Gołębiewski Dariusz
PZU Group, Warsaw, Poland

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

Towards a process based management system for oil port infrastructure in context of insurance

Keywords

process based management system, business continuity management, risk evaluation, oil port infrastructure, insurance, key performance indicators

Abstract

This article addresses selected methodological aspects of a *process based management system* based on analysis of hazards and threats and risk evaluation for an oil port infrastructure in context of insurance. The oil port terminal is regarded as important system of the critical infrastructure that require careful system oriented approach to deal with integrated aspects of environmental, safety and security management to reduce risk of potential consequences of abnormalities and accidents, especially major accidents with catastrophic consequences. The risk of potential economic losses should be also minimised applying in practice an effective *business continuity management* system. Careful evaluations of relevant risks carried out for the oil port infrastructure are crucial also for the insurance company. Some requirements and activities of the risk engineer and the underwriter in the insurance process are outlined including important factors influencing risks. It is emphasised that determining and evaluating a set of *key performance indicators* based on data from site audits and analyses can be useful for the safety management of the oil port and its insurance.

1. Introduction

The oil ports play an important role in the energy sector economy and *Critical Infrastructure* (CI) of the country. In the *management system* (MS) of oil port infrastructure relevant existing safety and security-related recommendations and requirements have to be considered [11], [14], [36], [37].

Also important aspects of business continuity management should be taken into account to propose effective economic technical and organisational solutions. However, due to uncertainty involved the decision making in life cycle, relevant management processes should be based on evaluations of risks to be reduced and controlled in time [2], [30]. An integrated *process safety management* (PSM) methodology is of particular interest [22], [31].

This article addresses selected methodological aspects of a *process based management system* (PBMS) based on analysis of hazards and threats and risk evaluation for an oil port infrastructure in context of insurance. It is known that the information gathered during the insurance audit can be useful in either of safety and security management of maritime infrastructure, in particular the oil port terminals.

General idea of the PBMS is outlined. The aim of such approach is to ensure that requirements for safety are not considered separately but put in the context of all the other requirements, for example those for security, safeguards, environment, personal safety and economy. It will also require that the management system reflect the processes established in the organization to ensure safety [15], [16], [22], [23]. In the PBMS a PDCA (*Plan-Do-Check-Act*) model according to a Deming concept, adapted in quality management standard ISO 9001 [23], is proposed to be applied.

The insurance auditors visit the organisation and installations, identify the hazards and threats, and

specify more important factors influencing risks. The insurance audit results are then to be analysed by an underwriter to evaluate whether to issue an insurance policy and at what cost to be paid as an insurance premium. In the insurance policy some additional statements (terms) are usually specified concerning conditions and limitations of the insurance of given company.
Some requirements and activities of the *risk engineer* and the *underwriter* in the insurance related processes are outlined including important factors influencing risks. It is emphasised that determining and evaluating a set of *key performance indicators* (KPIs) based on data from site audits and further evaluations can be useful for the safety management of the oil port and its insurance.

2. Concepts and challenges in safety, security and business continuity management

2.1. General requirements for risk evaluation and management

Today organizations face various problems due to internal and external influences that make them uncertain to achieve business and operation related objectives. The effect of uncertainty on these objectives is popularly understood as risk [26]. Almost all activities of an organization involve risk. Thus, the organizations should manage the risk by identifying and evaluating it in order to meet certain acceptance criteria.
Risk management can be applied to the entire organization, at its distinguished levels and areas, and to specific projects and activities, processes and functions. Establishing context of risk management requires considering the environment in which the objectives are to be achieved, opinions of stakeholders and relevant risk criteria. It should help to reveal and assess the nature of hazards and threats that can cause damages.
Objectives can be related to different aspects, such as financial, health and safety of employees, technological safety, and environmental safety goals etc. They can be formulated for different organization's levels, such as strategic, organization-wide, project, and defined processes in realization of operation tasks and products.
The *risk management process* includes systematic application of management policies, procedures and good practices to the coordinated activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risks to direct and control an organization regarding elaborated objectives, however often in conditions of significant uncertainty [26]. *Uncertainty* is understood here as the state of deficiency of information related to knowledge about an event of interest (e.g. accident scenario) in evaluating its consequence and/or likelihood (frequency).
As it is known several sources of uncertainty may exist and it is worth to mention about the distinction between *epistemic uncertainty* and *aleatory uncertainty*, because it is essential for careful risk assessment to provide honest support for safety-related decision making [30]. Uncertainties are characterized as *epistemic*, if the modeller sees a possibility to reduce them by gathering more data or by refining models (assuming randomness of repeatable phenomena). Uncertainties are categorized as *aleatory* if the modeller does not foresee the possibility of reducing them, because knowledge about considered issues is not sufficient at present.
Risk management process is illustrated in *Figure1*. *Risk assessment* is defined as overall process of hazards and/or threats identification, preliminary ranking of specific risks (during risk identification), risk analysis and risk evaluation regarding the risk criteria [26]. Risk identification process aims at finding, recognizing and describing risk sources, and hazardous events with their causes and consequences. Risk identification can involve historical data, theoretical analysis, and expert opinions regarding emerging risks, and stakeholder's needs.

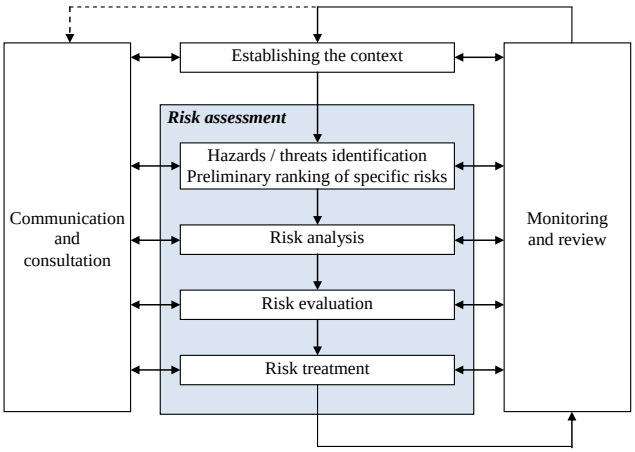

Figure 1. Risk management process (based on [26])

Risk criteria are defined as terms of reference against which the significance of a risk is evaluated. Risk criteria are based on organizational objectives, and external and internal context. Risk criteria can be derived from standards, laws, policies, expert opinions and other requirements if available.
Following principles have been formulated for the *risk management* (RM) to be successfully applied at relevant organization's levels, because the RM [26]:
a) creates and protects values,
b) is an integral part of organizational processes,

c) is part of conscious decision making in solving complex problems,
d) explicitly addresses uncertainty issue,
e) is systematic, structured and timely,
f) is based on the best available information,
g) is tailored but taking into account important external influences,
h) takes human and cultural factors into account,
i) is transparent and inclusive,
j) is dynamic, iterative and responsive to internal and external changes,
k) facilitates continual improvement of the organization.

The outlined above risk management approach should be fully integrated with the organization's governance structure, regarding requirements of the quality management system based on defined *processes* and *procedures* [23], [26].

2.2. Process safety management

The publication [22] summarizes the OSHA 3132 final *process safety management* (PSM) standard. The standard applies mainly to manufacturing industries particularly, those pertaining to chemicals and transportation equipment.

The key provision of PSM is *process hazard analysis* (PHA), i.e. a careful review of what could go wrong and what safeguards must be implemented to prevent releases of hazardous chemicals. Covered employers have to identify those processes that pose the greatest risks and begin evaluating those first.

PSM clarifies the responsibilities of employers and contractors involved in work that affects or takes place near covered processes to ensure that the safety of both plant and contractor employees is considered.

The standard also mandates written operating procedures, employee training, prestartup safety reviews, evaluation of mechanical integrity of critical equipment, and written procedures for managing change.

In addition PSM specifies a permit system for hot work, investigation of incidents involving releases or near misses of covered chemicals, emergency, action plans, compliance audits at least every three years, and trade secret protection.

To understand PSM and its requirements, employers and employees need to understand how OSHA uses the term “process” in PSM. Process means any activity involving a hazardous chemical including using, storing, manufacturing, handling, or moving such chemicals at the site, or any combination of these activities.

Process safety information must include information on the hazards of the highly hazardous chemicals used or produced by the process, information on the technology of the process, and information on the equipment in the process.

Information on the technology of the process must include at least the following [22]:

- A block flow diagram or simplified process flow diagram,
- Process chemistry,
- Maximum intended inventory,
- Safe upper and lower limits for such items as temperatures, pressures, flows or compositions,
- Evaluation of the consequences of deviations, including those affecting the safety and health of employees.

Where the original technical information does not exist, such information may be developed in conjunction with the process hazard analysis in sufficient detail to support the analysis. Information on the equipment in the process must include the following [22]:

- Materials of construction,
- Piping and instrument diagrams (P&IDs),
- Electrical classification,
- Relief system design and design basis,
- Ventilation system design,
- Design codes and standards employed,
- Material and energy balances for processes, and
- Safety systems (e.g., interlocks, detection, or suppression systems) and their functions.

The employer must develop and implement written operating procedures, consistent with the process safety information, that provide clear instructions for safely conducting activities involved in each covered process. OSHA believes that tasks and procedures related to the covered process must be appropriate, clear, consistent, and most importantly, well communicated to employees.

The procedures must address at least the following elements for each operating phase [22]:

- Initial start-up;
- Normal operations;
- Temporary operations;
- Emergency shutdown, including the conditions under which emergency shutdown is required, and the assignment of shut down responsibility to qualified operators to ensure that emergency shutdown is executed in a safe and timely manner;
- Emergency operations;
- Normal shutdown; and
- Start-up following a turnaround, or after an emergency shutdown.

To ensure that a ready and up-to-date reference is available, and to form a foundation for needed employee training, operating procedures must be readily accessible to employees who work in or maintain a process.

The operating procedures must be reviewed as often as necessary to ensure that they reflect current operating practices, including changes in process chemicals, technology, and equipment, and facilities. To guard against outdated or inaccurate operating procedures, the employer must certify annually that these operating procedures are current and accurate, and developed with regard verified rules.
OSHA 3132 emphasises that it is important to maintain the mechanical integrity of critical process equipment to ensure it is designed and installed correctly and operates properly. The PSM mechanical integrity requirements apply to the following equipment [22]:

- Pressure vessels and storage tanks;
- Piping systems (including piping components such as valves);
- Relief and vent systems and devices;
- Emergency shutdown systems;
- Controls (including monitoring devices and sensors, alarms, and interlocks); and
- Pumps.

The employer has to establish and implement written procedures to maintain the ongoing integrity of process equipment. Employees involved in maintaining the ongoing integrity of process equipment must be trained in an overview of that process and its hazards and trained in the procedures applicable to the employees's job tasks.
To be certain process safety management is effective, employers must certify that they have evaluated compliance with the provisions of PSM at least every three years This will verify that the procedures and practices developed under the standard are adequate and are being followed.
The compliance audit must be conducted by at least one person knowledgeable in the process and a report of the findings of the audit must be developed and documented noting deficiencies that have been corrected. The two most recent compliance audit reports must be kept on file.

2.3. Business continuity management

Nowadays one of the most important issue in industrial practice is to provide the *business continuity management* (BCM). Basic requirements for setting up an effective *business continuity management system* (BCMS) are specified in international standard ISO 22301 [25].
Business continuity (BC) is defined as a strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level
BCM is holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
An important part of BCM is risk assessment and management. *Risk assessment* is overall process of risk identification, analysis and evaluation. *Risk management* includes structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling responding to risk.
Risk appetite is defined as a total amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time.
BCM is a business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that can be characterised as follows [25]:

- proactively improves an organization's resilience against the disruption of its ability to achieve its key objectives;
- provides a rehearsed method of restoring an organization's ability to supply its key products and services to an agreed level within an agreed time after a disruption; and
- delivers a proven capability to manage a business disruption and protect the organization's reputation and brand.

While the individual processes of business continuity can change with an organization's size, structures and responsibilities, the basic principles remain exactly the same for voluntary, private or public sector organizations, regardless of their size, scope or complexity.
The BCMS should be a part of the overall *management system* (MS) that establishes, implements, operates, monitors, reviews, maintain and improves in time business continuity [25]. Such overall MS includes organisational structure, policies, planning activities, responsibilities, processes, procedures and resources as it has been specified in the standard ISO 9001 [23].
According to requirements given in ISO 22301 the organisation shall establish, implement, and maintain formally documented the *risk assessment process* that systematically identifies, analyses, and evaluates the risk of potential disruptive incidents in the organization. It is suggested to made this assessment in accordance with ISO 31000, characterized above. An organisation should [25], [26]:

1) identify risks of disruption to the organisation's prioritized activities and the processes, systems, information, people, assets, outsource partners and other resources that support them,
2) systematically analyse related risks,
3) evaluate which disruption related risks require treatment,
4) identify treatments commensurate with *business continuity objectives* regarding the organisation's *risk appetite*.

The organisation should be aware that certain financial or governmental obligations require the communication of relevant risks at varying levels of details. The organisation should also conduct evaluations of its business continuity procedures and capabilities in order to ensure their continuing suitability, adequacy and effectiveness. These evaluations are expected to be undertaken through periodic reviews, exercising, testing, post-incident reporting and performance analyses. Significant changes arising should be reflected in the procedure(s) in a timely manner [25].

The ISO 22301 adopts the PDCA (Plan-Do-Check-Act) model for planning, establishing, implementing, monitoring, reviewing, maintaining, and continually improving in life cycle the effectiveness of BCMS within an organisation. This ensures a certain level of consistency with other management systems standards of series: ISO 9000 (*Quality management systems*), ISO 14000 (*Environmental management systems*), ISO/IEC 27000 (*Information security management)*, and ISO 28000 (*Specification for security management systems for the supply chain*), to support consistent and integrated implementation and operation with mentioned management systems.

3. Towards process based management system for oil port infrastructure

3.1. Risk sources and risk management

Organizations are exposed to many sources of risk, which might be characterized into four broad categories:

I. Safety and security related,
II. Production / operations,
III. Commercial / financial, and
IV. Strategic.

For each issue or potential event requiring a decision, managers can benefit from adopting a systematic approach to identifying the potential risks, looking specifically at the sector in which the proposal falls, but also looking at the intersection with the other sectors. The idea is to try to identify all of the consequences of a particular issue or potential event, in order to find an optimal decision set to minimize adverse effects and maximize social and business objectives in a cost efficient manner.

Four following steps of a risk management framework providing a systematic approach are to be proposed [15]:

1. Identify hazards/threats and evaluate risks to specify:
   - *List*
   - *Measure*
   - *Rank*
2. Identify techniques / strategies to manage risks:
   - *Reduction of risk,*
   - *Retention of risk,*
   - *Transfer of risk.*
3. Implement risk management strategies.
4. Monitor effectiveness of solutions.

In step 2 often a combination of tools, techniques, and strategies have been used, rather than a single approach. The development team and senior management should be aware of the attendant risks and maintain a prioritized risk register specifying the risks, their likelihood, their impact on the project and the measures the organization will take to mitigate the risks.

Some risks and related challenges will stem from the cultural issues associated with any organizational change [15], [39]. Thus, the implementation of a process based management system requires a shift in thinking and organizational culture.

3.2. Major premise for developing process based management systems

An interesting proposal was recently published concerning development and implementation of a *process based management* (PBM) *system* for nuclear energy installations [16]. Some opinions have been expressed that a process based management system enhances traditional quality programmes, and, when properly implemented, enables the organization to satisfy external agencies and registrars for certification of management systems such as ISO 9001 [23], ISO 14001 [24], OHSAS 18001, and regulatory acceptance of security related standards [27], [28].

The PBM also ensures knowledge retention and the retention of all important aspects of existing programmes. As part of implementation, and to facilitate the same, organizations can develop maps, descriptions and other documents demonstrating how the certified *quality assurance* (QA) and *quality management* (QM) programmes have been addressed in the process based management system documents.

There are several steps to be undertaken within an organization to make the transition from QA/QM oriented system to a process management system that will include conventionally formulated requirements [16]:

- Assessing major differences and similarities between QA/QM systems and other existing management systems integrating the objectives of an organization;
- Setting policies, goals and objectives and preparing the organization to implement a PBM system;
- Developing strategies and options, and engaging stakeholders;
- Developing detailed plans for implementation;
- Making the transition;
- Assessing the effectiveness of implementation and continually improving.

These will require coordinated activities of experienced specialists to establish and implement an effective *Process based management system* (PBMS), especially for those who directs, controls and assesses the licensed organization at the highest level. General idea as illustrated in *Figure 2*. The aim is to ensure that requirements for safety are not considered separately but put in the context of all the other requirements, for example those for security, safeguards, environment, personal safety and economy. It will also require that the management system reflect the processes established in the organization to ensure safety [15], [16], [22], [23].

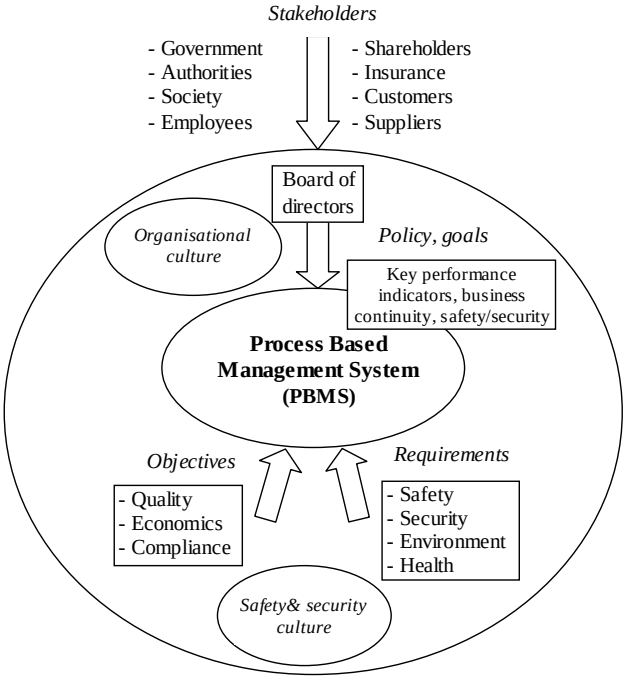

Figure 2. Conditions and sources of requirements influencing a process based management system

In the *process based management system* (PBMS) a PDCA (*Plan-Do-Check-Act*) model according to a Deming concept (adapted in quality management standard ISO 9001 [23]) is applied that includes four elements to be repeated in circle:

- ***Plan*** - establish vision, mission, values, goals and objectives, policy statements, business continuity policy, targets, controls, processes and procedures relevant to improve the *performance key indicators* (KPIs), *business continuity* (BC), and safety and security in order to deliver results that align with the organization's overall policies and objectives.
- ***Do*** - implement and operate the plan elaborated to implement the business continuity strategy and the safety and security objectives, and in relation to developed processes, procedures and controls.
- ***Check*** - monitor and review performance against policies and objectives, report the results to management for review, and determine and authorize actions for improvement, review results of internal audits or independent assessments.
- ***Act*** - maintain and improve the management system by taking corrective actions, based on the results of management review and reappraising the scope of safety and security, and business continuity policy and objectives with regard to *key performance indicators* (KPIs) of interest in given organization.

3.3. Proposals of processes and procedures for a management system

A hierarchy of decisions, information flow, documents and activities in a process based management system is presented in *Figure 3*. The strategic decisions concerning given organization are made at level 1 taking into account opinions of various stakeholders (see *Figure 2*) and are transferred to lower levels of hierarchy.

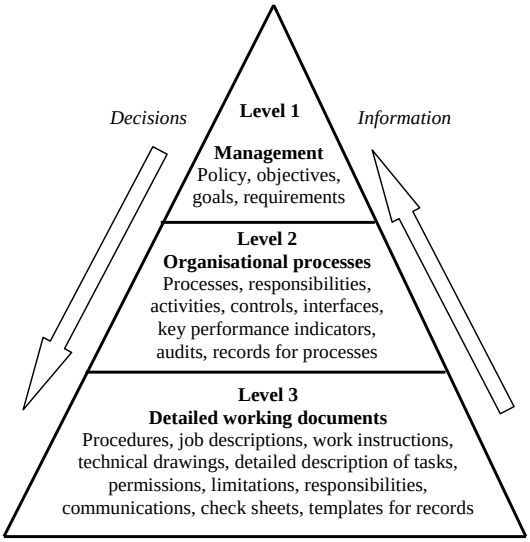

Figure 3. A hierarchy of decisions, information flow, documents and activities in a process based management system

At level 1 generic recommendations and specific requirements are considered for making strategic and tactic decisions concerning mission, policy, goals for organisation. In particular, the safety and security recommendations concerning the oil port terminals and maritime infrastructure are analysed including the international conventions SOLAS [38] and MARPOL [34], and a guide ISGOTT [21]. In Poland a decree of Economy Minister concerning requirements for the oil bases and terminals [7] with relevant amendments are of special interest.
The IMO issued also a convention STCW [39] on standards of training, certification and watchkeeping for seafarers. These general documents are useful not only when internal management policy and requirements are formulated, but also to assess the situation during periodic audits of particular oil port according general requirements of international standards concerning the quality management system ISO 9001 [23] and environmental management system ISO 14001 [24].
At level 2 the organizational processes and relevant procedures are placed, and other elements, e.g. activities related to shaping the key performance indicators (KPIs) [3]. According to rules of the quality management standard for each process the owner (responsible specialist) has to be assigned [15], [23].
The main objective to implement the PBMS in an oil port, preferably with regard to opinions of regulatory body and other stakeholders specified in *Figure 2* (e.g. insurance company), is to assure satisfactory level of business effectiveness thanks to an advanced and effective BCM system with periodic evaluation of KPIs including health, environment, safety and security aspects.

It requires careful identification of hazards / threats, evaluate related risks as well as elaborate strategies and tactics to be implemented in time cycle using relevant processes and procedures to reduce long term risks. Three categories of processes can be distinguished in an organization [16], [23]:

- *Executive Processes,*
- *Core Processes,*
- *Support Processes.*

The process oriented model developed by the oil port management staff can differ as regards some processes and procedures elaborated from the model postulated by stakeholders, e.g. regulatory body or insurance company. It requires further research to work out the consensus models for implementing in practice in given sector taking into account its experience, new requirements and changing in time contents of international standards mentioned before. A leading role in this respect will presumably play the international standard of the ISO 9000 series.
Below some examples of business, safety and security related processes and procedures are specified for further development to be implemented as an advanced oil port management system:

Executive Processes (EP:)
EP1 Managing the organization and business continuity,
EP2 Managing the processes and procedures,
EP3 Evaluating in time and improving KPIs,
EP4 Coordinating external relations including stakeholders, etc,

Core Processes (CP):
CP1 Monitoring operation of installations, equipment and infrastructure,
CP2 Scheduling services, tests and establishing maintenance programs,
CP3 Monitoring environmental conditions, emissions and effluents,
CP4 Managing operation and assessing safety and vulnerability of installations, and site physical security,
CP5 Managing security of organization's computer system and network,
CP6 Evaluating functional safety and security of industrial automation and control systems, etc,

Support Processes (SP)*:*
SP1 Providing human resources and training,
SP2 Providing personnel occupational health and safety services,
SP3 Providing IT services and updating software and protection equipment,
SP4 Providing procurement and contracting,

SP5 Providing environmental and emergency services, etc.

Taking into account current needs and challenges in area of safety and security management of the oil ports following *procedures* (PR) are of interest to be useful in practical realization of relevant processes (given in parentheses):

PR1 Evaluation of indicators, factors and risks relevant to BCM and shaping KPIs (EP1, EP3),
PR2 Evaluation of overfill and leak related risks of terminal tanks (CP1, CP3, CP6),
PR3 Evaluation of individual, group/social and operational risks for oil port terminal (CP2, CP4, CP6, SP2),
PR4 Evaluation long distance piping operational risks (CP5, CP6),
PR5 Evaluation of functional safety in life cycle of the control and protection systems for planning tests and maintenance of equipment (CP1, CP2, CP4, CP6),
PR6 Layer of protection analysis including alarm system and human factors (CP4, CP6),
PR7 Human task analysis in context of communication and interfaces for supporting Human Reliability Analysis (HRA) (CP1, CP4, CP6),
PR8 Integrated safety and security management of Industrial Automation and Control Systems (IACS) (CP4, CP5, CP6),
PR9 Staff and personnel recruitment, training and competence management (EP1, SP1),
PR10 Audit of organizational, safety and security culture (EP1, EP2),
PR11 Evaluation of Estimated Maximum Loss (EML) / Probable Maximum Loss (PML) for decision making and insurance (EP1, EP4).
PR12 Evaluation and ranking indicators and factors for development strategy and current tactic of risk reduction, retention and transfer to insurance company (EP1, EP3, EP4).

Due planned contribution to the HAZARD project it is proposed to develop relevant methods to be useful in implementing procedures: *PR1, PR2, PR5, PR6, PR7, PR8 and PR12.*

3.4. Sources of knowledge and methods useful for functional safety analysis within process based management system

The functional safety concept for reducing risks in hazardous plants using safety-related systems, i.e. the *electrical, electronic and programmable electronic (*E/E/PE) *systems* and *the safety instrumented systems* (SIS) is described respectively in standards IEC 61508 [17] and IEC 61511 [18]. The allocation of requirements [35], using acceptance criteria for individual and/or societal risk, for consecutive *safety function* (SF) defined to be implemented using these systems is illustrated in *Figure 4*.

The *safety integrity level* (SIL) of given SF is expressed by a natural number from 1 to 4 and is related to the necessary risk reduction when given SF is implemented. In some cases determining the *hardware fault tolerance* (HFT) is required. The functional safety methodology is described in the monograph [30].

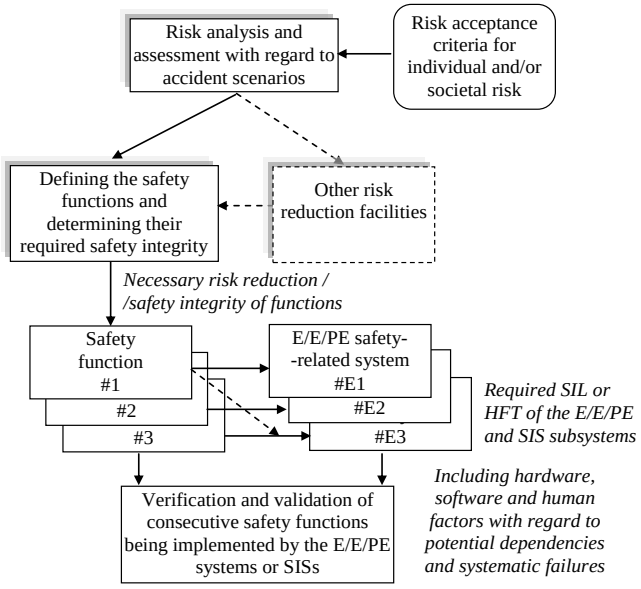

Figure 4. Allocation of requirements for safety-related systems: E/E/PE or SIS

Proposed framework for knowledge-based functional safety and security management is shown in *Figure 5*. In the centre of this figure a block of "Process based *management* system (PBMS)..." in given hazardous process installation/plant" is situated.

The framework includes knowledge and methods of relevant scientific domains (mathematics, informatics, computer science, control engineering, reliability, ergonomics, economics, management, etc.) including integrated safety and security analyses and assessments with regard to risk-related criteria to be applied within a procedure of the PBMS.

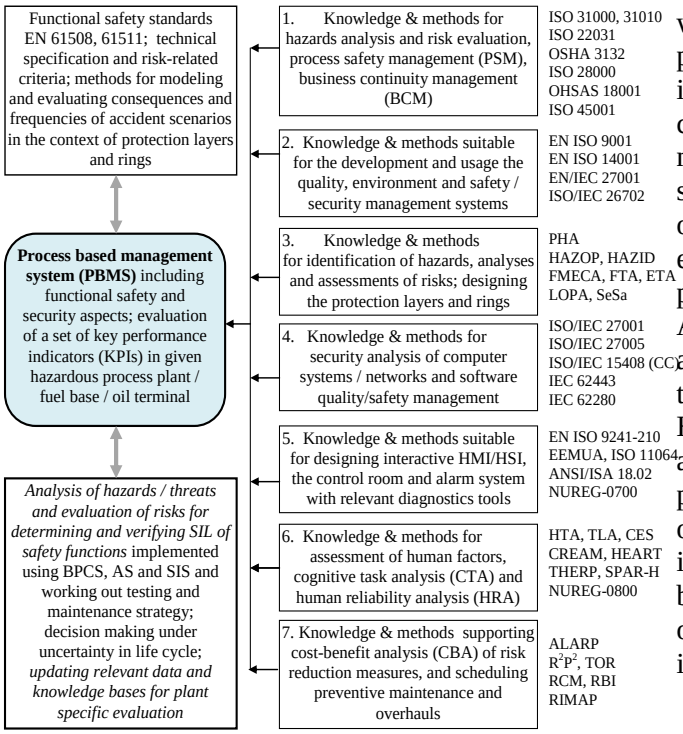

Figure 5. Process based functional safety and security management

Seven categories of domain knowledge, methods and data for supporting the functional safety analysis and management in the design and operation of hazardous installations are distinguished in *Figure 5*. On the right side of this figure the blocks numbered from 1 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 publications [1], [29], [40].

As it was mentioned several sources of uncertainty may exist and it is worth to mention about the distinction between *epistemic uncertainty* and *aleatory uncertainty*, because it is essential for careful risk assessment to provide honest support for safety-related decision making.

The methods, standards and reports specified above form a *knowledge base* (KB) supporting integrated *systemic functional safety and security management* of the control and protection systems in hazardous plants and systems of *critical infrastructure* (CI) including the oil port terminals.

4. Insurance issues of high risk plants and critical infrastructure systems

4.1. General remarks

The main goal of industrial company is satisfying his clients and making profit. The management is charged with the responsibility of manufacturing products or providing services at a sufficient profit to make new investments based on advanced technology to be competitive on the market. However, when the manufacturing facility and its equipment would be seriously damaged, e.g. by fire, explosion, mechanical or electrical breakdown or other peril, even the most effective management effort might fail to maintain profitability in several years after major accident.

An important issue in industrial plant is also appropriate risk management, e.g. by reducing risk or transferring certain level of risk to the insurer. However, the insurer should carefully manage a profile of insured risk in such a way to guarantee his profit. It requires to offer the insurance proposal based on careful evaluation of risk in existing conditions of industrial plant considered minimizing own risk before an insurance policy is specified for the period of liability [10]. Main parts of the route of data in the insurance activity are shown in *Figure 6*.

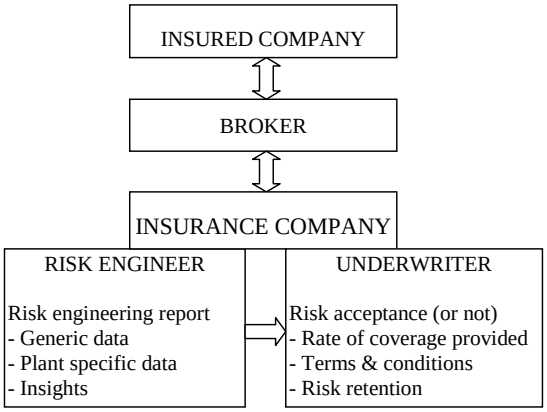

Figure 6. Main parts of the route of data in the insurance activity

The major challenge of an *underwriter* activity is to build up a "risk velvet" whose level of damages will not be higher than the level taken in the process of establishing insurance tariffs. Therefore, the underwriter should have as wide knowledge concerning the insuring organization as possible and especially about risk related factors. Sources of knowledge for the underwriter include *survey reports* written by the *risk engineers* on the base of an insurance audit or broker's slip.

The range and quality of data about the insuring risk are crucial for profitability of any insurance company, especially in a competitive insurance market. A high risk plant presents its own specific risk to the underwriter. The risk will revolve round the process carried out, the quality of management control, the safeguards incorporated into the system, the hazards from the materials stored on the site and the situation of the site in relations to other properties. The underwriter is also concerned with the possible

pollution risk caused by accidental discharges from premises.

When underwriting an engineering risk, insurers rely on a variety of information most of which is factual. Judgment is needed concerning specific risk factors expressed often qualitatively and this is based on what the underwriter knows from experience, intelligence about the risks in given branch and some survey reports [10].

Survey reports are intended to:

- set a risk into a context of other similar risks,
- evaluate whether relevant specifications have been complied with,
- identify any unusual features which might influence attention of an underwriter
- provide more detail information than an underwriting submission,
- make recommendations for improvements to reduce risks.

If the report prepared by the risk engineers shows clearly that the risk level is too high, according to risk tolerance criteria established in an insurance company, following decisions can be undertaken by the underwriter:

- refuse to offer terms,
- charge a higher premium, or
- restrict covering of specific hazards and threats.

Expertise is required in each of these aspects, if risks are to be properly considered. Reports from technical specialists with limited insurance understanding may focus too heavily on the technology of what has been surveyed and insufficiently on the factors and indicators that determine the range of risk and what should be done to manage them better.

Large insurers, reinsurers and brokers have teams of surveyors who usually work in a fairly standardized way with defined routines and report formats including rules to govern what goes into a report and how it is interpreted. The underwriter has to decide if their in-house team has sufficient expertise or whether to appoint an external specialist. In-house teams may be focused on the type of risks that generate large numbers of surveys (and thus predictable workload) and may not have expertise on some types of hazards / threats. They may not be prepared or allowed to work in some sites due to difficult security situations. Both the underwriters and client may benefit from input of the independent risk engineers.

4.2. Basic issues of an oil port insurance

An oil port is exposed to a wide range of hazards / threats and associated risks. An evolving, and unique, risk profile requires a balanced insurance strategy to address appropriate risk mitigation [6], [9], [10]. Such strategy would include risk transfer through the use of traditional insurance policies, together with innovative solutions tailored to the specific expectations and requirements of the client. Presented approach demands a sophisticated risk analysis and evaluation process in so many aspects of activity as coverage insurance policy offers.

Insurance risk engineers and advisors often assists the oil terminal operators in understanding, quantifying and managing insurable risk exposures arising from proposed or actual ownership and operation of a port or terminal assets, including exposure to past, current, and potential *liabilities*.

They also assess whether the insurance cover proposed for the facilities addressed risks appropriate for the oil terminal operator, including *non-damage business interruption*. The insurer also analyses the length of the business interruption insurance indemnity period, whether an insurance cover is compliant with insurance provisions contained within key commercial contracts entered into, the scope of insurance cover in respect of contract works that are the responsibility of the owner, and the adherence with statutory requirements to purchase insurance cover.

The oil terminal operators and the insurer should maintain constant control for design and planning implementation of solutions during all other lifecycle stages, in accordance with national standards requirements. This recommendation applies to the oil terminals involving the use, production, storage or transfer of relevant hazardous substances with regard to the possibility of soil and groundwater contamination, or having a potential adverse impact on other vulnerable parts such as water-courses of the receiving environment at the site of the industrial facility.

The oil terminal insurance decision process should take into account the risk of exposing property, human populations and vulnerable habitats to the hazards of toxic and flammable materials. The consequences of "worst case scenarios" need to be considered as a main part of insurance risk analysis process to a specific site location.

In this context must be stated that though several definitions of „worst case scenario" are already in existence, yet none of them cover the full scope of the problem. In 1973 the definitions of the *probable maximum loss* (PML) and the *estimated maximum loss* (EML) in the field of technical and fire insurance were established [10]. Either PML or EML indicators are useful in demonstrating the relationship between the level of insurance premium being obtained and the likely extent of loss.

In addition, the purpose of PML/EML is to allow insurers to optimize their net retentions and thus to keep as much premium as possible for their own

account. In other words, the purpose is to decide how large a monetary loss the company should be prepared to bear for its own account, set against its own financial strength, or possibly pass on to its reinsurance programme. By writing a share on maximum loss basis, an insurer can write more of risk, but consequences of the PML/EML concept failure might be damaging. It must be kept in mind that mostly insurances offer all risk coverage. Therefore, the individual dangers are decisive for the determination of the PML/EML.

Below some explanations are outlined with regard the publication [8]. It is assumed that the loss events, corresponding to the values belonging to the interval $(0, x_m]$ are rare. The upper limit x_m, representing the most severe loss (PML/EML) which the insured is concerned with, is assumed to exist finite. Each severity class or loss interval $(x_1, x_2] \subseteq (0, x_m]$, corresponds to a stochastic "number of loss" variable $\tilde{n}_{x_1,x_2:f}$ distributed as

$$P(\tilde{n}_{x_1,x_2:f} = n) := \frac{e^{-\int_{x_1}^{x_2} f(x)dx} \left(\int_{x_1}^{x_2} f(x)dx\right)^n}{n!} \qquad (1)$$

where $P(\tilde{n}_{x_1,x_2:f} = n)$ represents the probability that n losses valued in the generic severity class $(x_1, x_2] \subseteq (0, x_m]$ occur during the year and f is the expected loss function that corresponds to the classical „expected frequency / loss severity" relationship used often in risk management.

The theoretical research works concerning evaluation of PML/EML are still under development. In practice the EML or PML are estimated by dividing the risk to be evaluated into complexes. A complex may consist of one or more buildings or rooms or structures that contain themselves structural boundaries or separations. They need not be completely separated from neighboring buildings or structures. Caution should be exercised in defining complexes because experience has shown that structural separation in the conventional sense is no longer entirely effective in the event of a loss.

For example, today's rapid technological advancement has greatly increased fire loads and the danger of explosion. It is necessary to identify the complex with the greatest exposure. Additionally, it should be considered that a fire can also spread to other complexes. The possibility that a fire may spread beyond the complex in which it starts is suggested to be evaluated by the following risk characteristics or events:

a) Risk of explosion;
b) Risk of consequential damage resulting from corrosive gases or vapours;
c) Risks created by the neighbourhood;
d) Cases of simultaneous arson in several separate complexes;
e) Disaster-like effects of external factors connected neither directly nor indirectly with the risk insured, e.g. plane crash.

A special difficulty arises with the insurance of large industrial complexes for instance an oil port. As a rule, no detailed complex descriptions exist (large open air sites prevail, building complexes are of minor importance). The underwriter is recommended to reach an agreement on a compensation limit which may then be referred to as the PML/EML. As far as applicable, with respect to the oil port, the so called UVCE (*Unconfined Vapour Cloud Explosion*) is regarded as the PML/EML defining occurrence.

The following aspects should be taken into account for assessing underwriting indicator of worst scenario:

(a) General layout of the facility. Safety distance between the oil terminal facilities such as tank farms, pumping stations, loading stations, flares, relief devices and blow-down systems, emergency access, fire pumps etc. Facility siting can have significant effects on the hazards of the oil terminals;

(b) Spatial separation and property values concentration.

(c) Construction e.g. resistance to effects of fire (thermal radiation) and or explosion (overpressure);

(d) Domino effects: Are there nearby sources (equipment / installations) that could threaten the entire site by potential failure;

(e) Emergency access and response support access for emergency response teams (e.g. fire brigade);

(f) Power supplies: the need for emergency equipment such as lighting, fire pumps, sprinkler system to operate when the main power source is impaired;

(g) Occupied buildings (e.g. control rooms, meeting rooms and offices);

(h) The consideration of location of occupied buildings to minimise risk for the occupants in an emergency situation such as fire or explosion;

(i) In the case of control rooms, provision of uninterruptible power supplies to control systems in the event of power failure;

(j) Provision of fire water and fire protection systems; these may be provided via specific systems within the oil terminal or local city supply or from harbour;

(k) Security systems and access controls; provision of a secure perimeter fence (land side) and measures to prevent unauthorized access from water side.

Assessing the PML/EML is only one goal of insurance audit. Such audit is a more complex structured process of collecting independent information on the efficiency, effectiveness, and reliability for insurance purposes. It should lead to a plan for corrective action. Intervals between audits should not exceed 3 years.
Audits and reviews should be performed at all stages of the lifecycle of the oil terminals, including the routine monitoring of performance (i.e. active monitoring). Feedback of audit findings should be available within e.g. 1 month of the audit to all parties including management and staff at the oil terminal. Corrective actions need to be covered in follow-up reviews scheduled within 1 year of the audit.
Insurer experts lead periodic audits of the plant in order to revise the worst scenario consequences and assessing main risk features as follows:

(a) *Operation, maintenance and testing crucial applied technical systems*. The technical condition assessment is a high level review to identify equipment of high risk for safe and reliable continuation of production. The condition review may be based on site observations, review of documentation, management systems and interviews of personnel. The objective is to evaluate the future operating conditions and production scenarios and identify the challenges for the facility to continue operations with equipment considered as critical.

(b) *Management systems*. The effective management of plant is fundamental to the maintenance of process safety on a high hazard site. As such, it is imperative that the oil terminal operator has a clear understanding of the processes to manage and their effectiveness. Oil terminal operators should implement an integrated and comprehensive management system that systematically and continuously identifies hazards, evaluate and manage risks, including risk due to potential human error/failure, to achieve finally acceptable levels of risks.

(c) *Protection infrastructure*. Fire water sources (storage tanks, city water supplies, harbour water), fire pumps, sprinkler systems, fire fighting foam systems, deluge systems, steerable deck monitor nozzles (with or without foam injection). Also portable equipment, like fire trucks/pumpers, fire hoses, portable monitors, fire extinguishers, personal protective equipment, emergency power supply, hazard detection systems: gas & fire detection equipment, emergency & rescue equipment for potential human and/or environmental damages.

5. Key performance indicators evaluation for supporting safety and business continuity management

Key Performance Indicators (KPIs) should be developed to help organizations understand how well they are performing in relation to their strategic goals and objectives [4], [20]. KPIs provide the most important performance information that enables organizations and their stakeholders to understand whether the organization keeps track in realization of relevant activities and processes or not.
The aim is to develop a set of KPIs for given organization to reduce the complex nature of organizational performance to a small number of key indicators in order to make the complex management problem more understandable and transparent for decision making.
A KPI is something that can be counted and compared; it provides evidence of the degree to which an objective is being attained over a specified time. The issue is whether to use *qualitative or quantitative metrics*. The analysis is often most powerful when the analyst uses both qualitative and quantitative metrics to work with [20].
Some organizations have a preference for choosing quantitative metrics collecting numbers of inertest. The quantitative data is often easier to collect and to translate into meaningful metrics. However, it is important to balance numeric data with qualitative (non numeric) assessment of performance, as this can be a powerful way to highlight issues that are important to customers and stakeholders. It is especially useful in management of complex systems and organizations.
A typical KPI should be easily understood and have the following characteristics [4], [20]:

- be aligned to service delivery goals,
- provide context,
- create meaning at relevant organisational levels,
- be based on clear measurable data or expert opinions,
- be easy to understand,
- lead to action.

Obviously, a set of Key Performance Indicators (KPIs) can be proposed to support the *process safety management* (PSM) in hazardous plants [3]. They can be also useful for insurance purposes. The set of process safety related KPIs is needed to establish both a baseline of realistic current process safety performance, and also enable all levels of the organisation to understand and drive improvements in process safety performance in the short to medium

term. Also a set of business continuity related KPIs would be useful to support decision making in manage business in relevant time horizon.
The safety related KPI development activity should start from understanding how the company managed process safety at the time. The assessment can include such activities as: PSM systems implementation assessment; quality of *Hazard and Operability* (HAZOP) analysis, and *Layers of Protection Analysis* (LOPA) study [31], [32], design of automation and control systems, alarm system rationalization, control room operator competency review, training of staff and personnel, business related risk segmentation and assessment, safety and security culture assessment [3], [5], etc.
The strength of developing process safety related KPIs in this context is to utilize the objective findings of the assessment activities, which will highlight gaps in process safety management in relation to targets.
Examples of KPIs regarding publications [3], [12], [13], [19], [30], [33], [40], [41] are as follows:

- Percentage of pre-start up audits containing significant process safety findings;
- Number of permit violations observed during local *permit to work* (PTW) audits;
- Number of PTW reviews per week by asset managers/asset;
- Percentage compliance with corrective maintenance plan;
- Percentage compliance with preventative maintenance plan;
- Number of approved waivers & safeguarding overrides;
- Number of excursions outside asset operating envelop;
- Availability of critical devices and installations;
- Total alarm rate in human system interface;
- Safety integrity level (SIL) of safety functions;
- Security assurance level (SAL) of industrial computer network conduits; etc.

The set of safety and business continuity related KPIs for the oil port terminal are at developing stage to be useful in supporting the *process based management system* (PBMS) and for insurance related decision making.

6. Conclusions

The oil ports play an important role in the energy sector economy and *Critical Infrastructure* (CI) of the country. In the *management system* (MS) of oil port infrastructure relevant existing safety and security-related recommendations and requirements have been considered.
Also important aspects of business continuity management have been be taken into account to develop effective economic technical and organisational solutions. However, due to uncertainty involved the decision making in life cycle, relevant management processes are based on evaluations of risks to be reduced and controlled in time.
Methodological aspects of a *process based management system* (PBMS) based on analysis of hazards and threats and risk evaluation for an oil port infrastructure in context of insurance have been outlined. It was postulated that the information gathered during the insurance audit can be useful in either of safety and security management of maritime infrastructure, in particular the oil port terminals.
The purpose to apply in practice the PBMS approach is to ensure that requirements for safety are not considered separately but put in the context of all the other requirements concerning safety, security, safeguards, environment, occupational safety and economy. The approach is based on the PDCA (*Plan-Do-Check-Act*) model according to a Deming concept, adapted in quality management standard ISO 9001. Some processes and procedures within the PBMS have been defined.
The scope of an insurance audit of the organisation and installations has been outlined to identify the hazards and threats, and specify more important factors influencing risks. Some activities of the *risk engineer* and the *underwriter* in the insurance related processes are outlined including identification of more important factors influencing risks.
The issue of evaluating the *probable maximum loss* (PML) and the *estimated maximum loss* (EML) is emphasized. The theoretical works concerning evaluation of PML/EML are still under development. In practice the EML or PML are estimated by dividing the risk to be evaluated into complexes.
It is emphasised that determining and evaluating a set of *key performance indicators* (KPIs) based on data from site audits and further evaluations can be useful for the safety management of the oil port and its insurance. Further contribution to the HAZARD project it is proposed to develop relevant methods supporting procedures for integrated safety and security management of *industrial automation and control systems* (IACS) and a set of KPIs.

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/

"Scientific work granted by Poland's Ministry of Science and High Education from financial resources for science in the years 2016-2019 awarded for the implementation of an international co-financed project."

References

[1] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2010). Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issues. *Proceedings of PSAM 10*, Seattle.

[2] Berg, H.P. (2010). Risk management: procedures, methods and experiences. *Reliability: Theory & Applications* (RT&A), No. 2 (17).

[3] Brown, M. (2009). Developing KPIs that drive process safety improvement. Hazards SSI, Symposium series No. 155, IChemE. Lloyds Register EMEA, Aberdeen.

[4] BIFM (2014). Measuring contractors performance using KPIs, Guidance notes for facilities managers. British Institute of Facilities Management.

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

[6] CRO Forum (2014). Cyber resilience, The cyber risk challenge and the role of insurance. KMPG Advisory, Amstelveen.

[7] Decree PL (2011). Decree of Economy Minister concerning technical conditions for bases and stations of liquid fuel, and long-distance transfer pipelines for transportation of crude oil and petroleum products, and their location. 1633, 16.12.2011, Dz.U. No. 276, pos. 1663.

[8] Ghisellini, R. (1997). Insurance policy value and Pareto-optimal retention in the hypothesis of rare loss events. *Sistemi Srl*, Milano.

[9] Gołębiewski, D. & Kosmowski, K.T. (2005). *Risk analysis for insurance of technical systems.* ESREL, Advances in Safety and Reliability (ed. Kołowrocki), A.A. Balkema Publishers, Taylor & Francis Group, London, 683-687.

[10] Gołębiewski, D. (2010). *Insurance Audit, Practical methods of risk analysis* (in Polish). Poltext Publishers, Warsaw.

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

[12] Grøtan, T.O., Jaatun, M.G., Øien, K. & Onshus, T. (2007). The SeSa Method for Assesing Secure Remote Access to Safety Instrumented Systems (SINTEF A1626). Trondheim.

[13] Hildebrandt, P. (2000). *Critical aspects of safety, availability and communication in the control of a subsea gas pipeline, Requirements and Solutions* HIMA.

[14] HSE (2001). Marine risk assessment. Offshore Technology Report 2001/063 prepared by Det Norke Veritas.

[15] IAEA (2001). Risk management: A tool for improving nuclear power plant performance. IAEA-TECDOC-1209. International Atomic Energy Agency, Vienna.

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

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

[18] IEC 61511 (2015). Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva.

[19] IEC 62443 (2013). Security for industrial automation and control systems. Parts 1-13 (undergoing development). International Electrotechnical Commission, Geneva.

[20] Intrafocus (2014). Developing Meaningful KPIs. Park Road, Winchester.

[21] ISGOTT (1996). International Safety Guide for Oil Tankers & Terminals, International Chamber of Shipping, London.

[22] OSHA 3132 (2000). PSM - Process Safety Management. U.S. Department of Labor, Occupational Safety and Health Administration.

[23] ISO 9001 (2015). Quality management systems - Requirements. International Organisation for Standardisation.

[24] ISO 14001 (2015). Environmental management systems - Requirements with guidance for use. International Organisation for Standardisation.

[25] ISO 22301 (2012). Societal security - Business continuity management - Requirements. The International Organisation for Standardisation.

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

[27] ISO/IEC 15408 (1999). Information technology Security techniques – Evaluation criteria for IT security. Part 1-3. International Electrotechnical Commission, Geneva.

[28] ISO/IEC 27001 (2013). Information technology - Security techniques - Information security management systems - Requirements.

[29] Kosmowski, K.T., Śliwiński, M. & Barnert, T. (2006). Functional safety and security

assessment of the control and protection systems. *Proc. European Safety & Reliability Conference – ESREL,* Estoril. Taylor & Francis Group, London.

[30] Kosmowski, K.T. (2013). *Functional safety and reliability analysis methodology for hazardous industrial plants.* Gdańsk University of Technology Publishers.

[31] Lebecki, K. Rosmus, P., Martyka, J. & Markowski, A. (2013). *Integrated methods of occupational, social and environmental risk management for hazards of major industrial accidents* (in Polish). Główny Instytut Górnictwa (GIG), Katowice.

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

[33] Mahan, R.E. (et al.) (2011). Secure Data Transfer Guidance for Industrial Control and SCADA Systems. PNNL-20776, Pacific Northwest National Laboratory, Richland.

[34] MARPOL (2005). International Convention for the Prevention of Pollution from Ships, Lloyd's Register Rulefinder.

[35] Missala, T. (2010). Book of procedures for functional safety compliance evaluation of protection systems in the process industry. Report no. 8795, PIAP, Warsaw.

[36] Muhlbauer, K. (2004). *Pipeline Risk Management Manual Ideas, Techniques, and Resources,* Third edition, Elsevier.

[37] SESAMO (2014). Integrated Design and Evaluation Methodology. Security and Safety modelling. Artemis JU Grant Agr. no. 2295354.

[38] SOLAS (2005). International Convention for the Safety of Life at Sea. Lloyd's Register Rulefinder.

[39] STCW (1996). Convention International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, International Maritime Organization London.

[40] Śliwiński, M., Kosmowski, K.T. & Piesik, E. (2015). *Verification of the safety integrity levels with regard of information security issues* (in Polish), In: Advanced Systems for Automation and Diagnostics, PWNT, Gdańsk.

[41] UN (2006). Maritime security: elements of an analytical framework for compliance measurement and risk assessment. United Nations, New York and Geneva.