Kosmowski Kazimierz T.

Śliwiński Marcin
Gdańsk University of Technology, Gdańsk, Poland

Organizational culture as prerequisite of proactive safety and security management in critical infrastructure systems including hazardous plants and ports

Keywords

behaviour-based safety, organizational culture, proactive safety and security management

Abstract

This article addresses selected aspects of organizational culture to be considered in the context of knowledge based proactive safety and security management of plants, ports and systems of critical infrastructure. It has been often emphasized in the domain literature that business effectiveness of such plants and their resilience against hazards and threats to avoid major accidents depends substantially on human and organizational factors. It becomes obvious that appropriate shaping of these factors is crucial and should be considered in life cycle. Some terms have been also introduced such as safety culture and security culture. Current research topic in this domain includes an interface between safety and security. The article discusses these issues in the context of knowledge based proactive safety and security management being a new challenge, especially in cases of hazardous plants, ports and other complex systems of critical infrastructure.
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 accidents in industrial plants indicate that broadly understood *human failures*, resulting often from organisational inadequacies and neglects, are determining factors in 70-90% of cases, depending on industrial sector and plant category [19], [27]. 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 [28].
It has been emphasized that such accidents arose from a combination of *latent and active human errors*. 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 and *active frontline human errors*, can contribute to a major accident. Some categorizations of human actions and related errors have been proposed, e.g. by Gertman and Blackman [29], Rasmussen [27], and Reason [28].
The human errors are to 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.
The probabilities of failure events depend on various human and organisational factors, categorised usually as a set of performance shaping factors (PSFs) relevant to the situation or scenario under consideration [3], [19]. The PFSs are divided into internal, stressor and external ones and can be evaluated applying various methods [7].
Traditionally, potential human and organisational influences that deteriorate industrial plant operation are to be incorporated into the probabilistic models as defined failure events with relevant probabilities

evaluated using selected method of human reliability analysis (HRA) [7].
Careful analysis of expected human behaviour (including context oriented diagnosis, decision making and actions), and potential errors is prerequisite of correct (credible) risk assessment and rational safety-related decision making.
Some terms have been introduced in the domain literature such as *safety culture* and *security culture*. They are in certain relation to *organizational culture*. The article discusses the issue of organizational culture in the context of proactive safety and security management. This is an important current research topic and challenge in industrial firms, especially in cases of hazardous plants, ports and other complex systems of *critical infrastructure* (CI).

2. Towards organizational culture for effective business and safety

2.1. Traditional behavior-based safety concept

Developed in the late 1970s the *behavior-based safety* (BBS) approach has been aimed to bring together parts of *behavioral science* with *industrial safety experience* to create a process for promoting safety as important organizational value.
As it was mentioned many research works have indicated (published from the middle of previous century) that depending on industrial sector 70-90% of all accidents were caused by unsafe behavior of workers. According to some researchers the BBS has had an impressive record in improving safety of employees in the industry [6].
From that time various traditional engineering and management approaches have been developed to implement such technical and administrative solutions as automation, procedure compliance, administrative controls and OSHA type standards and rules. They have been often successful and contributed to certain extent in reducing the number of accidents and scope of losses. However, relatively many of incidents and accidents have been still bothersome to managers and workers [6], [9], [25].
It was postulated that evaluating the percent of safe acts could be one of leading safety indicator. This means that the observation and feedback techniques of BBS might be used to predict that safety problems in given facility. Rather doubtful idea was raised that intensifying the BBS observation cycle would contribute to preventing injuries or accidents.
Most behavioral safety processes have been tailored to the work and management environment of the site. The behavioral safety processes can be divided in principle into three major components [6]:

1. Development of a list of at-risk behaviors,
2. Observations, and
3. Feedback.

The process starts with a behavioral hazard analysis to identify at-risk behaviors. These can be determined using accident/incident reports, job hazards analysis, employee interviews and brainstorming. In some instances a combination of these information sources proved to be useful.
Having the at-risk behaviors, a checklist can be then developed to assist in the observation of work behavior. In addition, a list of corresponding behavior definitions is helpful in maintaining consistency between observers and the resulting data. Observers record safe and at-risk behaviors on the datasheet and provide feedback to workers as regards their performance. It was assumed that this feedback reinforces an inclination for safe behaviors [6].
The observation data should be also used to identify existing barriers to safe behavior. Removing these barriers contribute to lowering the exposure to at-risk conditions and makes it easier for employees to work efficiently and safely. In addition, communicating safer solutions increase positively involvement of employees in the work processes.
Seven guiding principles have been proposed for *integrated safety management system* (ISMS) in a context of BBS processes [6]:

1. Line management responsibility for safety (the responsibility for safety and the BBS processes is shared by management and front-line workers; all levels of the organization are involved in an effective BBS process).
2. Clear roles and responsibilities (functions within the BBS process are performed at the proper level and are integrated and adapted to fit for the organization itself).
3. Competence of employees commensurate with responsibilities (an effective BBS process provides the skills needed to perform the tasks and functions associated with the job in a timely manner).
4. Balanced priorities (BBS provides the consistent safety data that enables managers to balance safety priorities with production and other operational needs).
5. Identification of safety standards and requirements (such standards and requirements can offer aid in developing the list of behaviors and definitions used in the BBS process).
6. Hazard controls tailored to work/tasks being performed (the observation provides monitoring of processes so that hazard controls reflect the risks associated with work being performed in changing conditions).
7. Operations authorization (the BBS process helps in providing the behavior-related safety

information necessary to make decisions prior to initiating operations).

In addition five core functions of such ISMS have been distinguished [6]:

(1) Define the scope of work and safety-related tasks.
(2) Analyze the hazards involved.
(3) Develop and implement hazard controls.
(4) Perform work and tasks within controls.
(5) Provide feedback from experience and continuous improvement.

There are also indicated five conditions that increase the success likelihood of BBS processes [6]:

(A) Safety leadership.
(B) Establishing integrated safety management system.
(C) Employee empowerment and participation in safety related activities.
(D) Organization's safety culture.
(E) Measurement and accountability.

Setting up a *Steering Committee* (SC) was proposed for the implementation and continuation of the BBS process in a large organization. The initial SC should be selected from qualified employees representing each distinct group, team, etc. of the organization. Basic responsibilities of the SC include [6]:

- Develop the at-risk behaviors inventory;
- Participate in the training and coaching of observers to provide mentoring the process;
- Design the observation process;
- Analyze periodically the observation data;
- Build action plans to respond to the leading indicators seen in the data;
- Ensure communication with observers;
- Ensure that BBS is promoted and communicated to all organizational levels.

The observation data gathered are used to develop plans for risk reduction. Customizing the inventory is also critical in promoting acceptance and ownership of the process by the employees. Critical behaviors should be organized by risk-related factors, and in order to indicate their potential severity.

The results obtained in terms of percentage injury reduction indicate the effect of safety-related solutions [6], [9]: engineering (29% reduction), management audits (19%), poster campaigns (14%), near miss reporting (0%), but reported 51.6% due to *comprehensive ergonomics* and 59.6% due to *behavior safety–related modification*. It indicates that the BBS approach can influence different aspects of the safety problem.

The results of observations should be reviewed periodically (at least annually) for applicability by the SC. New at-risk behaviors should be identified especially when new equipment, facilities and processes are introduced. Organizations that properly implement BBS see the return on the investment (ROI) of spending safety resources directly in the active work area, and this also leads to the reduction of injuries [6].

Thus, the BBS has been recognized by some researchers as a process that provides organizations the opportunity to move to a higher level of safety excellence by promoting *proactive responding* to leading indicators that are statistically valid, building ownership, trust, and unity across the team, and developing empowerment opportunities which relate to employee safety.

However, there are also critical remarks in the literature concerning the BBS approach [9], because it focuses mainly on worker behavior rather than systemic problems of hazards inherent to the work processes. By focusing on unsafe acts of workers as the causes of injuries and illnesses, companies could sometimes do little to address potential root causes of safety and health related risks. In this sense it is considered as a *reactive approach*.

2.2. Toward more proactive safety management

Some models have been proposed to compare the method used by *health and safety at work* (HSW) programs versus the method used by the BBS programs [9]. The HSW process uses usually all the information available for identifying hazards and controls. Past experience and knowledge are embodied in standards and regulations.

This method seeks input information from abnormal activities of workers and includes systematic analysis of injury and illness records. The review should be objective, not prejudiced by an assumption that the overwhelming majority of injuries and illnesses are caused by unsafe acts. The hazards can be then prioritized based on the risk levels according to the risk analysis model. Finally, the hazards should be controlled using the most effective methods designated by a hierarchy of controls.

The hierarchy of health and safety at work controls includes [9]:

(1) Elimination or substitution (substitute for hazardous material; reduce energy, speed, pressure, voltage, sound level, force; change process to eliminate noise; perform task at ground level; automated material handling, etc.).

(2) Engineering controls (ventilation systems; machine guarding; sound enclosures; circuit breakers; platforms and guard railing; interlocks, lift tables; conveyors; balancers).

(3) Warnings (computer warnings; odor in natural gas; signs; backup alarms; beepers; horns; labels).

(4) Training, procedures and administrative controls (safe job procedures; rotation of workers; safety equipment inspections; hazard communication training; lock out; confined space entry).

(5) Personal protective equipment (safety glasses; ear plugs; face shields; safety harnesses and lanyards; back belts, etc.).

One of the most successful efforts in occupational fatality prevention was implemented at *General Motors* in 1992. General Motors had a long history of fall fatalities [9]. The *United Automobile Workers (*UAW*) Union* and *General Motors* were determined to address this problem. A fall prevention program was developed and implemented at all of General Motor's United States operations.

The program has been applied the identification, evaluation and control model. Methods of control were selected using the hierarchy. Major emphasis was placed on eliminating work at heights whenever possible and installing engineering controls. Personal fall protection equipment was used as a last resort. It contributed to significant decreasing of injuries and fatalities.

With the introduction of greater automation and more complex manufacturing machinery and equipment, the percentage of workers in skilled trades climbed to the current level of about 21%, a 36% increase in the population of skilled trades workers. In addition, production workers were expected to perform more complex tasks that include setup, minor troubleshooting, un-jamming of parts, preventive maintenance, and fault clearance.

The efforts undertaken included following technical and organizational solutions [9]:

1. Establishment of written lockout programs.
2. Installation of additional safeguards, and machinery modifications to enable workers to perform tasks outside of the hazardous area that had previously required lockout (gauges, valves and lubrication systems moved outside safeguarded area).
3. A review of all machines and equipment with multiple energy sources and those with single energy sources where the energy isolation devices were not conspicuously located.
4. Evaluation to insure that energy isolation devices were capable of being locked out.
5. Posting of identification labels on energy isolation devices.
6. Formulation of machine or equipment-specific lockout procedures and posting of procedures on placards.
7. Training of appropriate personnel.
8. Establishment of periodic audits.

The process led to uncovering major deficiencies, including machinery that could not be locked out, tasks that could not be performed with the machinery locked out and for which alternative safeguards were not available. Professional health and safety oriented approach can be characterized as follows [9]:

1. Hazards are controlled at the source and a hierarchy of controls is applied.
2. Relationship to modern quality control, as advocated by Deming, is suggested to be consistent by emphasizing work on correcting common cause failures (CCF) in the system and recognizing that management has to change the most.
3. Responsibility of management in addressing fundamental system problems is crucial and every part of the business should be mobilized to carry out its role in preventing injuries and illnesses.
4. Hierarchy of controls is implemented that include: elimination or substitution, engineering controls, warnings, procedures and training, and personal protection equipment.
5. Employee involvement by establishing joint health and safety committees. Workers are trained in hazard identification and methods of control. Employees to have input on job/workstation design and opportunity to communicate problems.
6. Ergonomics related methods are applied with emphasis on evaluating current and proposed jobs for risk factors; force, repetition, and posture. The controls, based on the hierarchy (design and engineering), are applied.
7. Evaluation potential chemical exposure by analyzing injury and illness data. Comply with standards and latest research findings. Reducing chemicals and maintaining effective ventilation.
8. An aspect of the management strategy can be noise exposure. Buy quiet machinery and equipment. Apply engineering noise control to sources of noise.
9. Consider where to work more effectively for process improvement. Work upstream on the procurement, design, and modification of processes.

Workers have been assigned to advanced engineering on a full-time basis with sole purpose of making health, safety, and ergonomics improvements upstream at the earliest stages of the design process.

Although worker involvement is important, it has limitations and is not a substitute for technically competent health and safety experts reviewing both existing and future operations to insure that hazards are identified and controlled.

However, workers can provide insight into the tasks that they need to perform and the problems that they encounter, as well as into injuries, illnesses, near-misses that have occurred. This means that the system is analyzed to determine *errors and mistakes* that can occur. Design and engineering modifications should be used especially to prevent the mistakes with serious consequences.

As it has been mentioned, the responsibility of management in addressing fundamental system problems is crucial and every part of the business should be mobilized to carry out its role in preventing injuries and illnesses. A proactive safety management can be implemented in given organization in relation to modern *quality management system*, with defining relevant processes and procedures [14].

2.3. Organizational culture

According to *BusinessDictionary.com* organizational culture is characterized by the values and behaviors that contribute to the unique social and psychological environment of an organization. *Organizational culture* includes the organization's expectations, experiences, philosophy, and values that hold it together, and is expressed in its self-image, inner workings, interactions with the outside world, and future expectations.

Organizational culture is based on shared attitudes, beliefs, customs, and written and unwritten rules that have been developed over time and are considered to be valid. In relevant cases it is also called as *corporate culture* being expressed as follows:

(1) the ways the organization conducts its business, treats its employees, customers, and the wider community;

(2) the extent to which freedom is allowed in decision making, developing new ideas, and personal expression;

(3) how power and information flow up and down through its hierarchy; and

(4) how employees are involved and committed towards collective objectives.

Undoubtedly, this culture affects the organization's productivity and performance, and provides guidelines on customer care and service, product quality and safety, attendance and punctuality, and concern for the environment.

According to Needle [25], *organizational culture* represents the collective values, beliefs and principles of organizational members and is a product of such factors as history, product, market, technology, strategy, type of employees, management style, national culture and tradition. Such culture includes the organization's vision, values, norms, systems, symbols, language, assumptions, beliefs, and habits.

An interesting Denison's model (1990) asserts that organizational culture can be described by four dimensions:

- *Mission* – strategic direction and intent, goals and objectives and vision;
- *Adaptability* – creating change, customer focus and organizational learning;
- *Involvement* – empowerment, team orientation and capability development
- *Consistency* – core values, agreement, coordination and integration

Each of these general dimensions is further described by sub-dimensions. Denison's model allows to describe cultures broadly as *externally* or *internally* focused as well as *flexible* versus *stable*. The model has been typically used to diagnose cultural problems in organizations. It seems that this model can be useful for analysis the safety and security aspects in organization of hazardous industrial plants.

According to Schein (1992) there are two main reasons why cultures develop in organizations, i.e. *external adaptation* and *internal integration*. *External adaptation* reflects an evolutionary approach to organizational culture and suggests that culture develops and persist because they help an organization to survive and be successful, often in unfriendly or unsafe environment.

If the culture is valuable, then it holds the potential for generating sustained competitive advantages. Additionally, *internal integration* is an important function since social structures are required for organizations to exist. Organizational practices are learned through socialization at the workplace. Work environments reinforce culture on a daily basis by encouraging employees to exercise cultural values.

Organizational culture is shaped by a number of factors, including the following:

- Industrial sector;
- External environment;
- Size, nature and competence of the organization's workforce;
- Technologies the organization uses;
- Organization's history and ownership;
- Involvement of the management, staff and personnel in creating and shaping culture in time.

Strong culture exists where staff respond to stimulus because of their alignment to organizational values. In such environments, strong cultures help firms operate effectively, engaging in outstanding execution with only limited adjustments to existing procedures as required.

Conversely, there is *weak culture* where there is little alignment with organizational values, and control must be exercised through extensive bureaucracy and not always justified or poorly developed procedures.

Organisational culture influences:

- Employees involvement and activity that require relevant competences;
- Quality and effectiveness of work and technological processes;

- Risk evaluation of existing or emerging hazards and threats;
- Health and safety of workforce;
- Safety and security of employees and organisation assets;
- Relations with clients, consumers and stakeholders;
- Opening for new domain knowledge for creating or applying innovations;
- Reacting possibly without delay on international and state regulations, and relevant standards;
- Integrated proactive management of implemented processes that include the quality, environmental, economic, safety and security aspects.

Thus, the organizational culture affects the ways people and groups interact with each other, with clients and stakeholders. *Organizational culture* may affect how much employees identify themselves with given organization and it has influence on the *safety and security culture*. The issues of the safety and culture will be discussed later on.

2.4. Evaluation issues of organisation's business and supporting processes

At present there is available at the market an ISRS methodology and supporting software package. First edition of the *International Safety Rating System* (ISRS) [5], available on the market from 1978, was oriented mainly on selected aspects of *occupational health and safety* management. Next editions of this system have been designed with an objective to help in assessing and improve the health of an organization's business and supporting processes. The ISRS was designed to help organizations and their stakeholders to be more convinced that the processes and operations are safe and sustainable.

Organizations are under increasing scrutiny from a growing number of stakeholders [5]. Regulators, customers, employees and society expect using high standards of safety and sustainability. Satisfying these expectations is usually a matter of business survival and is one of the major challenges facing organizations today.

Seventh edition of ISRS was developed in 2005 with identical acronym but a new meaning: *International Sustainability Rating System*. Its scope expanded beyond occupational health and safety management to address on assumption best available practices in a range of issues including *environmental, quality, safety and security management* and sustainability reporting. These changes were made to address the changing needs of organizations and the increasing expectations of their stakeholders.

Eighth edition of ISRS was launched in 2009. Its scope was expanded to help organizations improve process safety management following growing industry concerns over the increasing frequency of major accidents according to requirements of Seveso II Directive. It was due to reasons that many organizations have major hazard processes with the potential for significant accidents e.g. fire, explosion or release of flammable or toxic materials above permissible threshold levels.

Consecutive generations of ISRS have been developed to help organizations in effective risk management by implementing the necessary processes for risk evaluation concerning employees, the community and the business [5]. Many organizations would like to identify the scenarios and related risks associated with specific hazards for occupational health and safety, process safety, environment, security and quality.

Site management would like also to identify the business risks which threaten the survival or reputation of the organization associated with major internal or external events, the loss of major clients, key supply chain partners or key personnel.

Adequate risk controls might be then proposed to be in relevant places including engineering design, rules, procedures, training and protective equipment to meet defined performance standards. Preventing major hazardous events requires checking that the necessary process and plant barriers are in place [5].

Eighth edition of ISRS consists of 15 key processes, embedded as intended in a continual improvement Deming loop. Each process contains sub-processes and questions. An ISRS assessment is a thorough evaluation of these questions and involves interviews with *process owners*/*leaders* where the questions are scored and commented.

Seventh and eighth editions of ISRS are structured with 15 processes embedded in a continuous improvement loop [5]:

1. Leadership
2. Planning and administration
3. Risk evaluation
4. Human resources
5. Compliance assurance
6. Project management
7. Training and competence
8. Communication and promotion
9. Risk control
10. Asset management
11. Contractor management and purchasing
12. Emergency preparedness
13. Learning from events
14. Risk monitoring
15. Results and review.

The scope of the assessment is intended to be flexible, determined by the size and complexity of the organization and the management requirements.

The process scores determine an overall level of performance between one and ten. The results provide a detailed measure of performance and a gap analysis against the organization's desired level of performance. This becomes a basis for planning and improvement during the following period.
In addition, ISRS eighth edition includes the requirements for some international standards to guide organizations in improving their systems to meet certification requirements [5].

- OHSAS 18001:2007 - Health and Safety Management;
- ISO 14001:2004 - Environmental Management;
- ISO 9001:2008 - Quality Management;
- ISO 31000:2009 - Risk Management;
- Global Reporting Initiative 2006 - Sustainability Reporting;
- PAS 55:2004 - Asset Management;
- OSHA 1910.119 - Process Safety Management;
- Seveso II Directive - 96/82/EC - Process Safety Management.

The idea of evaluations and assessments in this system is in principle qualitative based on distinguished categories of attributes of an organisation with assigned scores (from 1 to 10). The ISRS does not consists of more formal models and methods to make quantitative and/or qualitative risk evaluations of the system for necessary risk mitigation of potential hazardous events, e.g. using safety and/or security functions implemented within *industrial control systems* (ICS).

3. Shaping safety and security culture in organizations responsible for plants and systems of critical infrastructure

3.1. Etics in science and safety engineering

Lately, in some papers the selected aspects of safety and ethics are discussed, in particular in the context of the risk informed decision making [1], [19]. Ethics, also known as moral philosophy, is a branch of philosophy that involves systematizing, defending and recommending concepts of right and wrong conduct.
Ethics is divided into four major areas of study:

- *meta-ethics*, about the theoretical meaning and reference of moral propositions and how their truth values (if any) may be determined;
- *normative ethics*, about the practical means of determining a moral course of action;
- *applied ethics*, about how moral outcomes can be achieved in specific situations;
- *descriptive ethics*, also known as comparative ethics, is the study of people's beliefs about morality.

Applied ethics is a discipline of philosophy that attempts to apply ethical theory to real-life situations. The discipline has many specialized fields, such as *engineering ethics*, *bioethics*, *geoethics*, *public service ethics* and *business ethics*.
Engineering ethics is the field of applied ethics and a system of moral principles that apply to the practice of engineering. The field examines and sets the obligations by engineers to society, to their clients, and to the profession. As a scholarly discipline, it is closely related to subjects such as the *philosophy of science*, the *philosophy of engineering*, and the *ethics of technology.*
In times of dynamic changes of technology it has been often emphasized the responsibility of engineers [27]. The majority of engineers recognizes that the greatest merit is the deep knowledge and professional work to serving society for the welfare and progress of the majority. By transforming nature for the benefit of mankind, the engineer must increase his awareness of the world and knowledge of nature and society to make the world more fairer, safer and possibly happier.
There is no doubt that tragic episodes like *Three Mile Island NPP* accident (1979), *Space Shuttle Columbia* disaster (2003), *Bhopal* disaster (1984), *Chernobyl NPP* disaster (1986), *Fukushima NPP* disaster after tsunami (2011) and many other disasters happened not only due to technical causes but first of all because of the organizational inadequacies rooted in forgetting about basic principles of engineering ethics resulting in fatal human errors with serious consequences.
Therefore, the domain engineers should reject any technical and organizational solution within a project that can potentially harm the general interest, thus avoiding a situation that might be hazardous or threatening to the environment, life, health, or other rights of human beings. In many cases it is not realistic to eliminate fully hazards or threats, then the organisation has to mitigate relevant risks, e.g. according to the ALARP (*as low as reasonably practicable*) principle.
Thus, creating organisational culture with regard to principles of healthy competition in business and engineering ethics will enable to shape in time a high safety and security culture. It will obviously contribute to effective business, when supported by modern *integrated management system* (IMS). Within such IMS relevant processes are distinguished that include relevant quality, environment, safety and security aspects and models.

3.2. Challenges in shaping safety and security culture in organizations

As it was mentioned *safety culture* is related to the ways in which safety is managed in the workplace, and often reflects the attitudes, beliefs, perceptions and values that employees share in relation to safety. Slightly modified definition was proposed by the ACSNI (*Advisory Committee on the Safety of Nuclear Installations*): the *safety culture* of an organization as the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organization's health and safety management.

In several reports/guidelines of the IAEA, e.g. INSAG-24 [11] *safety culture* was defined as: *assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance*.

Lately, there was also proposed definition of *nuclear security culture* as *assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security*; *nuclear security culture aims to ensure that the implementation of nuclear security measures receives the attention warranted by their significance* [11], [13].

Nuclear security is understood as the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear or other radioactive substances or their associated facilities.

It should be noted that *nuclear security* includes *physical protection*, as that term is taken from consideration of the *Physical Protection Objectives and Fundamental Principles*, the *Convention on the Physical Protection of Nuclear Material* (CPPNM), and the Amendment to the CPPNM.

In March 2005, the IAEA international conference on Nuclear Security: Global Directions for the Future, held in London, recognized that the risk of successful malicious attacks remains high and stated: *The fundamental principles of nuclear security include embedding a nuclear security culture throughout the organizations involved.* By the coherent implementation of a nuclear security culture, staff remain vigilant of the need to maintain a high level of security.

There are various safety and security aspects to be considered during design and operation of hazardous plants. An important aspect is associated with the safety and security related functions, implemented using the *information technology* (IT) [13] and the control and protection systems that are designed and operated according to functional safety requirements [18], [19]. It will be discussed later on.

Controlling access to sensitive information is a vital part of the security function. Accordingly, the organization must implement classification and control measures for protecting sensitive information. The security culture indicators for information security are as follows [11], [13]:

- classification and control requirements are clearly documented and well understood by staff;
- clear and effective processes and protocols exist for classifying and handling information both inside and outside the organization;
- classified information is securely segregated, stored and managed;
- staff members are aware of and understand the importance of the controls on information;
- cyber systems are maintained to ensure that they are secure, that they are accredited by an appropriate authority and are operated in accordance with procedures.

In latest publications there is clear-cut indication of the necessity to integrate the safety and security aspects for safety management of nuclear power plant in life cycle [13], [14]. Both safety and security should be built on a legal and regulatory framework. That framework should define the responsibilities of key organizations: the State, the regulatory authority or authorities, and the operating organizations. The general features of nuclear safety and security culture are presented in *Figure 1*.

Figure 1. General features of nuclear safety and security culture (based on [11])

The operating organization has the prime responsibility for the safety and security of the nuclear power plant, although in the case of security, the operator's responsibility may be limited to defence against a design basis threat.
This allocation of responsibility reflects the reality that operating staff are in the best position to identify the risks arising at the nuclear power plant (NPP) and to ensure compliance with regulatory requirements. In this context, the operators must [11]:

- design, implement and maintain technical solutions and other arrangements to satisfy regulatory requirements related to both safety and security;
- ensure first level control;
- verify the skills and appropriate training of personnel;
- inform the regulatory authorities of any event likely to affect the safety or security of the NPP and, as appropriate, request support;
- maintain coordination with State organizations that are involved in safety or security; and
- implement a *quality assurance system* in both the safety and security fields.

Operators should have a centralized information system and a centralized command centre for directing operations during a safety or security related event.
As it was described the functional safety solutions contribute significantly to the safety and security of hazardous plants, in particular nuclear power plants, providing vital functions for the control, protection and monitoring, especially in abnormal and accident conditions. Thus their designing and operating should include both safety and security aspects.

3.3. Interface between safety and security

Site security programs include physical security and cyber security. The purpose of establishing and maintaining an effective interface between safety and security at a facility is to ensure that potential adverse effects from implementation of changes to safety and security measures are considered and addressed prior to implementation [10]-[11], [26].
The interface between safety and security is an important element of both programs relative to ensuring public health and safety. The licensee should address plant activities that could compete or conflict with the capability of the site security program to provide high assurance of adequate protection of the common defense and security [11].
Conversely, changes in the site security program could also adversely affect plant operations; safety-related structures, systems, and components; operator actions; or emergency responses necessary to prevent or mitigate postulated design-basis accidents and to protect public health and safety and the environment.
The proliferation of digital technology must be considered and addressed when changes are made to safety systems, because the safety system components which previously contained no digital equipment are becoming increasingly digital. Also, as cyber security measures are put in place, impacts to safety analyses must be considered and addressed.

3.4. Safety and security in ports

The primary aim of maritime security assessment models is to assess the level of security within and across the maritime network [8], [26], [29]. According to international and state regulators and programmes the owners and operators of certain maritime facilities are required to conduct assessments of security vulnerabilities, develop security plans to mitigate these vulnerabilities. It is especially important for ports.
Ports are typically characterized by asymmetrical activities dispersed over a large area of land and water so that they can simultaneously accommodate ship, truck and rail traffic, petroleum product/liquid offload, storage or piping, or container storage.
Unfortunately, ports and shipping remain attractive targets not only for criminals and organized crime, but also for terrorists. They understand the fact that a strike on a large port facility could cripple a nation's economy, significantly impact world stock markets and cause significant casualties and potential long-term environmental damage.
No simple security countermeasure such as the *container security initiative* (CSI) or the terrorist watch list, can adequately address port or maritime security and safety concerns. Technology alone cannot secure ports and shipping, nor can adding additional security procedures, physical barriers, or additional manpower fully mitigate the risk [26].
What will work more effectively is an integrated, carefully planned approach that incorporates the best elements of technical, physical, organizational, procedural and information security domains into a comprehensive strategy [29].
Control and monitoring of the port processes can be effected using modern systems such as a *dedicated control console* (DCC) or a *remote control terminal* (RCT). Such systems incorporates intelligent video, radar, sonar, and audio technologies as well as redundant Programmable Logic Controllers (PLCs), and Safety PLCs [8]. The system can be designed and installed that automatically detects intruders and suspicious objects left behind (or removed) within a user defined video security zone.

Careful considering safety and security aspects is especially important in case of the oil port installations where the remote monitoring and control functions are extensively used. Such functions are implemented in the DCS *(distributed control system*) with relevant SCADA (*supervisory control and data acquisition*) software supporting of human operators. In addition various protection systems are in operation that mitigate risks of major accidents. For such systems both safety and security aspects should be evaluated and managed in life cycle [21].

3.5. Advantages of integrated approach

An integrated approach ensures that the solutions for safety do not adversely affect the effectiveness of the delivery of security and vice versa. Some typical issues and the advantages that integrated experience of organizations include [10]:

(1) Research & Development (R&D) − when research concerning new technology or processes focuses only on safety and ignores potential security implications − introducing security considerations into R&D can identify potential vulnerabilities.

(2) Conceptual design − when an organisation evaluates technology options for business without considering security vulnerabilities − integrating security and safety can contribute to optimizing the technology selection process at the outset and avoid expensive changes later.

(3) Design − an organization locates safety-related plants or equipment without considering their vulnerability to terrorist attack − when security and safety teams work together, facilities can be designed that deliver both safety and security.

(4) Operations − because plant malfunctions and maintenance requirements reduce overall safety and security protective barriers, leading to inadvertent reductions in safety and/or security margins − a co-ordinated approach to safety and security management enables both safety and security departments to take rational actions.

(5) Operations − plant potential malfunctions and maintenance requirements reduce overall safety and security protective barriers, leading to inadvertent reductions in safety and/or security margins − a co-ordinated approach to safety and security management enables both safety and security departments to take rational actions.

More details concerning integrated approach to safety and security in nuclear energy sector are described in a guide [10]. In this guide following five levels of safety and security integration are proposed:

Level 1 − an organization has no integration or communication between its safety and security departments; its safety team is not aware of security arrangements, and its security team does not understand plant safety; as a result, there is a serious risk that decisions will be taken in one area that adversely affect the other area.

Level 2 − an organization whose safety and security departments are not integrated; however, limited communication does take place between safety and security professionals regarding the importance of vital area protection. Due to lack of coordination, however, the organization may suffer from business risks.

Level 3 − an organization that clearly understands how security impacts safety. It recognizes that lack of co-ordination between its safety and security departments poses important business risks, but it has made inadequate arrangements to manage such risks.

Level 4 − an organization has integrated its safety and security management systems, and professionals from both departments work together to manage business risk.

Level 5 − organization has integrated its safety and security management system. The entire staff not only recognize this, but also know that the company considers integration to be a core value because it minimizes risk to the company and society.

By identifying where given organization falls, it will be known what should be done to improve the integration of safety and security aspects.

4. Examples of issues for considering in proactive safety and security management

4.1. General principles of proactive safety and security management

Due to complexity of the risk evaluation and management in industrial hazardous plants, to overcome difficulties in safety-related decision making, it has been proposed to apply in nuclear industry an approach known as the *Risk Informed Decision Making* (RIDM) [2], [12]. The purpose was to enable the safety-related decision making in a more systematic and transparent way, often under significant uncertainties.

In the publications [25], [26] an idea was proposed to update this approach for dealing more systematically with the functional safety analysis of programmable control and protection systems described in standards IEC 61508 [15] and IEC 61511 [16]. These systems contribute nowadays substantially to the risk mitigation of potential accidents. However, due to new hazards, it was necessary to tackle some additional aspects including security related issues, and more systematic treating the human and organizational factors.

General principles concerning the safety and security management system (S&S MS) in hazardous plants, in life cycle, are shown in *Figure 2*.

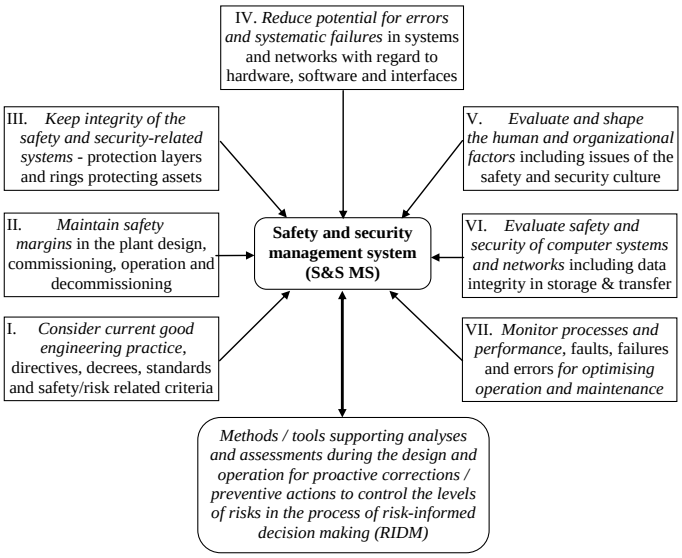

Figure 2. General principles for adopting within the integrated safety and security management system

Following general principles, which are common to most industrial hazardous plants, have been distinguished:

Principle I: *Consider and implement current good engineering practice*,

Principle II: *Maintain safety margins*,

Principle III: *Keep integrity of the safety and security-related systems*,

Principle IV: *Reduce potential for errors and systematic failures*,

Principle V: *Evaluate and shape the human and organizational factors*,

Principle VI: *Evaluate safety and security of computer systems and networks*,

Principle VII: *Monitor relevant processes and performance for optimising business, operation, maintenance to protect environment and mitigate safety and security related risks*.

These principles should be incorporated in decision making processes by applying relevant methods and tools for supporting analyses and assessments during the design and operation for *proactive corrections and preventive actions* to control relevant risks.

The problem is that these requirements and methods require integration, and due to complexity of the problem, using a *knowledge-based framework* was proposed [20]. To handle complex systemic safety and security aspects it is proposed to define relevant processes according to ideas of quality management within integrated management system of given organisation [14].

4.2. Example of knowledge based systemic functional safety and security management

Proposed framework for knowledge-based functional safety and security management is shown in *Figure 3*. In the centre of this figure a block of "S*ystemic functional safety and security management* in given hazardous process installation/plant" is situated. On the left side a block "*Knowledge-based safety and security* management in hazardous process plants in life cycle" was placed.

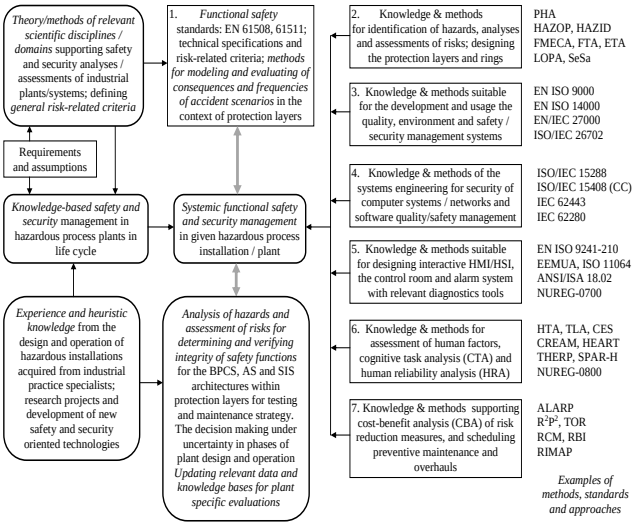

Figure 3. Scope of knowledge-based systemic functional safety and security management

The framework includes knowledge and methods (a block above) of relevant scientific domains (mathematics, informatics, computer science, control engineering, reliability, ergonomics, economics, management, etc.) supporting integrated safety and security analyses and assessments with regard to risk-related criteria.

The experience and heuristic knowledge (a block below) are useful to create elements of consensus knowledge that consist of principles, rules and methods of *good engineering practice*, also those included in relevant international standards.

Seven categories of domain knowledge, methods and data for supporting the functional safety analysis and management in the design and operation of hazardous installations have been distinguished in *Figure 2*. On the right side of this figure the blocks numbered from 2 to 7 selected examples of information sources, including relevant standards, methods and approaches of interest, are specified. Consecutive blocks and information sources have been characterised in details in publication [20].

Knowledge is understood here widely as a familiarity, awareness or understanding of facts, information, descriptions, or skills, which are

acquired through education and experience by perceiving, discovering, learning or training. Knowledge can refer to the theoretical or practical understanding of a subject, as well as appreciated information sources, e.g. standard [17], guidelines [4], [22], [24], and publication [23].

These methods, standards and reports form knowledge base (KB) support integrated *systemic functional safety and security management* of the control and protection systems of hazardous plants, ports and systems of critical infrastructure (CI).

Several procedures have been developed and some are still under development regarding requirements of international standards [15]-[16], how to integrate the KB facts and methods effectively for distinguished categories hazardous plants, ports and systems of CI. These procedures have been designed to be useful within defined process based integrated management system. General idea of such system was outlined in a relatively new publication of the IAEA [14].

5. Conclusions

Selected aspects of the behavioral based safety (BBS), organizational culture, safety culture and security culture have been considered in the context of knowledge based, integrated proactive safety and security management of plants, ports and other complex systems of critical infrastructure.

Although the BBS process can be considered to some extent as reactive approach, it can be useful for solving practical safety at work problems.

It has been emphasized that business effectiveness, safety and security related systems, and their resilience against hazards and threats to avoid abnormal events and accidents depends substantially on various factors relevant to mentioned cultures.

Current topic that requires further research includes the interface between safety and security. The article discusses these issues on example of knowledge based proactive functional safety and security management system.

References

[1] Berg, H. P. (2011). *Safety Culture*. Summer Safety & Reliability Seminars, SSARS 2011, Educational & Training Course, Gdańsk–Sopot.

[2] Berg, H. P. (2013). *Considerations on Applying the Risk-Informed Decision Making Process to Security Issues*. Summer Safety & Reliability Seminars. SSARS 2013, Educational & Training Course, Gdańsk–Sopot.

[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] CCPS (2008). *Guidelines for Hazard Evaluation Procedures*. New York: Center for Chemical Process Safety. Wiley-Interscience, A John Wiley & Sons.

[5] DNV (2014). *ISRS for the health of your business*. DNV GL - Business Assurance. Ravello, Katy.

[6] DOE-HDBK (2002). *Behavior Based Safety Process, vol. 1: Summary of Behavior Based Safety*. U.S. Department of Energy, Washington, D.C.

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

[8] Goslin, Ch. (2008). *Maritime and port security*. Duos Technologies, Inc., Jacksonville.

[9] Howe, J. (2001). *A Union Critique of Behavior-Based Safety*. International Union, UAW Health and Safety Department, Detroit.

[10] Howsley, R. (2011). *An Integrated Approach to Nuclear Safety and Nuclear Security*. World Institute for Nuclear Security (WINS), Vienna.

[11] IAEA INSAG-24 (2010). *The Interface Between Safety and Security at Nuclear Power Plants. A report by the International Nuclear Safety Group*. International Atomic Energy Agency, Vienna.

[12] IAEA INSAG-25 (2011). *A Framework for an Integrated Risk Informed Decision Making Process. A report by the International Nuclear Safety Group*. International Atomic Energy Agency, Vienna.

[13] IAEA (2011). *Nuclear Security Series No 17: Computer Security at Nuclear Facilities. Technical Guidance / Reference Manual*. International Atomic Energy Agency, Vienna.

[14] IAEA (2015). *Development and implementation of a process based management system. Nuclear Energy Series Report NG-T-1.3*. International Atomic Energy Agency, Vienna.

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

[16] IEC 61511 (2014). *Functional safety: Safety Instrumented Systems for the process industry sector. Parts 1–3*. Geneva: International Electrotechnical Commission.

[17] ISO 31000 (2009). *Risk management - Principles and guidelines*. International Organization for Standardization, Geneva.

[18] Kosmowski, K. T. (Ed.) (2007). *Functional Safety Management in Critical Systems*. Gdansk University of Technology. Publishing House Of Gdansk University.
[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] Kosmowski, K. T., Śliwiński, M. & Piesik, E. (2015). Integrated safety and security analysis of hazardous plants and systems of critical infrastructure. *Journal of Polish Safety and Reliability Association*. 6, 2, 31-45.
[22] LOPA (2001). *Layer of Protection Analysis, Simplified Process Risk Assessment. Center for Chemical Process Safety*. American Institute of Chemical Engineers, New York.
[23] Lu, T. et al. (2015). Towards a Framework for Assuring Cyber Physical System Security. *International Journal of Security and Its Applications*. 9, 3, 25-40.
[24] Mahan, R. E. et al. (2011). *Secure Data Transfer Guidance for Industrial Control and SCADA Systems*. PNNL-20776, Pacific Northwest National Laboratory, Richland.
[25] Needle, D. (2004). *Business in Context: An Introduction to Business and Its Environment*. South Western Educational Publishing, Mason.
[26] NRC (2015). *Managing the Safety / Security Interface. Regulatory Guide 5.74*. U.S. Nuclear Regulatory Commission.
[27] Rasmussen, J. & Svedung, I. (2000). *Proactive Risk Management in a Dynamic Society*. Swedish Rescue Services Agency, Karlstad.
[28] Reason, J. (1990). *Human Error*. Cambridge University Press.
[29] UN (2006). *Maritime security: elements of an analytical framework for compliance measurement and risk assessment*. United Nations, New York and Geneva.