4. Operator and the alarm system (AS) as elements of protection layers

These layers should be independent what requires appropriate technical and organizational solutions. In case of PL1 and PL3 it can be achieved using separate sensors and input elements, input 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 the safety integrity level (SIL) of the SIS.

Only in case of independence of protection layers (IPLs) the frequency of *i*-th accident scenario F_i can be calculated using the formula [18]

$$F_i = F_i^I \cdot PFD_{i;IPL1} \cdot PFD_{i;IPL2} \cdot PFD_{i;IPL3} = F_i^I \cdot PFD_i \tag{5}$$

where F_i^I is the frequency of *i*–th initiating event *I* per tear [a^{-1}] and $PFD_{i;PLj}$ are probabilities of failure on demand of *j*-th protection layer shown in *Figure 4*, assuming IPLs. In case of the second layer $PFD_{i;IPL2} = HEP_{i;IPL2}$, and relevant HEP (*human error probability*) is evaluated using appropriate HRA method [8], [9].

Generally the dependency of relevant events should be assumed and the frequency of accident scenarios for potentially layers should be evaluated using relevant formula consisting of conditional probabilities

$$F_i^Z = F_i^I \cdot P(X_{i;PL1} \mid I) \cdot P(X_{i;PL2} \mid I \cdot X_{i;PL1}) \cdot P(X_{i;PL3} \mid I \cdot X_{i;PL1} X_{i;PL2}) = F_i^I \cdot PFD_i^D \tag{6}$$

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 evaluations have shown that assuming dependencies (D) of layers in a probabilistic model significantly increases the failure probability on demand at least an order of magnitude, thus $PFD_i^D >> PFD_i$ (see formula (5) and (6)).

If the risk reduction requirement for the protection system is 10^{-4} then it can be achieved, according to (5), by assigning as follows: 10^{-1} for IPL1 (BPCS: SIL 1), 10^{-1} for IPL2 (HEP) and 10^{-2} for IPL3 (SIS: SIL2), which are values relatively easily to achieve in industrial practice.

There is, however, a considerable problem concerning the layer PL2, i.e. OPERATOR who obtains information through relevant HMI/HSI from the BPCS and SIS, and also from the *alarm system* (AS) or the *decision support system* (DSS). The independency of these layers can be improved thanks to appropriate designing the alarm system (AS) to be physically and functionally separated [4].

Thus, significant meaning in reducing dependencies of mentioned above layers has appropriate designing of the *alarm system* (AS) and *decision support system* (DSS) [6] as well as the quality of the HMI/HSI design.

The human reliability may be improved by appropriate influence on *performance shaping factors* (PSFs). Some concepts and formulas for calculating HEPs regarding PSFs when performing the *human reliability analysis* (HRA) [26], [27] are discussed below.

4. Cognitive aspects in human reliability analysis

4.1. Human behaviour types and potential errors

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 that operates in environmental conditions. However, some basic assumptions made in HRA within *probabilistic safety analysis* (PSA) of hazardous systems are still the subject of dispute between researchers [8], [15].

It is worth to mention that the *functional safety analysis* (FSA) framework, including the safety-related functions to be implemented using the control and protection systems (BPCS, SIS) as well as assumptions concerning HMI/HSI in relation to the *alarm system* (AS) and *decision support system* (DSS) gives more insights in performing HRA [18].

In performing HRA some basic knowledge concerning concepts of human behaviour and error types is helpful. Rasmussen [23] 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 some common sense rules and previously developed procedures), and
- *knowledge-based* (performance of novel actions when familiar patterns and rules cannot be applied directly, and actions that follow the information processing with the inclusion of diagnosis, planning and decision making).

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

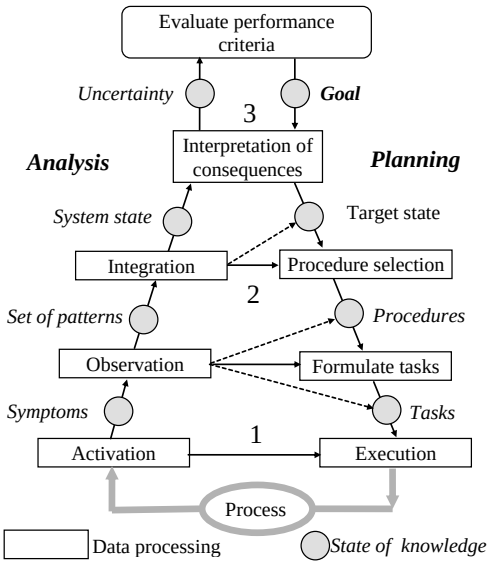

Figure 5. Schematic representation of information processing by operators and human behaviour types (1 - *skill*, 2 - *rules*, 3 – *knowledge*)

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 [23].

Described above behaviour types seem to involve different error mechanisms, which may mean radically different human reliability characteristics. Reason [25] 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 rather 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 6*, which combines two frameworks outlined above [16]. Three error types are

distinguished: (1) *skill-based*, (2) *rule-based*, and (3) *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 [12]. The error of omission and error of commission are distinguished according to THERP methodology developed by Swain and Guttmann [27].

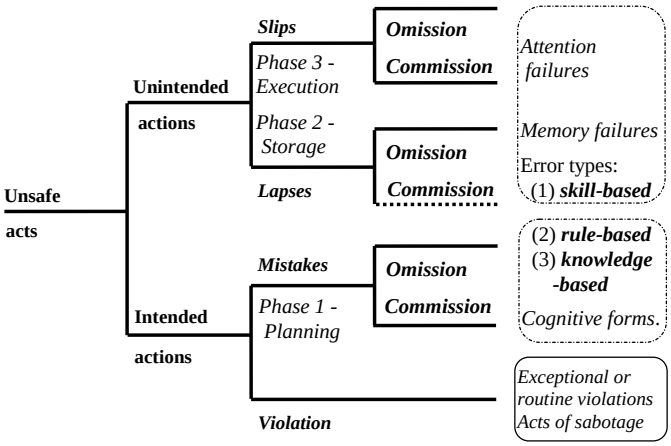

Figure 6. Classification of human unsafe acts and error types

4.2. Cognitive processes modelling issues

Systems engineering (SE) has traditionally focused on the technological aspects of system design, such as hardware, software and automation, while largely ignoring the fact that these systems will ultimately be used in the service of humans to meet the mission / production goals and the demands work domains. The omission in considering humans as key components of an enterprise is a serious issue in the current practice of SE [2], [7].

The fact is that modern enterprise can be characterised as a complex interaction of humans and processes as well as hardware and software systems, and humans will be always be central players in such enterprises because of their creativity, expertise, and adaptability [7]. The goal of *cognitive engineering* (CE) is to develop systems, training, and other products that support cognitive functions in decision-making, situation assessment, course-of-action selection, resource allocation and other information processing tasks .

The CE methods and models are classified with regard to their focus and application purpose. Five categories of CE modelling methods are distinguished as shown in Figure 7:

1. *Human-machine systems,*
2. *Behavioral processes,*
3. *Behavioral and cognitive processes,*
4. *Cognitive processes,*
5. *Identification of erroneous diagnoses and/or actions.*

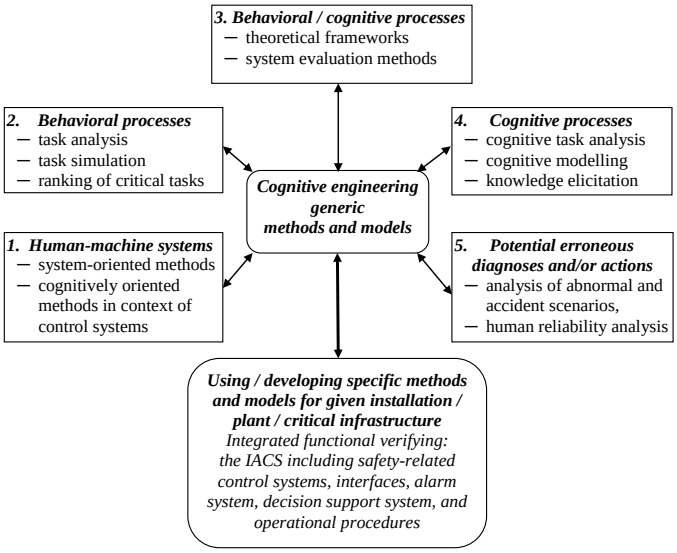

Figure 7. Classification of cognitive engineering methods (based on [2])

Each of these categories can be subdivided into some specific methods to be used depending on the issue to be analysed. For instance, following methods are available in the *cognitive task analysis* (CTA) (see block 4 in *Figure 7*) [2], [14]:

- *Skill-based CTA framework,*
- *Applied CTA,*
- *Critical decision method,*
- *Task-knowledge structures,*
- *Goal-directed task analysis,*
- *Cognitive function model,*
- *Cognitively oriented task analysis,*
- *Hierarchical task analysis,*
- *Interacting cognitive subsystems,*
- *Knowledge analysis and documentation system.*

One or more of these methods are of interest in following engineering phases [2]:

- Concept definition,
- Requirements analysis,
- Function analysis,
- Function allocation,
- Task design,
- Interface & team development,
- Performance, workload, and training estimation,
- Requirements review,
- Personnel selection,
- Training development,

– Performance assurance,
– Problem investigation,
– Competence management.

Analysis of abnormal and accident scenarios before performing human reliability analysis (block 5 in Figure 7) can be supporting using one or more selected techniques from following methods:

– *Event tree analysis (ETA),*
– *Fault tree analysis (FTA),*
– *Failure modes and effects analysis (FMEA),*
– *Barrier analysis (BA),*
– *Hazard and operability analysis (HAZOP),*
– *Management oversight risk tree (MORT),*
– *Work safety analysis (WSA),*
– *Confusion matrices (CM),*
– *Operator action event tree (OAET),*
– *Generic error modeling system (GEMS),*
– Cognitive reliability and error analysis method (CREAM).

Embrey distinguishes in his publication [5] two categories of task analysis techniques:

(1) Action oriented techniques, e.g. *Hierarchical task analysis (HTA)*, and *Operation action event tree (OAET)*,

(2) Cognitive task analysis techniques, e.g. *Critical action and decision evaluation technique* (CADET), and the *Influence modeling and assessment system* (IMAS) .

The selection of particular method depend on the problem to be solved. An important criterion is its maturity and effectiveness of implementing in the plant design or during operation. Their usefulness can differ depending on engineering phase.

4.3. Towards improved goals oriented human-operator decisions and actions

Depending on the complexity of the function and tasks there can be several levels of activities distinguished. The high level function is broken into sub-functions. The sub-functions can be broken into tasks, the tasks into task steps. The steps can be further broken into activities (*Figure 8*). Activities are at the lowest level of analysis and describe behaviours such as monitoring a process state.

To achieve consecutive goal the operators use a procedure from a set of predefined procedures developed for some categories of transients, abnormalities and accident situations. The structure of the function based displays using the results of task analysis and functional decomposition is shown in *Figure 9*.

A few goals can be extracted from the procedure, and these goals can be achieved by defined functions. These functions can be further decomposed into tasks. Thus this figure shows the display design model of a function based display distinguishing three levels of pages/screens for: I - function (a page with concise information), II - sub-functions and III – tasks consisting of more detailed information.

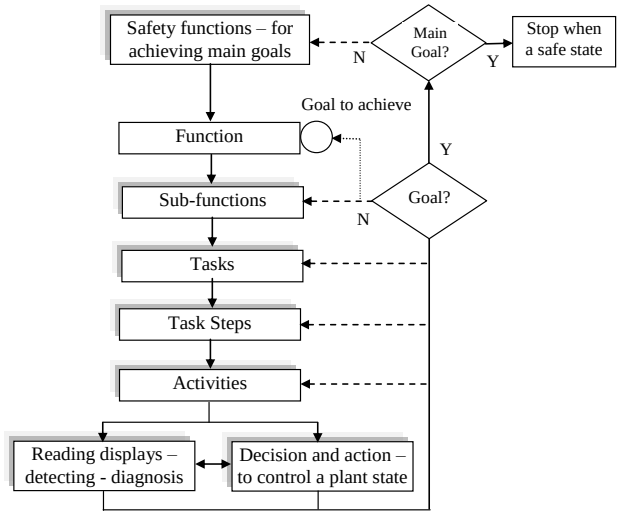

Figure 8. Hierarchy of goals, functions, tasks and human operator activities

The task and sequence related information may be significant inputs in procedure development. In fact, draft procedures can be written directly from the task analysis, especially when new tasks are issued from the function allocation. The documentation should be produced to verify human factors involvement in the control room design.

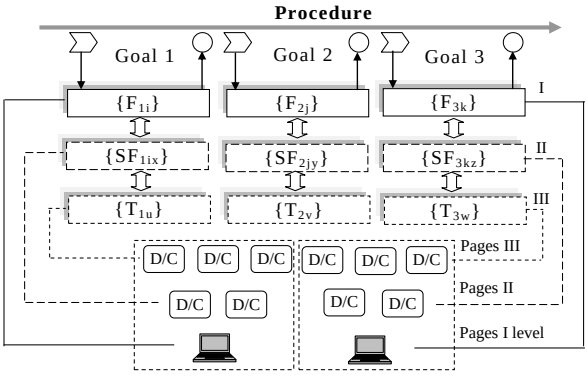

Figure 9. Functions (F), sub-functions (SF) and tasks (T) based HSI design model with three levels of display/control (D/C) pages

The task related data should be stored on a database system to allow manipulation and updating of information. When completed, the task area database will incorporate all event sequences, and the related results from the analysis of those sequences.

The issues outlined above require further research due to functional limitations and flaws of currently used

solutions, especially interfaces related to the alarm system [4].

4.4. Issues of human reliability analysis

Practically all HRA methods assume that it is meaningful to use the concept of human errors and it is justified to estimate their probabilities [9], [27]. Such point of view is sometimes questioned due to not fully verified assumptions concerning human behaviour and potential errors. There are even opinions raised that the HRA results are of limited value as input for the PSA, mainly because of oversimplified conception of human performance and human error. It concerns first generation of HRA techniques.

The direction is to develop next generation of HRA methods including cognitive aspects of human actions and potential errors. There is no doubt that potential human errors should be considered in given context (process dynamic, automation, protection, HMI/HSI, quality of procedures, etc). Some potential human errors in a process installation and their rough consequences are presented in *Figure 10*.

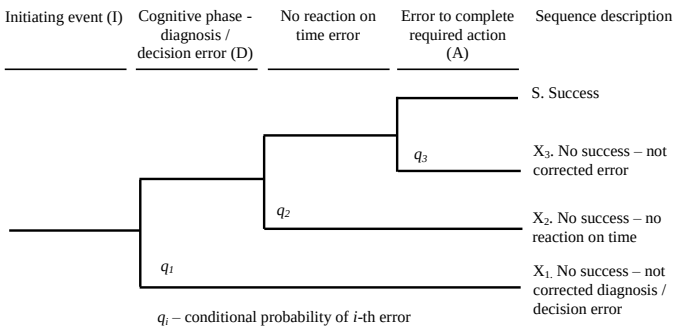

Figure 10. Examples of human-operator errors and their consequences

Several traditional HRA methods are used in PSA practice, e.g. THERP method [27], developed for the nuclear industry, applied also in various industrial sectors. Other HRA methods more often used in industrial practice are: *Accident Sequence Evaluation Procedure* (ASEP), *Human Error Assessment and Reduction Technique* (HEART), and *Success Likelihood Index Method* (SLIM). These conventional HRA methods are characterised in various papers, monographs and reports [9], [16].

In several publication selected HRA methods have been evaluated taking into account either relatively widespread usage and opinions of experts. The main interest was in using following techniques:

- *Technique for Human Error Rate Prediction* (THERP) [27];
- *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 the *human error probabilities* (HEPs) for situations encountered in practice of PSA. Comparisons were also made in relation to relatively new SPAR-H method [26]. The final conclusion was formulated that the enhanced SPAR-H methodology is useful as an easy-to-use, broadly applicable, HRA screening tool. However, lately some critical opinions have been raised concerning this technique, especially as regards assumptions concerning the *nominal human error probability* (NHEP) for diagnosis and action (see formula (8) below).

The results of various research indicate that the HEP in a dynamic process installation depends strongly on its complexity and the time available for the diagnosis, decision making and actions. In *Figure 11* the results of a nominal diagnosis model is presented for evaluating the HEP for diagnosis of one abnormal event by the control room personnel within time window T available. For time window T below 5 minutes the HEP is above 0.5. It shows that assuming in some studies HEP = 0.1 [11] is not justified in complex systems.

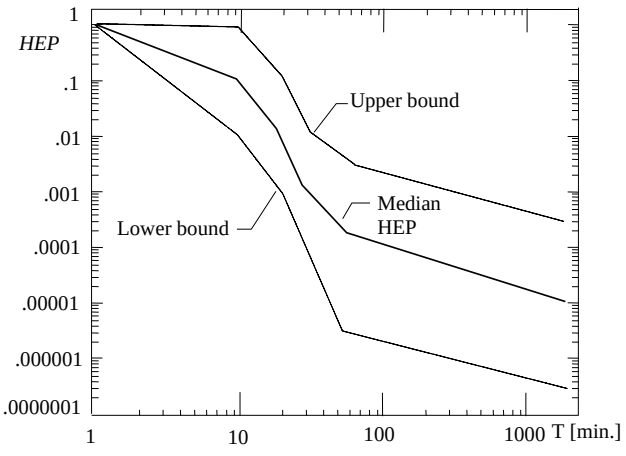

Figure 11. Human error probability for diagnosis within time window T of one abnormal event by the control room personnel [27]

The HEP is evaluated when the human failure event is placed into the probabilistic model structure of the system considered. In the HRA performed within PSA only more important human failure events are considered [8]. Then, for an abnormal situation context to be considered the *performance shaping*

factors (PSFs) [3], [27] are evaluated according to rules of given HRA method. As the result of HRA a particular value of HEP is calculated using relevant formulas. Obtained HEP value is used in the PSA for quantitative evaluation of accident scenario.
Different approaches are used for evaluating HEP regarding a set of PSFs [15], e.g. assuming a linear relationship for each identified PSF_k and its weight w_k, with constant C for the model calibration

$$HEP = HEP_{nominal} \sum_k w_k PSF_k + C \tag{7}$$

or nonlinear relationship used in the SPAR-H methodology [26]

$$HEP = \frac{NHEP \cdot PSF_{composite}}{NHEP(PSF_{composite} - 1) + 1} \tag{8}$$

where: NHEP is the nominal HEP; the NHEP is assumed to be equal 0.01 for diagnosis (D), and 0.001 for action (A) (see *Figure 10*).
An appreciated method for performing HRA for a set of PSFs is SLIM [9]. The SLIM is oriented on success probabilities of events to accomplish specified tasks. However, the probabilistic modeling for the risk evaluation 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 oriented indices SI_j for *j*-th task are as follows

$$\lg HEP_j = c \cdot SI_j + d \tag{9}$$

$$SI_j = \sum_i w_i r_{ij} \tag{10}$$

where: w_i - normalized 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 (normalized scaling value is $0 \le r_{ij} \le 1$).

If for cases considered the success indices SI_j have been 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* are determined and the HEP value is calculated for particular task of interest.

4.5. Oil port installations and cognitive human reliability analysis in context of functional safety

The contribution to the HAZARD project is proposed to elaborate methods of probabilistic modelling of the oil port installations and the IACS that implement safety functions for reducing risks, useful in developing procedures for:
- *Evaluation of overfill and leak related risks of terminal tanks,*
- *Evaluation of short and long distance piping operational risks,*
- *Evaluation of functional safety in life cycle of the control and protection systems for planning tests and maintenance of equipment,*
- *Layer of protection analysis including the alarm system and human factors.*

For developing these procedures applying the *cognitive task analysis* (CTA) methods are of prime importance, in context of communication measures, interfaces and procedures, for verifying SIL of safety functions implemented in the IACS. The focus will be on more probable abnormal states and accidents, and identification of potential human errors. This will support dependable cognitive *human reliability analysis* (HRA) for evaluation of relevant risks and safety-related decision making in life cycle.
The research scope planned within the HAZARD project include the tank overfill related risks. It is known that the safety of an oil port terminal depend on available functions of the IACS, HMI/HSI interfaces, communication measures and available diagnostics. The consequences of incorrect human-operator decisions and/or actions can be very serious. These issues are considered in the API 2350 guidelines [1].
Tank overfills are a major concern to the petroleum industry and oil port terminals. The industry has worked jointly to develop a new API/ANSI Standard 2350 Edition 4: *Overfill Protection for Storage Tanks in Petroleum Facilities*. This standard contains a description of the *minimum requirements* required to comply with modern best practices in this specific application. The main purpose is to prevent overfills, but another common result of applying this standard is increased operational efficiency and higher tank availability [1].
The API 2350 proposes the latest principles for management systems, e.g. a *business continuity management system*. Generally, the operational improvements may result from [1], [28]:
- Simplified and clarified response to alarms,
- More usable tank capacity,
- Generalized understanding and use of the *Management of change* (MOC) process,
- Operator training and qualification,
- Inspection, maintenance and testing,
- Procedures for normal and abnormal conditions,

- Lessons learned used to evolve better operational, maintenance and facility practices,
- Management System, *Overfill prevention Process* (OPP),
- Risk assessment system,
- Operating parameters – *levels of concern* (LOCs) and alarms, categories, response time,
- Procedures.

Following categories of the overfill protection systems will be considered in ongoing research and case studies to be compatible with API 2350 [1]:

Category I system - local manual operations using hand gauging or *automatic tank gauging* (ATG), manual intervention by local operator,

Category II system - local and/or remote manual operations, tank level may be read using ATG or sensor(s), manual intervention by local operator and/or remote operator or automated shutdown,

Category III system - local and/or remote manual operations, tank level given by ATG, independent *alarm level high-high* (LAHH), manual intervention by local operator and/or remote operator,

AOPS (*Automatic overfill prevention system*) system - this system is independent of and in addition to the basic systems of categories: 1, 2 and 3, the *level shutdown high* (LSH) automatically, without operator intervention, terminates incoming flow.

5. Conclusions

The cognitive engineering is considered nowadays as interesting multidisciplinary domain that might improve the relations between humans and the complex systems that are supervised and operated.

The industrial automation and control systems (IACS) in hazardous plants are increasingly computerized and perform various safety functions, designed and operated according to the functional safety concept. The objective is to maintain high performance / productivity and reduce various risks related to identified hazards and threats.

In the second edition of *functional safety* standards the importance of *human factors* and the *human reliability analysis* (HRA) is emphasized. However, there are no clear indication how the cognitive engineering might support functional safety analysis and safety management of complex plants.

An approach is proposed to apply selected cognitive engineering methods for verifying proposed design of the functional safety solutions to be implemented in given hazardous plant in context the IACS design, protection layers, operator interfaces, communication means and procedures. The methodology developed might be applied for integrated safety and security management of industrial hazardous plants and oil port terminals.

Acknowledgements

The paper presents the results developed in the scope of the HAZARD project titled "Mitigating the Effects of Emergencies in Baltic Sea Region Ports" that has received funding from the Interreg Baltic Sea Region Programme 2014-2020 under grant agreement No #R023. https://blogit.utu.fi/hazard/

References

[1] API 2350 (2012). Overfill Protection for Storage Tanks in Petroleum Facilities, ANSI/API Standard 2350.

[2] Bonaceto, C., Burns, K. (2005). Using Cognitive Engineering to Improve Systems Engineering. MITRE Corporation, Bedford.

[3] 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.

[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] Embrey, D. (2000). Task analysis techniques. Human Reliability Associates Ltd.

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

[7] Gersh, J.R., McKneely, J.A. & Remington, R.W. (2005). Cognitive Engineering: Understanding Human Interaction with Complex Systems. *John Hopkins Technical Digest*, Vol. 26, No. 4.

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

[9] HRA-HSE (2009). Review of human reliability assessment methods. Research Report RR679 prepared for Health and Safety Executive.

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

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

[12] IEC 62443 (2013). Security for industrial automation and control systems. Parts 1-13

(undergoing development). International Electrotechnical Commission, Geneva.
[13] ISO 31000 (2009). Risk management - Principles and guidelines. International Organization for Standardization, Geneva.
[14] Kirwan, B., & Ainsworth, L. K. (1992). *A guide to task analysis*. New York: Taylor and Francis.
[15] Kirwan, B. (1994). *A Guide to Practical Human Reliability Assessment*. CRC Press, London.
[16] 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).
[17] Kosmowski, K.T. (2006). Functional Safety Concept for Hazardous System and New Challenges. *Journal of Loss Prevention in the Process Industries* 19 (298-305).
[18] Kosmowski, K.T. (2011). Functional Safety Analysis including Human Factors. *International Journal of Performability Engineering* 7 (1), 61-76.
[19] Kosmowski, K.T. (2013). *Functional safety and reliability analysis methodology for hazardous industrial plants*. Gdańsk University of Technology Publishers.
[20] Kosmowski, K.T. & Śliwiński, M. (2015). *Knowledge-based functional safety and security management in hazardous industrial plants with emphasis on human factors. In: Advanced Systems for Automation and Diagnostics*, PWNT, Gdańsk.
[21] Lintern, G. (2012). Cognitive Systems Engineering. Cognitive Systems Design, Melbourne.
[22] LOPA (2001). Layer of Protection Analysis, Simplified Process Risk Assessment. Center for Chemical Process Safety. American Institute of Chemical Engineers, New York.
[23] 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.
[24] Rasmussen, J., Svedung, I. (2000). *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, Karlstad.
[25] Reason, J. (1990). Human Error. Cambridge University Press.
[26] SPAR-H (2005). Human Reliability Analysis (HRA) Method, NUREG/CR-6883, INL/EXT-05-00509, USNRC.
[27] Swain, A.D. & Guttmann, H.E. (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278. Washington: US Nuclear Regulatory Commission.
[28] UN (2006). Maritime security: elements of an analytical framework for compliance measurement and risk assessment. United Nations, New York and Geneva.
[29] Wilson, R.A. & Keil F.C. (Eds.) (1999). The MIT Encyclopedia of the Cognitive Sciences. A Bradford Book, Massachusetts Institute of Technology (MIT), The MIT Press.