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

Gołębiewski Dariusz
PZU Group, Warsaw, Poland

Functional safety and cyber security analysis for life cycle management of industrial control systems in hazardous plants and oil port critical infrastructure including insurance

Keywords

functional safety, cyber security, hazardous plants, oil port infrastructure, industrial automation and control systems, hazards, threats, vulnerabilities, risk analysis, key performance indicators, integrated safety and security management, business continuity management, insurance

Abstract

This report addresses selected methodological aspects of proactive reliability, functional safety and cyber security management in life cycle of industrial automation and control systems (IACS) in hazardous plants and oil port critical installations based on the analysis of relevant hazards / threats and evaluation of related risks. In addition the insurance company point of view has been also considered, because nowadays the insurer, interested in decreasing risks to be insured, offers the expertise how to limit effectively risks in life cycle from the design conceptual stage of hazardous plant, through its reliable and safe operation, until decommissioning. Therefore, the risk evaluation model for insurance related decision making for the period considered, e.g. one year, should be plant specific with some predictive properties due to changing environment and business conditions, and usually considerable uncertainty involved.
The objective is to evaluate and mitigate risks, and control them proactively, through undertaking appropriate activities within a *process based management system* according to elaborated policy and strategy that includes organisational and technical aspects, including preventive maintenance activities of sensitive equipment and updating in time the training programmes. Careful evaluating and controlling risks is also crucial for the insurance company. Basic activities of the risk engineers and underwriters in the insurance process are outlined in the context of identified hazards/threats and defined factors that significantly influence risks to be considered in evaluating the insurance premium in the context of terms and conditions specified.

1. Introduction

The oil port installations and terminals play an important role in energy sector of the state economy and belong to the *critical infrastructure* (CI). There are numerous requirements, recommendations and guidelines how to design and operate hazardous plants including oil port installations and oil terminals [4, 25, 31, 46]. There are also guidelines concerning the hazard analysis and risk assessment methods to support the safety and security-related decision making [8, 10, 42, 51]. An important issue is to shape adequately the crew competences in maritime domain [12, 31, 50]. Various aspects are to be considered at the design stage of technical systems, and then evaluated during operation to manage in life cycle their reliability, safety and security to reduce and control in time related risks [30].

Nowadays, new challenges emerge in security area of hazardous plants and CI systems, in particular concerning security of information systems and networks [5, 6, 7]. These problems are directly related to the functional safety [22, 23] and cyber security [24] issues and implemented in practice solutions that can be more or less vulnerable to potential hazards and threats. The *industrial automation and control systems* (IACS) are in particular of significant interest because of the key role they play during the technical system operation, contributing significantly in mitigation of various risks [34, 43, 44, 45].
Lately, there is an increasing interest to apply in the industry advanced process based management systems [21, 26], covering also the *business continuity management* (BCM) and integrated *safety & security management.* This report addresses current issues of

proactive reliability, safety and security management of the *industrial control systems* (ICS) of hazardous plants and oil port installations within the process based safety and security management system. The idea has been developed within the HAZARD project and was initially outlined in the paper published in the Journal of PSRA [16]. The methodological issues of cyber security analysis and management are nowadays of special interest [3, 10, 11, 13, 19, 20]. also those including functional safety of ICS aspects [33, 36, 39].

These issues are considered below in relation to the Industry 4.0 idea, as a new stage in managing the industrial companies to control the entire value stream along the life cycle of products and services. It includes applying in industrial practice innovative technologies and organisational solutions based on coordinated in space and time activities, requiring advanced network solutions being supervised by competent specialists. Mentioned issues of the, reliability and safety management are of prime importance including security aspects of *OT / IT* (*operational technology / information technology*) convergence.

Proactive safety management involves systematic development and application in practice polices, processes and procedures in various activities including communicating and consulting, establishing the context, and monitoring for recording in time performances of interest. The issue of defining and evaluating the *key performance indicators* (KPIs) [2, 18, 29, 47, 47] is discussed for safety and security related decision making. Several categories and examples of KPIs have been distinguished and considered in the context of identified *controls / barriers* (C/B). They constitute a basis for further evaluation of the *influence factors* (IFs) of interest in systemic predictive probabilistic modelling and the risk evaluation of specific plant in relation to criteria specified to support safety and security related decision making.

In this rapport an approach is proposed for *proactive reliability and safety management* and *predictive risk* analysis within *integrated safety and security management.* It concerns especially hazardous plants and CI systems operating in changing conditions and includes *preventive maintenance* strategy to be elaborated. Evaluating and controlling risks is also crucial for the insurance company. Basic activities of the risk engineers and underwriters in the insurance process are outlined in the context of identified hazards/threats and defined technical and organisational factors that significantly influence risks to be assessed in evaluating the insurance premium in the context of terms and conditions specified.

2. The cyber security enhancing port safety

2.1. Legal requirements concerning port safety and security

Three years ago the Directive (EU) 2016/1148 of the European Parliament and the Council was published [5] that concerns some measures to be undertaken for a high common level of security of network and information systems across the Union. It is obvious that the network and information systems and services play at present a vital role in society. Their reliability, safety and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

However, the magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the critical infrastructure systems. Such incidents can significantly impede the economic activities and generate substantial financial losses undermining users' confidence and causing potentially major damage to the economy of given country and the Union as a whole [5].

In the water transport sector, security requirements for companies, ships, port facilities, ports and vessel traffic services under Union legal acts cover all operations, including radio and telecommunication systems, computer systems and networks [6, 49]. Part of the mandatory procedures to be followed includes the reporting of all incidents and should therefore be considered as *lex specialis* (specific prescription), as so far those requirements are at least equivalent to the corresponding provisions of the Directive 1148 [5]. In Annex II of this Directive that distinguishes sectors and subsectors of interest, for the transport sector and the water transport subsector following types of entities are specified:

— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council [49], not including the individual vessels operated by those companies;
— Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council [6], including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004 [49], and entities operating works and equipment contained within ports;
— Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council [7].

The Diplomatic Conference of the International Maritime Organisation (IMO) adopted on December 2002 amendments to the 1974 International Convention for the Safety of Life at Sea (SOLAS Convention) and an International Ship and Port Facility Security Code (ISPS Code). These documents were intended to enhance the security of ships used in international trade and associated port facilities. They comprise mandatory provisions, the scope of some of which in the Community should be clarified, and recommendations, some of which should be made mandatory within the Community. Then, the Maritime (ISPS Code) Regulations 2014 was published as the Maritime Transport Decree No. 20 [31].

It was decided that security should be enhanced not only for ships used in international shipping and the port facilities which serve them, but also for ships operating domestic services within the Community and their port facilities, in particular passenger ships, on account of the number of human lives which such trade puts at risk. Permanently applying all the security rules provided for in this Regulation to port facilities situated in ports which only occasionally serve international shipping might be disproportionate. Therefore, the Member States should determine, on the basis of the security assessments which they are to conduct, which ports are concerned and which alternative measures provide an adequate level of protection [4, 25, 46].

According to ISPS Code [31] a *security incident* means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high speed craft, or of a port facility or of any ship/port interface or any ship to ship activity. The *security level* was also defined for the qualification of the degree of risk that a security incident would be attempted or will occur. Three such levels are defined:

- *Security level 1* (*Normal*) means the level at which the ship or port facility normally operates with minimum appropriate protective security measures;
- *Security level 2* (*Heightened*) means the level applying for as long as there is a heightened risk of a security incident for which appropriate additional protective security measures shall be maintained;
- *Security level 3* (*Exceptional*) the level applying for the period of time when there is the probable or imminent risk of a security incident for which further specific protective security measures shall be maintained.

Port Facility means a location, as determined by the Authority, where ship/port interface takes place, and this includes areas such as anchorage, waiting berths and approaches from seaward. *Ship to Port Interface* means the physical, operational, or notional location in which ships and supporting watercraft engage port facility services. It is required in the ISPS Code [31] that the persons carrying out the assessment shall have appropriate skills to evaluate the security of the port facility in accordance with this regulation, taking into account the following elements:

(a) physical security;
(b) security equipment;
(c) security procedures;
(d) radio communications systems (*including IT systems and networks*);
(e) transportation infrastructure;
(f) utilities infrastructure;
(g) other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port, port facility or aboard ships adjacent thereto; and
(h) available expert assistance.

The port facility security assessments shall be reviewed and updated, annually taking into account changing threats and/or minor changes in the port facility and shall always be reviewed and updated when major changes to the port facility take place. Assets and infrastructure that should be considered important to protect may include [49]:

(1) accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
(2) cargo facilities, terminals, storage areas, and cargo handling equipment;
(3) systems such as electrical distribution systems, radio and telecommunication systems and *computer systems and networks*;
(4) port vessel traffic management systems and aids to navigation;
(5) power plants, cargo transfer piping, and water supplies;
(6) bridges, railways, roads;
(7) port service vessels, including pilot boats, tugs, lighters, etc.;
(8) security and surveillance equipment and systems;
(9) the waters adjacent to the port facility.

In order to achieve the security related objectives, this Code embodies a number of *functional requirements*. These include, but are not limited to [49]:

1) gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments;
2) requiring the maintenance of communication protocols for ships and port facilities;
3) preventing unauthorised access to ships, port facilities and their restricted areas;
4) preventing the introduction of unauthorised weapons, incendiary devices or explosives to ships or port facilities;

5) providing means for raising the alarm in reaction to security threats or security incidents;
6) requiring ship and port facility security plans based upon security assessments; and
7) requiring training, drills and exercises to ensure familiarity with security plans and procedures.

This HAZARD report is devoted to the computer systems and networks and is aimed to put the emphasis on the functional safety of the safety and security related computer systems and networks according to the international standard IEC 61508 [22], IEC 61511 [23] and IEC 62443 [24]. In designing the site specific functional safety and cyber security related functions with regard these standards the functional requirements specified above have to carefully considered.

It is worth to emphasize that enhancing oil port security is a significant challenge due to many substantial hazards and threats and relatively high risks of potential major accidents. Therefore, at least the *security level 2* should be implemented at the site of oil port, and in most cases the *security level 3* described above is of interest. Thus, the oil port safety and cyber security management is challenging issue due to various vulnerabilities involved [13].

Therefore, a site specific process based integrated safety and security management system is postulated to be developed for maintaining a high level of business continuity and reducing effectively safety and security related risks in life cycle. Obviously, it requires a systemic approach based on the MTE (*Man-Technology-Environment*) conceptual framework with regard to a set of reliability, functional safety and cyber security related KPIs (*Key Performance Indicators*) [1, 2, 17, 18, 47, 48] to enable proactive activities, and assessments of relevant risks in relation to the individual and societal risk criteria specified [8, 9, 10] including cyber security aspects [19, 20, 29].

2.2. Functional safety and cyber security in the context of Industry 4.0 idea

The term Industry 4.0 is lately often used to name the fourth industrial revolution. It is related to a next stage in managing of organisations and industrial companies to control the entire value stream along the life cycle of products and services. It concerns the innovative technologies and advanced activities of competent specialists and skilful supporting staff to be effectively supported by modern management systems.

Resolute leadership and system oriented thinking is needed in such management to achieve delineated objectives for elaborating business strategy, especially in the situation of increasing uncertainties. In case of hazardous industrial plants the reliability, safety and security aspects are becoming at present of prime importance. Fundamental here is the availability, confidentiality and on-line access to relevant information in relatively short time through the networking for all resources involved.

Connecting and interacting people and industrial installations, or more generally technical systems and objects, leads to the creation of dynamic, coordinated in time cross-organizational processes in networks that should be optimized according to a range of criteria, such as: functionality, availability, quality of products, costs, consumption of energy and resources, and environmental protection. In such complex distributed and interdependent processes to be reliably coordinated, the safety and security-related issues with defined risk criteria are becoming of prime importance for rational decision making at relevant control and decision-making levels in such complex systems [21, 30].

A final report of the *German Science and Industry Research Union on Industry 4.0*, issued in April 2013, provides some implementation recommendations and suggests needs for research identifying eights areas for actions that should be undertaken to provide useful in industrial practice:

1) *Standardisation* - open standards for the reference architectures, cross-organisational networking and integration via value networks.
2) *Management of complex systems* - use of models for automating activities as well as the integration of the digital and actual world.
3) *Area-wide broadband infrastructure for industry* - for exchanging relevant data in terms of volume, quality and time.
4) *Safety and security* - to guarantee operational safety, data privacy and *information technology* (IT) security.
5) *Work organisation and workplace design* - clarification of implications for involved people and employees as planners, decision-makers and workforce in possible scenarios.
6) *Training and further training* - formulation of positions and competences as well as innovative approaches for effective training and further training.
7) *Legal framework conditions* - the goal is to create the necessary legal framework conditions for the Industry 4.0 idea with Europe-wide uniformity to the extent justified (protection of digital assets, contract law, liability issues, etc.).
8) *Resource efficiency* - responsible and handling all resources (human, information and financial resources as well as raw materials and operating supplies) for innovative and effective future industrial production.

Thus, at present a fundamental issue to be properly solved in the design of industrial system and its

operation is to provide effective IT/OT convergence (see *Figure 1*), i.e. the integration of *information technology* (IT) used for data storage, processing and transferring for supporting decision-makers at relevant organization levels, with *operational technology* (OT) including hardware and software that control industrial installations, production lines and auxiliary equipment for conducting production on time (e.g. *just in time*) and optimising production processes with regard to the *quality* [26], *business continuity* (BC) [28] and *environmental* [27] aspects.
Figure 1 shows typical levels often distinguished in typical industrial process plant and its control system with indicating the area of OT/IT convergence (see levels 3and 4). At the level 1 there are sensors, actuators and conduits of the *industrial automation and control system* (IACS) that includes the *distributed control system* (DCS), *supervisory control and data acquisition* (SCADA) [11, 24], the *human system interface* (HSI) and *alarm system* (AS) (see the level 3). In functional safety standards IEC 61508 [22] and IEC 61511 [23] a domain-specific terminology is used, namely the *basic process control system* (BPCS) and *safety instrumented system* (SIS) that are treated safety-related.

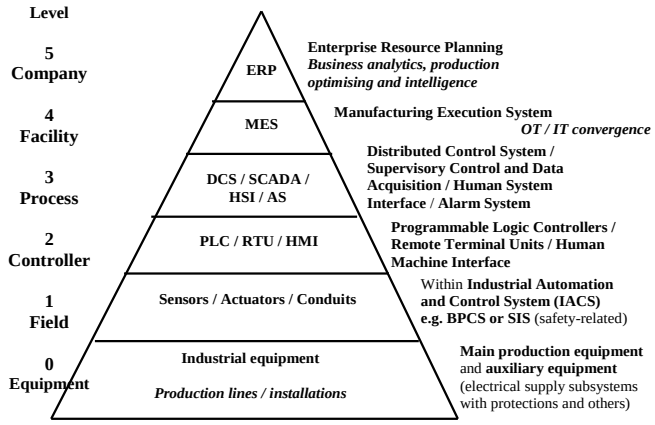

Figure 1. Typical levels in an industrial process plant and its control system indicating OT/IT convergence

The *sensors*, *actuators*, i.e. *equipment under control* (EUC), and communication *conduits* (see the level 1) connect them in an industrial computer network to relevant PLC or RTU (the level 2) or DCS / SCADA (the level 3). The benefits that come from advanced IT and OT convergence include enhanced information for undertaking decisions to optimize business processes, reduce costs, shorten projects, and reduce business risks [28, 30]. It requires advanced monitoring for better management of various processes, with regard to recorded operational data, for improved preventive maintenance, higher reliability of systems and more effective BCM. However, the safety and security management aspects have to be carefully considered to mitigate and effectively control relevant risks.

3. Risk analysis and management in organisations

3.1. Risk management general issues

Today many organizations and industrial companies face problems due to internal and external influences that make them uncertain to achieve business and development goals. Some of them can be more or less precisely described, especially those concerning business and operation objectives in changing and uncertain environment. It concerns also modern innovative industry, interested to follow principles and new challenges of the Industry 4.0 idea mentioned above. Any industrial plant operates in specific surrounding area and environment and is dependent on availability of some functions to be provided by operators of *technical infrastructure* especially *critical infrastructure* (CI), e.g. electric power grid, transport infrastructure, telecommunication and computer networks etc. [5].
In the ISO 31000 standard [30] a term of *risk* is generally defined as an effect of uncertainty on the organization objectives. Such effect can be e.g. a deviation from something expected that can be positive, negative or neutral. It addresses opportunities in context of hazards and threats. *Risk management* (RM) is understood as coordinated activities in time to direct and control an organisation with regard to evaluated risks. *Risk* can be expressed in terms of *risk sources* with regard to possible hazards and/or threats, resulting in some events / scenarios with their consequences and likelihood. Such definition of risk differs to other more specific definitions of risk, e.g. proposed in functional safety standards [22, 23].
In the second edition of ISO 31000 standard [30] a general risk management methodology is outlined that includes: *principles*, *framework*, and *process*, as shown in *Figure* 2.

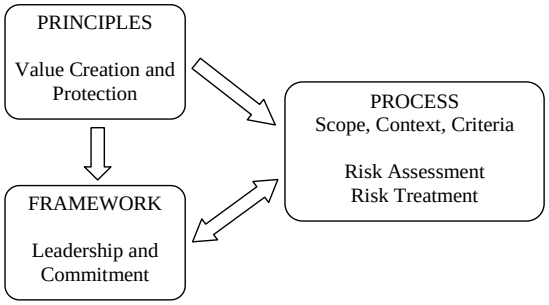

Figure 2. Relations between principles, framework and process in the risk management (based on [30])

Risk management can be applied to the entire organization, at its distinguished levels and areas of interest, and to specific projects and activities, processes and functions, including safety and security aspects. Establishing context of risk management requires considering the environment in which the objectives are to be achieved, opinions of stakeholders [26, 30] and relevant risk acceptance criteria. It should help to reveal and assess the nature of hazards / threats and their potential consequences that can result in the capital assets or other business-related economic losses. In case of hazardous plants the risk evaluation for potential major accidents with damages to people and environment should be of special interest with regard to existing safety and security-related regulations.

The *principles* specify how to create and protect value in an efficient *risk management* (RM) process that should be [30]:

a) *Integrated* - as an integral part of organizational activities,
b) *Structured and comprehensive* - contributing to consistent and comparable results,
c) *Customized* - to the organization's external and internal context, and its objectives,
d) *Inclusive* - to enable appropriate and timely involvement of stakeholders with considering their knowledge and opinions for improving awareness and risk informed management,
e) *Dynamic* - risks can emerge or change as the organization's external and internal context changes responding to possible changes and events in an appropriate and timely manner,
f) *Based on best available information* - the inputs to RM should contain historical and current information as well as future expectations,
g) *Relevant to human, organisational and cultural factors* - because culture, human behaviour and potential errors can significantly influence RM at each levels and stages,
h) *Continuously improved* - through learning, experience and knowledge acquisition, applying innovative technologies for secure IT / OT convergence to support effectively decision making in the organisation.

The *leadership and commitment* are important factors in the *framework* development (see *Figure 2*). The organization should evaluate its existing RM practices and processes, and eliminate or reduce existing gaps within the framework. Top *management* should ensure that diligent RM procedures are to be integrated into relevant organisational activities and should demonstrate adequate leadership and commitment.

Following activity components within the *risk management framework* should be customised to the needs and activities of particular *organisation* of *industrial plant*:

- *Integration* - it relies on understanding of organisational strategy, objectives, needs, structure, culture and context, and should be treated as a dynamic and iterative process,
- *Design* - to include the organisation's internal and external context with regard to complexity of networks and possible dependencies, defining the *key performance indicators* (KPIs) and considering more important *performance shaping factors* (PSFs) for dealing with human and organisational factors [32, 34, 35, 38, 40], legal requirements and expectations of authorities and stakeholders,
- *Implementation* - the organisation should develop appropriate plan including time objectives and required resources, and modify the decision making processes when justified to address uncertainties involved,
- *Evaluation* - the organisation should periodically reviewed the performance and effectiveness of the risk management framework against its purpose, implementation plans, indicators to be evaluated, to determine whether it remains suitable to achieve the organisation's objectives,
- *Improvement* - the organisation should monitor and adapt the risk management framework to address internal and external changes including legal requirements, innovative OT and IT solutions, environmental factors, experience and knowledge acquired, and other aspects important for considering in modern process based quality management system [21, 26].

The *risk management process* (see *Figure 3*) involves the systematic application of polices, processes, procedures, and practices to activities of communicating and consulting, establishing the context, and monitoring for recording performances of interest to be useful in evaluating of KPIs, PSFs, and the *influence factors* (IFs) relevant to the predictive risk evaluation and treatment. These issues are discussed further in this report.

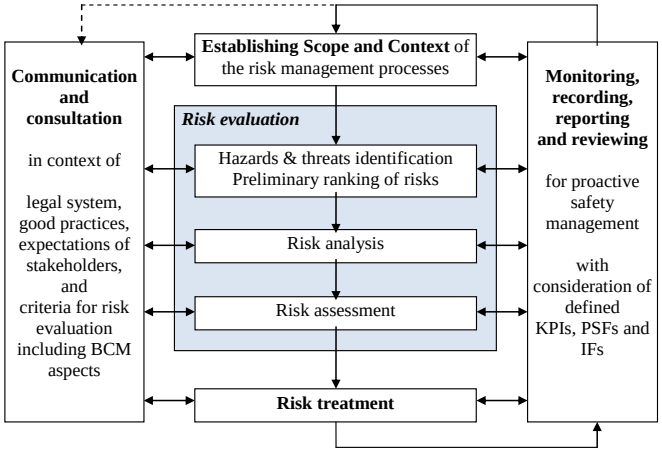

Figure 3. Risk management process (based on [30])

3.2. Functional safety and cyber security management

There are various sources of knowledge and relevant methods to be useful for functional safety analysis within process and procedure based management system [16, 37, 39]. 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 [22] and IEC 61511 [23]. The allocation of requirements 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*.

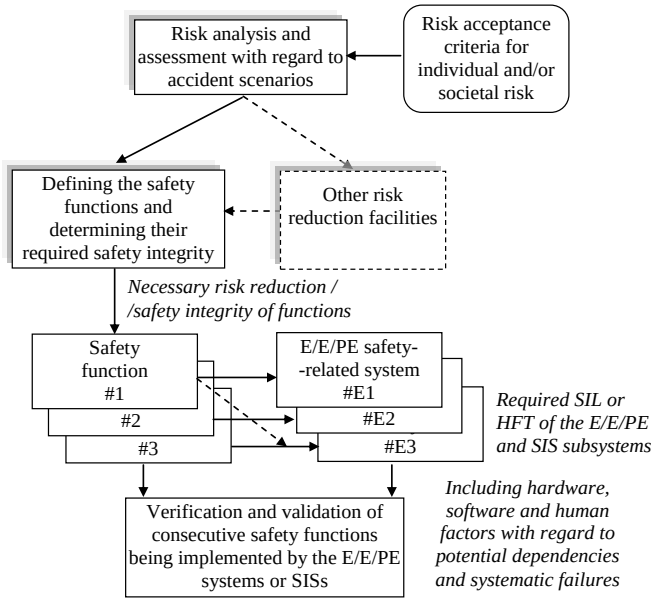

Figure 4. Allocation of requirements for safety-related systems: E/E/PE or SIS

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 numerous publications [33, 34, 35, 36, 41].

Proposed framework for knowledge-based functional safety and security analysis and management in life cycle is shown in *Figure 5*. The *process based management system* (PBMS) is supported by knowledge and methods of relevant scientific domains (mathematics, informatics, computer science, control engineering, reliability, ergonomics, human factors and reliability, economics, management, etc.) as characterized in consecutive blocks 1÷7 for integrated functional safety and cyber security analyses with regard to risk-related criteria to be applied within a step-by-step procedure [34, 37].

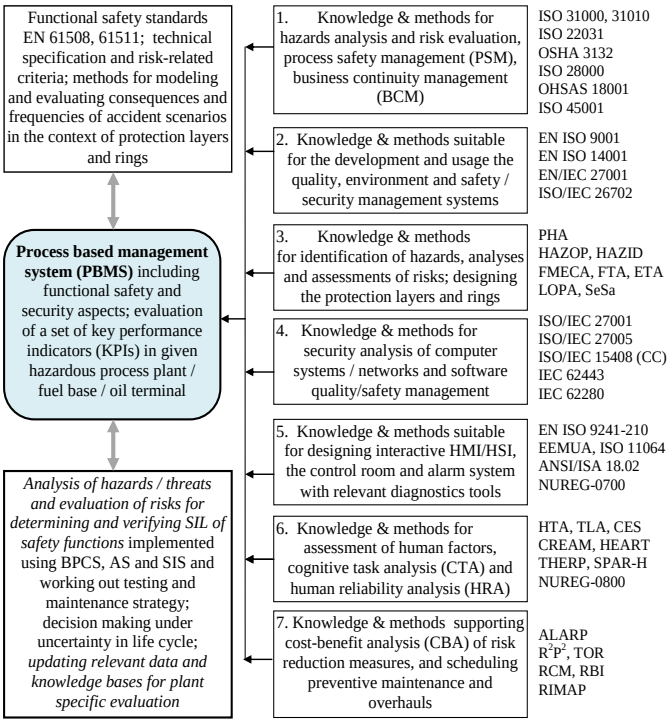

Figure 5. Process based functional safety and security management

Thus, selected methods, standards and reports form a *knowledge base* (KB) supporting integrated *systemic functional safety and cyber security management* of the control and protection systems in hazardous plants and systems of *critical infrastructure* (CI) including the oil port terminals. A current research and engineering challenge is how to integrate safety and security aspects.

As it is shown in *Figure 6* below there are two paths, respectively, of the safety and security analysis and management. In the middle of this figure there are blocks that are to be treated as joining elements of integrated analysis. They include:

– Analysis of safety and security environments,

- Applying system-oriented approach,
- Aggregating of qualitative and quantitative information, e.g. opinions of domain experts,
- Specification and integration issues,
- Comparative risk evaluations,
- Evaluating of processes, monitoring and assessing of events in life cycle.

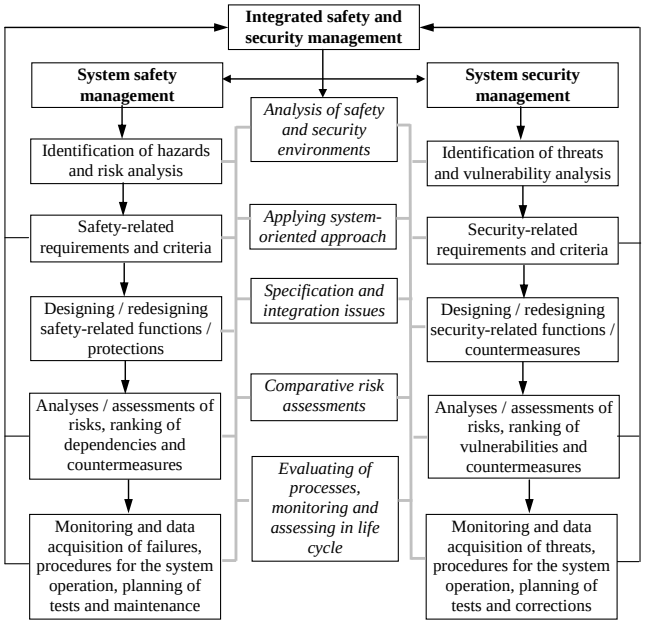

Figure 6. Integrated functional safety and cyber security analysis and management of critical infrastructure systems

3.3. Functional safety requirements for assumed individual and societal risk criteria

ALARP (*as low as reasonably practicable*) principle is proposed often to be used in practice to reduce a risk to a level which involves balancing reduction in risk against the time, difficulty and cost of achieving it, e.g. applying the *cost-benefit analysis* (CBA). This level represents the point, objectively assessed, at which the time, difficulty and cost of further reduction measures become unreasonably disproportionate to the additional risk reduction obtained [17]. Typical individual risk thresholds are presented in *Figure 7* for workers and other persons exposed to risk.

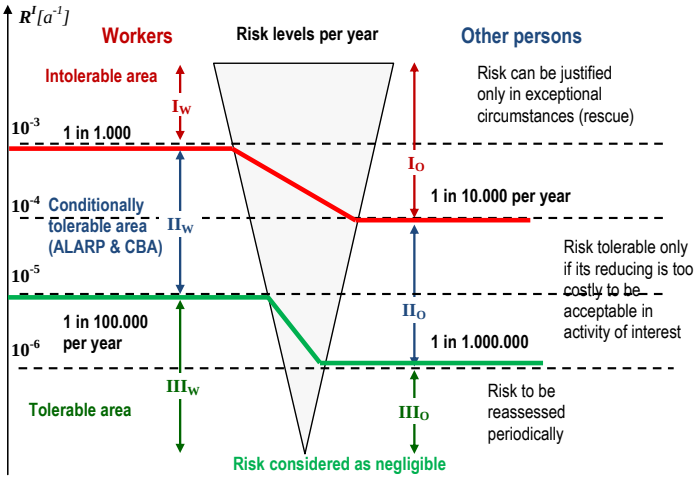

Figure 7. Individual risk criteria in the context of ALARP principle (based on [17])

Some examples of CBA methods are proposed in publications [35, 37]. The ALARP principle can be applied in a similar way to the societal risk [32, 34]. As it is known the societal risk is generally used to describe multiple injury and fatalities due to potential accidents. Such risk can be represented using F-N curves, what is a challenging task for group of experienced analysts, or a risk matrix [32, 42, 45] with defined categories of frequency and consequence of specified severity due to potential accidents. Example of the risk matrix is presented in *Table 1*. Four types of consequences are considered: *people/health*, *assets*, *environment*, and *reputation*, potentially of five levels of *severity*.

Table 1. Risk matrix for defining risk areas for distinguished categories of frequency and consequence with five levels of severity

Consequences*					Probability / frequency [a^{-1}]				
People – health	Assets	Environment	Reputation	Severity	A	B	C	D	E
					$F_A < 10^{-4}$ Improbable	$F_B < 10^{-3}$ Remote	$F_C < 10^{-2}$ Occasional	$F_D < 10^{-1}$ Probable	$F_E \geq 10^{-1}$ Frequent
Multiple fatalities ($< 10^{-5}a^{-1}$)	Extensive damage ($\geq$ \$100M)	Massive effect	Catastrophic (international impact)	5	RR^*_{5A}	RR^*_{5B}	RR^*_{5C}	RR^*_{5D}	RR^*_{5E}
Single fatality ($< 10^{-4}a^{-1}$)	Major damage ($<$ \$100M)	Major effect	Severe (national impact)	4	RR^*_{4A}	RR^*_{4B}	RR^*_{4C}	RR^*_{4D}	RR^*_{4E}
Major injury ($< 10^{-3}a^{-1}$)	Local damage ($<$ \$10M)	Localised effect	Considerable impact	3	RR^*_{3A}	RR^*_{3B}	RR^*_{3C}	RR^*_{3D}	RR^*_{3E}
Minor injury ($< 10^{-2}a^{-1}$)	Minor damage ($<$ \$1M)	Minor effect	Minor impact	2			RR^*_{2C}	RR^*_{2D}	RR^*_{2E}
Slight injury ($< 10^{-1}a^{-1}$)	Slight damage ($<$ \$100k)	Slight effect	Slight impact	1				RR^*_{1D}	RR^*_{1E}
No injuries	No damage	No effect	No impact	0					

If for accident scenario considered the risk understood as combination of consequence and frequency is non-tolerable (it is situated e.g. in cells: 5C, 5D, 5E, 4D, 4E, 3E), it means that the risk is not tolerable and should be reduced with the required risk reduction (RR), e.g. RR^h_{5D} for health (h) consequence or RR^e_{5D} in case of environmental (e) consequence. If such intolerable risks will be reduced for required RR using

a safety function to be designed according to *functional safety* concept [22, 23], the safety integrity level (SIL) required for this function is to be determined according to Table 2.

Table 2. Safety integrity level (SIL) to be determined for a safety function of required risk reduction (RR) and related PFD_{avg} criterion for safety-related system (E/E/PE or SIS)

Required risk reduction (RR)	Probability of Failure on Demand average (PFD_{avg}) for safety functions	Safety Integrity Level (SIL)
RR = 10	$PFD_{avg} \leq 10^{-1}$	SIL1
RR = 100	$PFD_{avg} \leq 10^{-2}$	SIL2
RR = 1000	$PFD_{avg} \leq 10^{-3}$	SIL3
RR = 10000	$PFD_{avg} \leq 10^{-4}$	SIL4

3.4. Cyber security requirements in the context of functional safety

Security level (SL) provide a qualitative approach to addressing security for a ICS zone [24]:
SL 1 for protection against casual or coincidental violation
SL 2 for protection against intentional violation using simple means with low resources, generic skills and low motivation
SL 3 for protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4 for protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation
In the standard IEC 62443 three categories of SLs are distinguished:
SL-C (*Capability*) A particular component or system is capable of being configured by an asset owner or system integrator to protect against a given type of threat.
SL-T **(***Target*) The asset owner or system integrator has determined through a risk assessment that they need to protect this particular zone, system or component against this level of threat.
SL-A **(***Achieved*) The asset owner, system integrator, product supplier and/or any combination of these has configured the zone, system or component to meet the particular security requirements defined for that SL.
According to this cyber-security concept, using in practice more effective countermeasures (technical and/or procedural), should permit to achieve a required level of risk for an acceptable SAL (*Security Assurance Level*) taking into account potential malicious acts (internal or external) and related paths of attacks. It requires careful identifying and classifying risks for each zone in the control system (IACS) for identified threats and vulnerabilities and range of potential consequences. The objective is to assign rationally to each security zone and information conduits required target SAL ranging from 1 to 4, similarly as required SIL in case of functional safety [22, 23].
Achieving required level of SIL of each safety function has to be then verified for considered system architecture as described in standards [22, 23] and monographs [33, 34]. Integrated approach concerning verification of SIL and SAL for the control system architectures of interest has been proposed in publications [33, 36, 39]. Below a method for evaluating SAL is outlined.

The assessment of *security level* (*SL*) is based on seven *foundational requirements* (*FRs*) [24]:
FR 1 Identification and authentication control (IAC),
FR 2 Use control (UC),
FR 3 System integrity (SI),
FR 4 Data confidentiality (DC),
FR 5 Restricted data flow (RDF),
FR 6 Timely response to events (TRE), and
FR 7 Resource availability (RA).
Instead of compressing *SL* down to a single number, it was proposed to apply a vector of *SL* that uses the seven *FRs* specified above. Such vector allows definable separations between *SL* and different *FRs*. Thus, a vector is used to describe the security requirements for a *zone, conduit, component, or system* instead of a single number. This vector may contain either a specific *SL* requirement or a zero value for consecutive foundational requirements. General format of the *security assurance level* (SAL) description is as follows [24]:

$$\text{SL-?}\ ([FR,]\ domain) = \{IAC\ \ UC\ \ SI\ \ DC\ \ RDF\ \ TRE\ \ RA\} \quad (1)$$

where:
SL-? = *(required)* the SL type: possible formats are: SL-T = *Target* SAL, SL-A = *Achieved* SAL, and SL-C = *Capabilities* SAL,
[*FR*,] = *(optional)* field indicating the *FR* that the SL value applies; *FRs* can be written out in abbreviated form instead of numerical form for better readability,
domain = (*required*) is applicable domain that SL applies; in the standards development process, this may be *procedure*, *system* or *component* - when applying the SL to a system, it may be for instance: *Zone A*, *Pumping Station*, *Engineering Workstation*, etc.

Some examples according to the standard [24]:
(a) SL-T (Control System Zone) = {2 2 0 1 3 1 3},

(b) SL-C (Engineer. Workstation) = {3 3 2 3 0 0 1},
(c) SL-C (RA, Safety PLC) = {4}.
In example (c) only the RA component is specified, of a 7-dimension SL-C.

If *achieved* SAL < *target* SAL, then some additional countermeasures are requested. The countermeasures to apply for increasing SAL include:
- *technical measures* (antivirus, antispyware, firewalls, encryption, virtual private networks - VPN, passwords, authentication systems, access control, intrusion detection and prevention, network segmentation, etc.),
- *organisational measures* (rights management, patch management for system & application, security incident management, training, etc.).

One of the countermeasures that can be considered is a *demilitarized zone* (DMZ) that aims to enforce the control network's policy for external information exchange and to provide external, e.g. untrustworthy sources, with restricted access to releasable information while shielding the control network from outside attacks [11, 20, 39].
In *Table 3* a risk matrix is presented for integrating the functional safety SIL-related requirements and the cyber security SAL-related minimal requirements for distinguished categories of criticality of consequences: four categories of probability, four categories of consequence, and four categories of risk: *very high risk* (VHR), *high risk* (HR), *medium risk* (MR), and *low risk* (LR). It is suggested that the level of SAL should be at least as high as SIL level, otherwise achieving SIL of given *safety function* (SF) is not guaranteed.

Table 3. Risk matrix consisting of requirements for safety integrity level (SIL) and security assurance level (SAL) for distinguished risk categories

SIL & SAL for **risk levels**		Criticality of consequences			
		Minor	*Low*	*Major*	*Severe*
Probability	*High*	***MR*** SIL 2 (SAL2)	***HR*** SIL 3 (SAL3)	***VHR*** SIL 4 (SAL4)	***VHR*** SIL 4 (SAL4)
	Medium	***MR*** SIL 2 (SAL2)	***HR*** SIL 3 (SAL3)	***VHR*** SIL 4 (SAL4)	***VHR*** SIL 4 (SAL4)
	Low	***LR*** SIL 1 (SAL1)	***MR*** SIL 2 (SAL2)	***HR*** SIL 3 (SAL3)	***HR*** SIL 3 (SAL3)
	Rare	***LR*** SIL 1 (SAL1)	***LR*** SIL 1 (SAL1)	***MR*** SIL 2 (SAL2)	***HR*** SIL 3 (SAL3)

3.5. Remarks on business continuity management

The *business continuity management* (BCM) is related to 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 risk level [28]. For effective BCM in an industrial plant the *reliability* and *availability measures* of the process installations and supporting equipment, including the information system and the control system (IACS), are of primary interest for the period of time considered, e.g. one year or five years.
Such measures can be considered as the *key performance indicators* (KPIs) [1] and evaluated for the time of interest. They usually depend strongly on the *maintenance strategy* applied in given industrial plant. As it was mentioned developing the *proactive / preventive maintenance strategy* is nowadays of special interest, especially when the Industry 4.0 idea is to be implemented in such plant.
Thus, the BCM can be considered as holistic management process that identifies potential hazards and threats to an organization including negative impacts to business operations that those hazards and threats, if realized, might cause. It should provide a framework for building organizational resilience with the capability of effective response to abnormal situations and hazardous events to avoid or mitigate potential losses [28].
Today, one of the most important objective for any organisation should be to ensure a high economic effectiveness to be achieved by implementing a proactive BCM *system*. It concerns also the industrial hazardous plants that should be designed and operated to reach possibly high reliability and availability measures, and mitigating effectively the safety and security-related risks. Basic requirements for setting up an effective BCM system are specified in the international standard ISO 22301.
In next chapter selected KPIs are reviewed that potentially are of interest in designing a *proactive management system* that include the *business continuity management* (BCM) and *integrated safety & security management* (IS&SM).

4. Tiers and KPIs in proactive process safety management

4.1. Tiers to be considered in process safety management

Lately, considerable effort has been focused on the prevention of potential incidents, and especially major accidents. The *International Association of Oil & Gas Producers* (OGP) has published the Report No. 456 [47] which provides advice on how to implement an *asset integrity management system* for new and existing assets in hazardous plants and installations. It also includes preliminary guidance on monitoring and review of events, and a proposal how to establish the *key performance indicators* (KPIs) to strengthen the risk-related controls, in physical barriers, in order to

prevent incidents and major accidents. Proposed system consists of four tiers as it is shown in *Figure* 8. Two classes of indicators are distinguished, namely: *leading* and *lagging*.
The evaluation concept proposed is similar to that existing in the *layers of protection analysis* (LOPA) methodology [43]. It is assumed below that hazards/threats can be controlled by some *protective barriers* (Bs) or *risk controls (Cs)* to avoid abnormal situations or accidents. They can be multiple within the plant specific *risk control options* (RCOs), proposed in the plant design and then its operation, to be supervised using *process-based management system* [16]. The RCOs can include the layers in protection system, procedures within management system, the physical containment, etc.

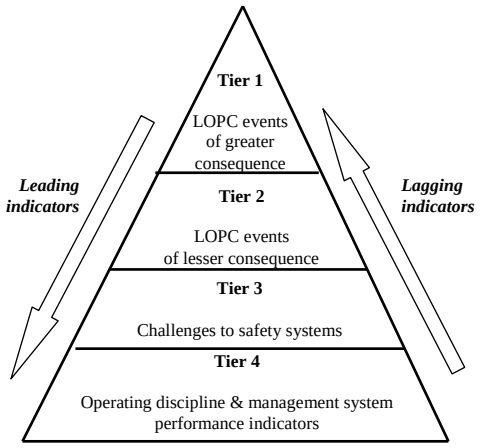

Figure 8. Hierarchy of tiers in an asset management system (based on [47])

Below, the interest is focused on the *loss of primary containment* (LOPC) due to weaknesses of barriers [47, 48], or more generally in *loss of assets integrity* (LAI). It might lead to various consequences, e.g. economic losses because of unplanned plant outages, but also to a major accident with serious consequences. Thus, the LOPC or LAI related events cause losses to: *people* (health of employees and people in the plant surroundings), the *physical assets* including *infrastructure*, and *environment* (potential pollutions and losses at site, close to distributed installation, in its surroundings, and in the region). The causes of hazardous events and their consequences are usually classified into several categories (see *Figure 9*).
Barriers to be designed and operated to limit consequences can have weaknesses, named often *holes*. Unfavourable alignment of these holes can contribute to the failure of several *prevention barriers* resulting in a *hazardous event*. Potential holes and escalation factors should be controlled to enable reaction on time to limit potential serious harm that could result from a fire, explosion or other destructive incidents.
The risk of a potential hazardous event, i.e. its frequency and consequence, is to be reduced using *mitigation and recovery controls* as it is shown in *Figure 9*. For the hazardous events distinguished in the plant specific risk model some relevant and effective *risk control options* (RCOs) are proposed to be implemented and supervised in life cycle [32, 43, 45].

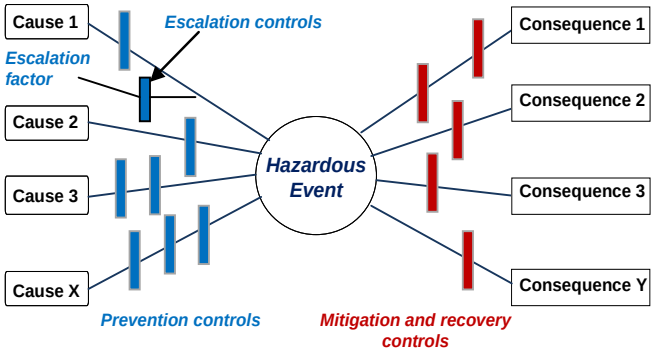

Figure 9. Bow tie diagram illustrating prevention and mitigation controls (based on [26])

4.2. Lagging and leading indicators in four tier model

Because major accidents are relatively infrequent the KPIs evaluated for such rare occurrences may not be fully convincing and useful to prevent future catastrophic incidents. Major incidents are the result of not only one but a combination of failures of the barriers that are designed to control asset integrity. Therefore, KPIs should be proposed for a broader set of more frequent events to be monitored and observed to obtain, if possible, statistically validated data [47]. These are based on observations of unsafe conditions, near misses or activations of safety systems, which can indicate some barrier weaknesses [18]. The data can also include KPIs for monitoring the extent of a company's effort to maintain or strengthen barriers through application of and integrated *health, safety and environment (HSE) management system* that consists of relevant *processes* and *procedures* designed with regard to requirements of a *quality management system* (QMS) [21, 26].
Thus, it is becoming clear that not one but a combination of measures is needed to monitor the *barrier* (B) performance within a process safety management system. To structure such combination of measures, the OGP recommend to apply a four tier framework (see *Figure 8*) with relevant process safety KPIs. In this way the extended dataset from these specific KPIs can be used to monitor proactively relevant events, useful for improving the most critical

safety barriers to prevent serious incidents and major accidents.

Tiers 1 and 2 shown in *Figure 8* are more *lagging measures* and cover asset integrity related to major and less severe incidents. So, Tier 1 and 2 indicators are defined with an intention that those would be reported by the company at the corporate level in both internal and external reports. In order to achieve consistency and comparability, the definitions of indicators should contain the scope and threshold values [47, 48].

Tiers 3 and 4 provide more *leading measures* (see *Figure 8*). The KPIs of these tiers are intended to be much more specific to the company's own management system and often will be specific to a particular activity (e.g. drilling or fuel pumping) or to an individual asset of hazardous plant. The companies may decide to aggregate data from such indicators. However, care should be taken to ensure that similar facilities or activities form the basis for the aggregation, otherwise comparisons may lead to erroneous judgments and decisions [47].

4.3. Hierarchy of asset integrity KPIs

The asset integrity KPIs have been established by some companies to meet three primary needs [18, 47]:

1) Internal monitoring and review of performance related to the *management system* (MS) and other actions to strengthen process safety barriers and reduce risk of incidents and accidents. These KPIs are often considered as fundamental to *continuous improvement* required in any modern *quality management system* (QMS) [26].
2) Assessing whether some measured performance related to the process safety meets or exceeds industry norms by benchmarking KPIs related data against industry sector averages and by sharing good practices and lessons learned together with other companies.
3) Providing transparent disclosure of performance to *stakeholders* such as employees, local communities, investors, governmental and non-governmental organizations, and also the general public. There are some opportunities for companies to communicate and engage with their stakeholders, but one important channel is through regular, typically annual reports, called e.g. as the *sustainability or corporate citizenship reports*.

The process safety KPIs being developed to meet these needs can vary across company's organization from an individual facility up to the corporate level [47, 48]. At the corporate level, data and other information should be selected carefully to be representative for the whole organization when compiled and consolidated to generate meaningful KPIs for decision making. The tier 1 and 2 KPIs are recommended for consolidation at company level for *corporate reporting* against all three needs listed above. In contrast, KPIs of tier 3 and 4 are more appropriate for monitoring *facility performance*, although some may be consolidated at the corporate level to test the management system controls implemented across the whole company.

In *Figure 10* some asset integrity related KPIs data are specified for supporting proactive reliability, safety and security management in a macro-system hierarchy. It is obvious that relevant activities in particular industrial sector, corporation and company are influenced not only by internal, but also by external factors including the state regulatory policy and inspectorate procedures.

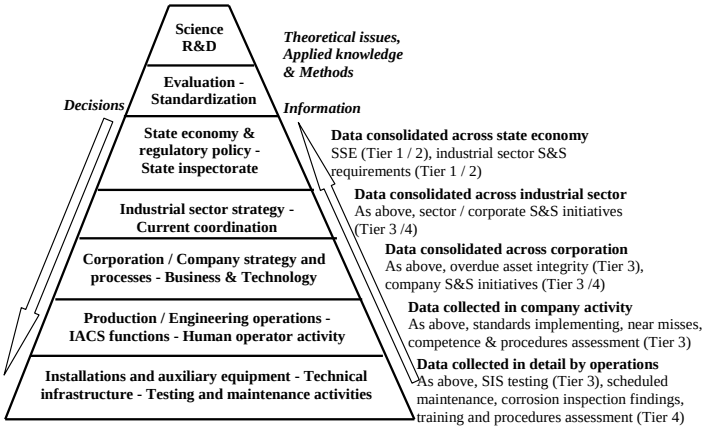

Figure 10. Asset integrity related KPIs data and decisions for proactive safety management in macro-system hierarchy

At the facility level, KPIs should be focused on more leading KPIs within Tiers 3 and 4 to locally assess specific *controls* (C) and *barriers* (B) such as procedural barriers (e.g. during plant start-ups and shut-downs), safety-related systems as functional safety layers (e.g. BPCS, alarm system supporting human operator abnormality awareness and reaction, SISs for automatic emergency shutdown) [22, 23], or people-sensitive barriers depending on a set of *performance shaping factors* [32] that include e.g. procedures and personnel competences with related training and retraining issues [21].

4.4. Selection process of KPIs for monitoring critical barriers

Establishing by the senior management of particular company and selected responsible team of the KPIs for identified categories of *controls / barriers* (C/B) is an essential initial step. It is necessary to ensure that relevant information and data collected will be continuously reviewed at relevant levels, where continuous and proactive improvement actions, are planned as regards technology applied, investments,

prioritization and resources deployment [18, 48]. Thus, the creation of effective *quality management system* (QMS) within the *proactive integrated management system* including the *business continuity* (BC) and *safety & security* (S&S) aspects, with regard requirements of relevant standards, is of primary importance.

The KPI implementation team needs to have clear lines of accountability within the company's management structure and should coordinate the implementation of steps specified in *Figure 11* with special attention on the safety and security management aspects that include the planning of audits, review of data gathering and evaluation of KPIs within periodic decision-making cycle.

The process plant category is determined (Step 1 in Figure 11) based on relevant directives, e.g. the *Control of Major Accident Hazards* (*COMAH*) *regulation* or Seveso III Directive, with regard to current state regulations in area of interest and specific requirements. After identifying more important hazards / threats in particular plant and its critical infrastructure, the periodical review of critical barriers and performance characteristics, including actions undertaken are needed to establish context for further analyses and evaluations (Step 2).

Based on results of the risk evaluation more critical processes are identified useful for determining scenarios of potential incidents and major accidents of higher consequences. To establish Tier 1 and Tier 2 KPIs (Step 3) confirming the criticality and integrity of barriers used on-site for preventing major accidents is required. Examples of Tier 1 and Tier 2 KPIs are described in next chapter.

While the Tier 1 and Tier 2 *process safety events* (PSEs) provide baseline performance information, because the number of events recorded is unlikely to be statistically sufficient or specific enough to assess barrier strength and drive continuous improvement. This is a key reason for implementing Tier 3 KPIs [18, 47]. Typically, Tier 1 and 2 PSEs are established with the standardized definitions within and across companies. These two types of KPIs should be retained year-on-year to provide a consistent record of a company's performance [48].

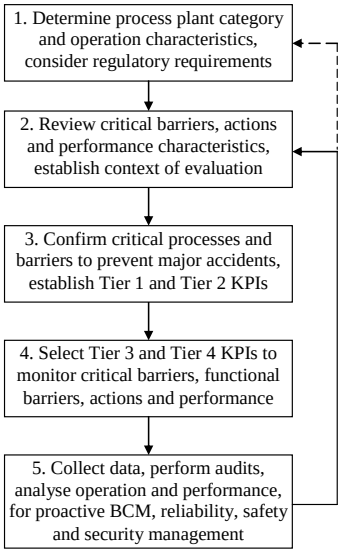

Figure 11. Steps for systematic performance analysis, monitoring and evaluations based on defined KPIs

Companies should select and implement appropriate the Tier 3 and Tier 4 KPIs (Step 4 in *Figure* 7) which would generate statistically relevant performance data that are specific to the critical barriers identified in Step 2. Because these KPIs need to reflect different operational activities and management systems of various facilities, there is a wide choice of Tier 3 and 4 KPIs [18, 47, 48]. Examples of Tier 3 and Tier 4 KPIs are described in next chapter.

It is essential to notice that the effort to collect and analyse the KPI related data (Step 5 in *Figure 11*) should not be directed only at counting the score but rather treated as an integral part of the continuous improvement cycle within a *health and safety management system* or more generally an *integrated management system* suggested in this report, including the safety, security and environmental aspects. In order to have confidence in the results from analyses it is valuable to establish a *quality assurance process* to verify the accuracy, consistency and completeness of data collected [18, 47, 48].

It is important to confirm that process safety KPIs remain focused on the most important barriers to prevent major incidents. While some KPIs, particularly the Tier 1 and 2 measures, are intended to be implemented and established for long-term review of performance, other KPIs may be used for a few years and then evolve to provide more detailed information on barriers strength [47]. Some KPIs should be removed or replaced in time if they do not provide information that enables performance improvement or if they monitor a barrier which is no longer critical. The KPIs should be informative, consistent and their number minimised to reduce

effort and confusion in audits, evaluations and management processes.

5. Examples of KPIs for proactive safety management of industrial installations

5.1. Examples of maintenance related KPIs

Maintenance related KPIs are useful for the reliability and business continuity management. The British / European standard [1] defines several sets of KPIs for the description of *maintenance performance* (MP) of technical assets with regard to *economical, technical and organizational aspects*. Systematic monitoring and appraising of the MP activities based on evaluation of relevant KPIs can significantly improve the equipment reliability and system availability contributing to more economic production being basic interest in an advanced BCM system.

The MP is associated with the utilization of resources in providing actions to retain an item in, or restore it to, a state in which it can perform the required functions. It can be expressed as an achieved or expected result. The MP is usually a complex activity that is dependent on both external and internal influencing factors such as: location, culture, transformation and service processes, size, utilization rate, etc. It is achieved by implementing *corrective, preventive and/or improvement maintenance* using *labour resources, information, materials, organizational methods, tools and operating techniques* [1].

When actual or expected performance is not satisfactory it should encourage the management to define objectives and strategies for improving. The *economic, technical or organizational* aspects are of interest using relevant indicators which allows the organization to [1]:

a) measure the status,
b) evaluate the performance,
c) compare performance,
d) identify strengths and weaknesses,
e) set objectives,
f) plan strategies and actions,
g) share the results in order to inform and motivate people,
h) make optimal investment decisions,
i) control progress and changes over time.

Below selected examples of KPIs are specified describing the MP processes useful in proactive reliability and business continuity management in hazardous process industry and oil port installations.

Examples of *maintenance technical* (MT) KPIs [1]:

- *MT1: Availability related to maintenance,*
- *MT2: Operational availability,*
- *MT3: Number of failures due to maintenance creating environmental damage per year,*
- *MT4: Annual volume of wastes or harmful effects related to maintenance (in the period of one year or 10 years,*
- *MT5: Number of injuries for people due to maintenance per working time,*
- *MT6:Planned / scheduled maintenance time causing production downtime in relation to planned / scheduled total maintenance time,*
- *MT: Mean time to restoration of devices important to continuity of installation operation.*

Examples of *maintenance organisational* (MO) KPIs are as follows [1]:

- *MO1: Number of injuries to maintenance personnel in relation to total maintenance personnel,*
- *MO2: Man-hours lost due to injuries for maintenance personnel in relation to total man-hours worked by maintenance personnel,*
- *MO3: Number of internal multi-skilled maintenance personnel in relation to the number of internal maintenance personnel,*
- *MO4: Immediate corrective maintenance man-hours in relation to total maintenance man-hours,*
- *MO5: Overtime internal maintenance man-hours in relation to total internal maintenance man-hours,*
- *MO6: Number of maintenance internal personnel man-hours for training in relation to total internal maintenance man-hours.*

5.2. Examples of KPIs concerning the automation and control system operation

Using KPIs for *production operations (PO) management* is motivated by the possibility to use them to improve the value creation processes of an enterprise [29]. Within an enterprise, the various operational areas, such as sales, manufacturing, engineering, marketing, and other business support functions, have different sets of performance indicators. Various performance indicators can be used to monitor the realization of enterprise business objectives. The motivation for using KPIs in the PO domain starts with a description of the *value creation processes*. Such KPIs can be useful for description of the *operation technology* (OT) and *information technology* (IT) characterised in *Chapter 2*.

A good KPI should have certain properties which ensure its usefulness in achieving various goals in the manufacturing operations. The KPIs should be evaluated, based on recorded operational information in time having some properties, i.e. if it is possible to be [29]: *aligned, balanced, standardized, valid, quantifiable, accurate, complete, unambiguous, documented, inexpensive*. The use of KPIs has become increasingly important for the success of manufactures to improve their business economics

and management. In addition human performance should be considered in relevant analyses including human-operator interactions with the IACS at relevant levels.

The ISO 22400 focuses on performance measures found to be particularly meaningful for the realization of operational performance improvement. These performance measures can be achieved through combining various measurements from operations and forming what are useful to KPI considered. The monitoring of performance should be focused on identified objectives of the enterprise, and KPIs are most useful when enable to identify trends relative to certain operational objectives.

Below some examples of KPIs for the *production operations* (PO) are specified based on the standard ISO 22400 [29]:

- *PO1: Worker efficiency - the relationships between the actual personnel work time (APWT) related to operation orders and the actual personnel attendance time (APAT) of the employee,*
- *PO2: Utilization efficiency - the ratio between the actual production time (APT) and the actual unit busy time (AUBT),*
- *PO3: Availability - the ratio between the actual production (operation) time (APT)and the planned busy time(PBT) for a operation unit,*
- *PO4: Mean time between failures (MTBF) - the mean of all operating time between failure (TBF) measures for all failure events (FE),*
- *PO5: Mean time to failure (MTTF) - the mean for all time to failure (TTF) measures all failure for all failure events (FE),*
- *PO6: Mean time to repair/restoration (MTTR) - calculated as the mean of all time to repair (TTR) measures for a operation unit for all failure events (FE),*
- *PO7: Corrective maintenance ratio - the corrective maintenance time (CMT) in relation to the total maintenance time expressed as the sum of CMT and planned maintenance time (PMT).*

In industrial hazardous plants some additional aspects are nowadaysimportant, namely the safety and security aspects of the IACS, in context of OT/IT including functions of the BPCS, AS and SIS (see *Figure 1*) that are designed and operated according to functional safety standards [22, 23]. For proactive safety management of these systems following KPIs can be useful in industrial practice:

Basic process Control System (BPCS)

- *BPCS1: Mean time to failure (MTTF),*
- *BPCS2: Mean time to abnormal performance requiring corrective maintenance with testing of subsystems/modules ($MTTF_C$),*
- *BPCS3: Mean time to restoration (MTTR) - calculated as the mean of all time to repair (TTR) measures for a operation unit for all failure events (FE),*
- *BPCS4: Safe failure fraction (S_{FF}) for architectures performing safety function,*
- *BPCS5: Mean time to spurious operation failure ($MTTF_S$) of safety functions,*
- *BPCS6: Period of audits and verifying procedure for functional safety management in life cycle.*

Alarm system (AS)

- *AS1: Alarm rates in normal operation per day (maximum and average),*
- *AS2: Number of alarms following an upset situation per hour,*
- *AS3: Number of alarms following an upset situation per 10 minutes,*
- *AS4: Percentage of hours containing more than 30 alarms,*
- *AS5: Percentage of 10-minute periods containing more than 5 alarms,*
- *AS6:Percentage of time the alarm system is in a flood condition,*
- *AS7: Percentage of alarms when access to procedure is not indicated or ambiguous.*

Safety Instrumented System (SIS)

- *SIS1: The number of demands on the SIS with implemented safety function*
- *SIS2: The time intervals of partial and overall testing of the redundant SIS*
- *SIS3: The number of failures of channels on tests in redundant SIS per month*
- *SIS4: Spurious operation rate of SIS channels per months*
- *SIS5: Average time to dangerous failure of channels ($MTTF_D$) in redundant system,*
- *SIS6: Safe failure fraction (S_{FF}) for subsystems of the safety-related system,*
- *SIS7: Period assumed for verifying technical, organisational and environmental factors influencing common cause failures (CCF),*
- *SIS8: Period for verifying procedure concerning the SIS operation in abnormal or faulty conditions.*

5.3. Examples of Tier 1 and Tier 2 KPIs proposed for hazardous installations

It is suggested in the OGP report [47] that companies implementing the Tier 1 and 2 KPIs should use the RP 754 document as a source document for detailed definitions and guidance. However, this document was developed for the refining and petrochemical industry, and not specifically for the upstream oil & gas industry or transportation of dangerous goods. Therefore, it is proposed in the OGP report to use

relevant threshold values for the amount of material released, e.g. through *Pressure Relief Device* (*PRD*) d*ischarge*, when analyzing Tier 1 and Tier 2 categories, to be based on international UN DG regulations for transport of dangerous materials. It could be also of interest in case of the oil port installations and terminals.

Details how to assume the reference for danger substances are described in several reports and international documents [47, 48]. Below some proposals are described in brief for Tier 1 and Tier 2 KPIs relevant to *process safety event* (PSE) [47]. The *loss of primary containment* (LOPC) or *pressure relief discharge* (PRD) is recordable as PSE when it results in one or more of the consequences, irrespective of the amount of material released.

The performance of *controls/barriers* (C/B) implemented to avoid the *minor consequence registered* (MCR) events with proposed threshold value is suggested to be considered as important KPI:

(1) Fatality or injury to employee or contractor
- *Tier 1 KPI:* Fatality and/or lost workday case - days away from work or *lost time injury* (LTI).
- *Tier 2 KPI:* Recordable occupational injury (restricted work case or medical treatment).

(2) Fatality or injury to third party
- *-Tier 1 KPI:* Fatality, or injury/illness that results in a hospital admission.
- *-Tier 2 KPI:* Informing about PSE and restricted area of admission.

(3) *Impact to the community*
- *Tier 1 KPI:* Officially declared community evacuation or community shelter-in-place.
- *Tier 2 KPI:* Informing about PSE and possible evacuation.

(4) Fire or explosion
- *Tier 1 KPI:* Fire or explosion resulting in greater than or equal to $100,000 of direct cost to the company.
- *Tier 2 KPI:* Fire or explosion resulting in above $10,000 and below $100,000 of direct cost to the company.

Other KPI categories with threshold values for Tier 1 and Tier 2 can be also proposed as suggested in publication [47] these values are proposed for hazardous events of:
- *LOPC material releases,*
- *PRD discharges,*
- *LOPC non toxic material release,*
- *LOPC toxic material release,*
- *LOPC other material release.*

The relevant KPI categories are selected and threshold values determined for particular hazardous plant installation. The *controls/barriers* (C/B) that are designed and operated to keep integrity of installations and functionality of relevant protecting systems are managed in life cycle applying in industrial practice an effective integrated *health, safety / security and environmental management system* using predefined procedures [17, 18, 47, 48].

5.4. Examples of Tier 3 and Tier 4 KPIs for process safety management

Examples of *Tier 3 and Tier 4 KPIs* are as follows[47]:

(A) Management and workforce engagement (MWE) in safety/security asset integrity

Tier 3 KPIs:
- Percentage of manager inspections delegated to subordinates,
- Percentage of safety meetings not fully attended by staff working that day,
- Number of barrier weaknesses, including unsafe conditions, identified from MWE activities.

Tier 4 KPIs:
- Percentage of manager inspections of work locations completed,
- Total hours spent on MWE activities by managers and by staff,
- Percentage of MWE suggestions implemented,
- Staff opinion/attitude survey outcomes on health of asset integrity/process safety barriers, including leadership, competence, safety culture and equipment design.

(B) Hazard identification and risk assessment (HIRA)

Tier 3 KPIs:
- Number of recommendations/actions unresolved by their due date,
- Number of actual or near-miss Loss of Primary Containment (LOPC) events where inadequate HIRA was a causal factor,
- Numbers of P&ID corrections and other actions identified during PHAs.

Tier 4 KPIs:
- Number of planned HIRA completed on schedule,
- Number of planned HIRA before and after changes in the safety and security-related systems,
- Average number of hours per P&ID for conducting (a) baseline PHAs, (b) PHA revalidations.

(C) Operational procedures (OP)

Tier 3 KPIs:
- Number of operational errors due to incorrect/unclear procedures,

- Number of operational shortcuts identified by near misses and incidents,
- Number of PHA recommendations related to inadequate operating procedures.

Tier 4 KPIs:

- Percentage of procedures to be reviewed and updated versus plan,
- Percentage of procedures to be reviewed and updated after changes or corrections within P&ID and/or AS in relation to IACS.

(D) Inspection & maintenance (I&M) focused on equipment critical to asset integrity/process safety

Tier 3 KPIs:

- Number of process leaks identified during operation or downtime,
- Number of temporary repairs or deferred maintenance items in service,
- Percentage of safety-critical equipment that performs to specification when tested was a causal factor.

Tier 4 KPIs:

- Percentage of maintenance plan completed on time,
- Percentage of planned preventative maintenance versus total maintenance (including unplanned).

(E) Safety instrumentation and alarms (SIA) within IACS in relation to alarm system (AS)

Tier 3 KPIs:

- Total number of SIA activations reported by operations,
- Total number of SIA faults reported during tests,
- Average and maximal number of alarms per hour during normal operation, transients and abnormal situations.

Tier 4 KPIs:

- Mean time between alarm activations and operator responses,
- Number of individual SIA tests versus schedule.

(F) Emergency management (EM)

Tier 3 KPIs:

- Number of emergency response elements that are not fully functional when activated in: (a) a real emergency, (b) an emergency exercise.

Tier 4 KPIs:

- Number of emergency exercises on schedule and total staff time involved,
- Percentage of staff who have participated in an emergency exercise,
- Number of emergency equipment and shutdown devices tested versus schedule.

(G) Compliance with regulations & standards

Tier 3 KPIs:

- Number of compliance violations related to asset integrity/process safety & security.

Tier 4 KPIs:

- Percentage of existing standards reviewed as per schedule to ensure evergreen status.

6. Issues of oil port infrastructure proactive safety and security management for mitigation of risks including insurance

6.1. Categories of KPIs proposed for proactive safety and security management

As it has been described above numerous KPIs have been suggested for reliability, safety and security management in hazardous plants. The problem is that KPIs considered for decision making in particular technical system / hazardous plant should be carefully selected to be relevant and effective in specific situation. Selected KPIs to be evaluated should inform adequately about the performance of relevant *controls* / *barriers* (C/B) in particular hazardous plant / distributed critical infrastructure / oil port terminal etc. Below seven steps are described for iterative KPIs defining, monitoring and evaluating in technical system, in particular industrial hazardous plant, to support proactively integrated management including reliability, safety and security aspects:

Step 1. Review current practice in defining, monitoring and evaluating KPIs - in particular technical system or industrial plant.

Step 2. Review existing KPIs and criteria useful for evaluating performance - that have been published in relevant guidelines, reports and regulations, or are defined in existing international standards (see chapter above).

Step 3. Determine functional and integrity requirements for C/B categories of interest in particular technical system - for decomposed facilities / installations that contribute to achieve the *reliability* and *business continuity management* (BCM) objectives, and the *safety* and *security*-related goals in life cycle with regard to expectations of stakeholders.

Step 4. Establish preliminary sets of KPIs for consecutive C/B categories - that potentially influence their integrity with regard to principles of the systemic MTE (*Man-Technology-Environment*) approach.

Step 5. Prioritise KPIs for consecutive C/B categories with regard to opinions of experts and stakeholders - regarding good engineering practices, results of previous technical studies and reports, and experience of insurance company.

Step 6. Eliminate inconsistencies, minimise the number of KPIs and propose a final set of KPIs to be approved by the company Technical Board - establish final set with definitions of KPIs including

measurement principles and frequency, define reporting and audit requirements, and inform owners of relevant processes management system.

Step 7. Evaluate periodically consecutive KPIs to support decision making - taking into account current results of measurements, audits and evaluations required in relevant processes or procedures, and return to relevant step described above according to elaborated change management procedure.

Two categories of KPIs concerning *controls / barriers* (C/B) are distinguished below useful in proactive management including insurance, namely:

A. *Basic KPIs* to be defined and evaluated for wide range of industrial plants,
B. *Complementary KPIs* to be defined and evaluated for safety/security critical industrial plants (e.g. SEVESO / COMAH type) and critical infrastructure systems.

For category A following subcategories of KPIs to be defined are of interest:

A1. Leadership and performance of integrated management system - based on principles, processes/procedures of quality and risk management standards, and systemic MTE concept including legal requirements and sector related directives and regulations, applying good engineering practices in context of highly regarded reports / guidelines and standards,

A2. Organisational culture - human resources and competencies, permits to work and change management, quality and periodic verification of procedures, training / retraining and validation of certificates, involvement of employees in transfer of operational problems to improve procedures and safety related activities, strategy and practice of BCM,

A3. Reliability and safety characteristics of installations - inherent safety properties, the auxiliary systems and protections, redundancy of equipment, the plant availability, layers of protection, inspections and preventive maintenance of technological installations, analyses directed towards avoiding common cause failures (CCF) and systematic failures,

A4. Operational Technology (OT) performance - digital systems and networks, functional safety/security performance criteria (PL/SIL, SAL), hardware and software architectures, HMI interfaces, communication channels, OT performance and security, Electro-Magnetic Compatibility (EMC) properties, testing and calibration of components, quality of procedures, analyses directed towards avoiding common cause failures (CCF) and systematic hardware/software failures,

A5. Information Technology (IT) performance - information storage, transfer and interfaces, communication channels and protection rings, IT performance and security, procedures for cases of hardware/software problems, procedures for the system recovery after failures and cyber attacks,

A6. IACS including AS performance - design requirements and for the DCS/SCADA and *Demilitarized zone* (DMZ), layers and rings of protection of BPCS/SIS for SIL/SAL criteria, quality of HSI interface and procedures, alarm system (AS) design and independence, quality of procedures, operator training/retraining,

A7. Maintenance activities and equipment performance - strategy for the main and auxiliary equipment, monitoring and inspection records, proactive/preventive maintenance based on statistics available and plant specific reliability data, planning of major overhauls,

A8. Evaluation of near misses and minor consequences - periodic analyses of near misses, injuries / fatalities, and abnormal events of minor consequence (MC), identification of causes in systemic context to improve HSE management system and training programme,

A9. Fire monitoring and protection system performance - design requirements, spurious operation records, plans for inspections, tests and preventive maintenance.

For category B following subcategories of KPIs to be defined are of interest related to:

B1. Safety and security culture in organisation - value system, self assessment and shaping, engineering ethics,

B2. Scope of proactive integrated management system (PIMS) - oriented on evaluations of risks, based on processes / procedures and requirements / criteria, covering the quality, occupational health and safety, environmental, reliability, safety and security aspects; PISM audits and improvement plan, management of changes, management of modernisations and investment risks,

B3. Applying concept of leading and lagging indicators - system monitoring, periodical audits and evaluations for tiers: 1, 2, 3 and 4,

B4. Operating procedures - for start-ups, transients, shut-downs, reconfigurations, and maneuvers, training for situations of disturbances and abnormalities,

B5. Emergency procedures - for potential major accidents to limit health, environmental and economic consequences, reaction plans for internal/external fire brigade, coordination rules and responsibility, exercise plans, periodic audits,

B6. Evacuation procedures - reaction plans, cooperation with external fire brigade and rescue

team, coordination rules and responsibility, exercise plans.

6.2. Examples of KPIs for proactive safety management of the oil port installations

Examples of KPIs category A for proactive safety management for are presented in *Table 4* with additional explanations below this table.

Table 4. Examples of KPIs of category A for the oil port installations

A	Examples of KPIs
A1	- Number of supervising visits per week/months to the site for checking the personnel/contractor maintenance activities - Scope of periodic reviews by the board of reports concerning the reliability/safety/security-related audits and correction plans - Employee satisfaction rate regarding job, training and position
A2	- Average number of training/retraining hours per employee - Percentage of human recourses spent on training - Employee rate per year contributing to improve the system functionality, reliability and safety
A3	- Number of unplanned outages per months - Number of safety inspections per month - Percentage compliance with corrective maintenance plan
A4	- The number of demands on the SIS with implemented safety function - The time intervals of partial and overall testing of the redundant SIS - The number of failures of channels on tests in redundant SIS per month - Spurious operation rate of SIS channels per months
A5	- Internet proxy server performance including identification of abnormal events and cyber attacks - Mean time between failures (MTBF) of the business sever for all failure events, - Storage utility service availability - Number of unplanned outages of corporate workstations per month
A6	- Mean time to failure (MTTF) of the BPCS for all failure events - Average time of the BPCS corrective maintenance and testing of modules - Alarm rates in normal operation per day (maximum and average) - Number of alarms following an upset situation per hour - Percentage of time the alarm system is in a flood condition
	- Percentage of alarms when access to procedure is not indicated or ambiguous
A7	- Percentage compliance with corrective maintenance plan - Percentage compliance with preventative maintenance plan - Availability related to maintenance - Operational availability - Mean time to restoration of devices important to continuity of installation operation
A8	- Number of near misses reported per year - Lost time due to accidents (including fatalities) - Lost time due to non-fatal accidents and human errors - Lost time injury frequency (LTIF) - Health and safety prevention costs within month
A9	- Mean time to failure of fire detectors for all failure - Testing time interval of smoke and fire detectors - Availability of fire sprinklers - Spurious operation of the fire alarm system - Preventive maintenance interval of the alarm system

In addition, other KPIs of *category A* have been considered to be for evaluating in practice that are specified in *Chapter 5*, concerning mainly the operation and preventive maintenance of safety-related control systems in oil port installations and terminals as follows:
- *Production operations (PO) (A3, A4),*
- *Safety instrumented systems (SIS) (A4),*
- *Basic process control systems (BPCS),*
- *Alarm system (A5, A6),* and
- *Maintenance performance (MP) (A3, A7).*

For hazardous installation that requires defining and evaluating complementary KPIs of category B additional effort is needed to be undertaken within proactive safety management system. For instance, for subcategory B3 examples of KPIs are specified in *subchapter 5.3* (Tier 1 and Tier 2 KPIs) and in *subchapter 5.4* (Tier 3 and Tier 4 KPIs).
For the oil port and its infrastructure the total number of KPIs that have been initially considered for evaluating in practice was around 70 and after prioritisation 55 was selected for final evaluation during periodic audit. These KPIs will be then assigned to mentioned below groups 1, 2 and 3 related to the process of decision making and implementing on site. Such approach is compatible with determining and verifying *terms of conditions* in the insurance process. For higher transparency of decision making

and effectiveness of correcting activities on site it was decided to prioritise the final KPIs into three groups:

Group 1 - KPIs evaluated to have greatest potential to cause performance improvement in particular technical system / industrial plant that require *immediate attention and actions*,

Group 2 - KPIs considered to have significant potential to drive performance improvement that require *attention in medium term*,

Group 3 - KPIs evaluated to have potential for improvement but require *attention in the longer term*.

6.3. Examples of questioning list during an insurance audit related to IT/OT security

Physical Security (PS)
- physical security policy,
- enforcing a clear desk policy at sites,
- physical security measures in place for access to the company data centres or server rooms, i.e. access cards and/or biometric access,
- data retention and destruction policy.

System Security (SS)
- firewalls in place at all external connection points,
- firewall rules, configurations and settings on at least a monthly basis,
- running anti-virus on system network including on all incoming traffic,
- vulnerability management patching policy for security patches (normal and critical),
- time frame for implementation critical patches,
- intrusion prevention, detection or data loss prevention software deployed on workstations and laptops,
- monitoring and reviewing intrusion logs (how often),
- response process and escalation for intrusion alerts,
- expected response time for a critical alert,
- are information security measures built in where software is developed internally or modified?
- completing penetration testing and a code review on all new systems/software before deployment,
- approximate number of servers on the network at site,
- number of locations where servers are located.

Network Assessment (NA)
- is the network externally assessed for penetration tests in last year?,
- is the network internally assessed for penetration tests in last year?,
- DMZ has been configured and tested in last year?,
- have all critical recommendations been implemented?
- if all critical recommendations have not been implemented please provide details of actions to be taken with deadlines.

Remote Access (RA)
- remote access to your corporate network is allowed?
- if yes, do you limit to two–factor authentication only?
- all connecting devices are required to have anti-virus and firewall installed in accordance with the company policy for updates and patching?

Risk Management (RM)
- procedures are available that govern RM?
- have you roles and responsibilities assigned that identify who is responsible for security in your company?
- have you a dedicated technical team responsible for configuring IT security measures?
- do managers ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested?
- is vulnerability management process regularly reviewed?
- are logs maintained that record all changes to information systems?
- do you allocate risk ratings / *Business Impacts* (BI) to your key systems/assets?
- do you have data for classification / categorisation measures in place?
- do you have a written *Incident Response Plan* (IRP) that addresses security breaches or data breaches?
- do you monitor for compliance and assess the adequacy of your information security plans and policies using any specific frameworks?
- are business methodologies and processes reviewed to ensure that information security is taken into account?
- is an approach applied to manage information security based on ISO 27001 and 27005 and their implementation reviewed independently at planned intervals?,
- is an approach applied to manage functional safety and cyber security of the control systems (IACS) based on IEC 61508 and IEC 62443 and their implementation reviewed independently at planned intervals?

6.4. Towards process based management system for industrial plants and oil ports

Organizations are exposed to various sources of risk, which might be characterized into four broad categories [14, 15, 16]:

(1) Safety and security related,
(2) Production / operations,
(3) Commercial / financial, and
(4) Strategic.

For each issue that requires decision making, managers can benefit from adopting a systematic approach to identifying the potential hazards and 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 particular issues or potential abnormal events, 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 in a risk management systematic framework are distinguished [16]:

1. Identify hazards/threats and evaluate and rank risks
2. Identify techniques and strategies to manage risks (*reduction, retention* or *transfer to insurance company)*
3. Implement risk management strategy.
4. Monitor solutions and effectiveness.

Some risks will stem from the culture issues and organizational changes in time. Thus, the implementation of a *proactive management system* requires creative thinking in context of organisational culture issues taking into account challenges in shaping safety and security culture in existing conditions.

An interesting proposal was recently published concerning development and implementation of a *process based management* (PBM) *system* for nuclear energy installations [21]. Some opinions have been expressed that a process based management system enhances traditional quality programs, and, when properly implemented, enables the organization to satisfy external agencies and registrars for certification of known management systems such as ISO 9001 [26], ISO 14001 [27] and other standards, e.g. ISO 31000 [30], and security related standards.

The *process based management system* (PBMS) also ensures knowledge retention and the retention of all important aspects of existing programs, e.g. *quality assurance* (QA) and *quality management* (QM) programs [21]. Thus, the *process management system* can include conventionally formulated requirements and issues:

- Assessing major differences and similarities between QA/QM systems and other existing management systems integrating the objectives of the 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 transitions and changes;
- Assessing the effectiveness of implementation and continually improving.

These will require coordinated activities of experienced specialists to establish and implement an effective PBMS, especially for those who directs, controls and assesses the licensed organization at the highest level. General idea as illustrated in *Figure 12*. 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 achievable high level of reliability, safety and security [16].

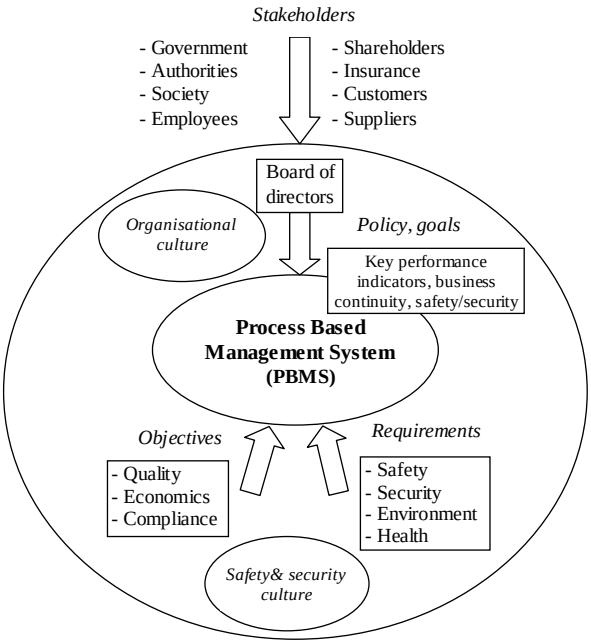

Figure 12. Conditions and requirements for a process based management system

In the PBMS a PDCA (*Plan-Do-Check-Act*) model according to a Deming concept adapted in quality management standard ISO 9001 [26] and risk management standard [30]) is applied that includes four elements to be repeated in circle [16]:

- *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.

A hierarchy of decisions, information flow, documents and activities in a process based management system is presented in *Figure 13.* The strategic decisions concerning of interest organization are made at level 1 taking into account opinions of various stakeholders (see *Figure 12*) and are transferred to lower levels of hierarchy.

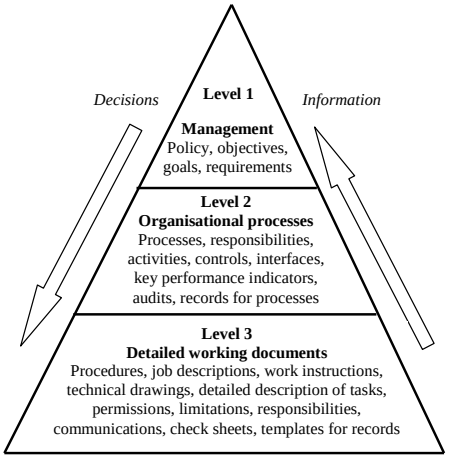

Figure 13. A hierarchy of decisions, information flow, documents and activities in a process based management system

At level 1 general 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 studied including the international conventions [25, 31, 50, 51]. In Poland a decree of Economy Minister concerning requirements for the oil bases and terminals [4] with relevant amendments are of interest.
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) as described in chapter 5. According to rules of the quality management standard for each process the *owner* (responsible specialist) has to be assigned [21, 26, 30].
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 12* (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. At level 3 detailed working document are elaborated as procedure, instructions etc.
Thus, the PBMS specifies various interrelated activities for careful identification of hazards / threats, evaluate related risks as well as describes strategies and tactics to be implemented in life cycle using relevant processes and procedures to reduce risks and control them in time in changing conditions.
Three categories of processes can be distinguished in an organization [21, 26, 30]:
- *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 operational experience, new requirements and changing in time regulations and related legal acts.
Below some examples of business, safety and security related processes and procedures are specified for further development to be proposed as an advanced PBMS:

Executive Processes (EP:)
EP1 Managing the organization and business continuity,
EP2 Managing the processes and procedures,
EP3 Evaluating in time defined 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 cyber security of industrial automation and control systems (IACS), 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 methodological challenges in area of safety and security management of the oil port infrastructure following *procedures* (PR) are of interest for practical implementation:
PR1 Evaluation of indicators, factors and risks relevant to BCM,
PR2 Evaluation of overfill and leak related risks of terminal tanks,
PR3 Evaluation of individual, group/social and operational risks for oil port terminal,
PR4 Evaluation long distance piping operational risks,
PR5 Evaluation of functional safety in life cycle of the control and protection systems for planning tests and preventive maintenance of equipment,
PR6 Evaluation of protection layers including alarm system and HMI (human factors),
PR7 Periodic human task analysis in context of communication and interfaces for supporting Human Reliability Analysis (HRA) to limit human error probability (HEP),
PR8 Periodic integrated safety and security evaluation of Industrial Automation and Control Systems (IACS),
PR9 Staff and personnel recruitment, training and competence management,
PR10 Evaluation of organizational, safety and security culture,
PR11 Defining, evaluating and ranking KPIs and aggregated risk-related factors for development strategy and current tactic of risk reduction, retention and transfer to insurance company.

6.5. Plant specific risk evaluation and mitigation strategy in context of insurance

The KPIs defined in *chapters 4* and *5* are important for proactive safety and security management but are not directly useful for predictive risk evaluation to elaborate risk mitigation plan. They are considered by insurance risk engineers together with other factors, facts and indicators gathered for years in a generic knowledge base for similar industrial plants and business processes. Therefore, the aggregation of information from various sources by the insurance risk engineers and experienced experts is usually made to complement specific information from particular site obtained in an insurance audit.
In Figure 3 some systemic analyses concerning systemic risk evaluation and treatment for considered abnormal or accident scenarios of specific plant of interest are presented. It concerns. Thus, additional effort is necessary evaluate factors, related to the organisation, hardware and environment, to make them useful for the predictive risk evaluation and decision making to mitigate and control in life cycle the individual risk and other risks in context of defined risk criteria (see *chapter 3*). It concerns also the evaluation of insurance risk [5, 6].
The *performance shaping factors* (PSFs) originated from analysis of the *human and organisational factors* and are used in the *human reliability analysis* (HRA) methods [32, 34]. Environmental influences are represented mainly by the *influence factors* (IFs). Selection and aggregation of these factors in predictive risk analysis is based often on *expert opinions*. A conceptual scheme of such aggregation that is traditionally based on the MTE (*Man-Technology-Environment*) concept applied in Formal Safety Assessment (FSA) methodology [12] is presented in *Figure 14*.

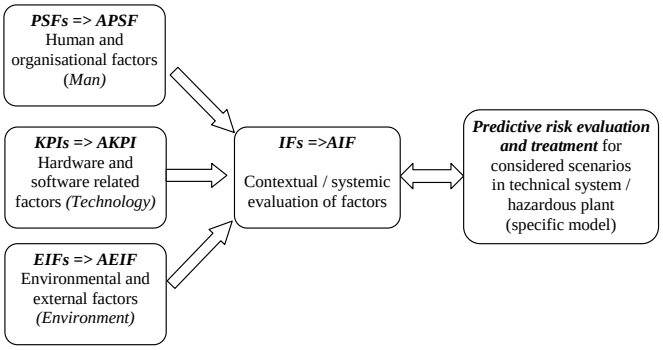

Figure 14. Defining and evaluating of factors for predictive risk evaluation and treatment

The PSFs, KPIs and EIFs (*Environmental Influence Factors*) are to be evaluated by experts to create aggregated APSF, AKPI and AEIF respectively depending on the scopes and objectives of probabilistic modelling developed for the predictive risk evaluation to support safety-related decision making. The evaluation of relevant factors require the weight coefficients to be provided by experts regarding contextual information and possible dependencies between some factors. These *influencing factors* (IFs) are to be further assessed into

aggregated AIF to enable predictive risk evaluation and treatment.

For effective representation and evaluation of the influencing factors a *hierarchical influence diagram* (HID) concept [32] was developed. The number of levels (see *Figure 15*) in particular HID is to be assumed depending on the purpose of evaluations and information suitable in specific modelling. Details of aggregating information in the HID is based on normalized ratings (r) and weights (w) of relevant factors to be aggregated at the levels of interest are described in the monograph [32].

Taking into account principles of the *Formal Safety Analysis* (FSA) methodology of *International Maritime Organisation* (IMO) [12], several levels of such factors can be proposed. For insurance purposes following two levels with relevant influence factors can be considered depending on the evaluation problem (see *Figure 15*):

Direct level

- *Human* – experience, competences, motivation, supporting equipment/tools,
- *Technology and software* – aging, construction, structure (redundancies), parameters, technical state, quality of materials, network/software functionality, protection and security,
- *Environment / surrounding & infrastructure* – vibration, humidity, neighbouring installations, accessibility, shape of land, atmospheric conditions etc.

Organizational level

- *Procedures* - documentation quality, updates, distribution, range),
- *Emergency procedures* - internal and external communication, exercises,
- *Safety & security policy* - safety & security culture, safety & security promotion,
- *Management systems* - BCM, integration of HSSE aspects,
- *Management of change* - requesting of change forms, frequency and quality of audits, etc.,
- *Maintenance and diagnostics* - planning preventive maintenance, supporting tools, spare parts, administrative control and inspections,
- *Competences and communication* - personnel training programs, etc.

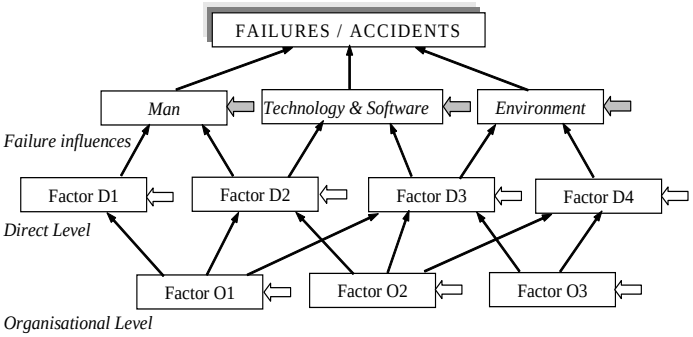

Figure 15. Two levels of factors for evaluation and aggregation using hierarchical influence diagram

Any insurance company has to manage carefully a profile of insured risks in such a way to guarantee profit in longer time horizon. Therefore, it offers an insurance coverage based on careful evaluation of risks in existing conditions of specific industrial hazardous plant to minimize its own risk, before an insurance policy is specified in details for the liability period. The data prepared by the responsible risk engineer during insurance audit on site are considered then by the *underwriter*. Main data sources in the insurance process are shown in *Figure 16*. Lately, the cyber risk challenge and the role of the insurance is emphasised [3].

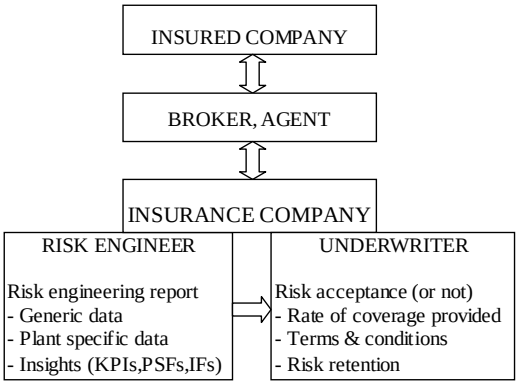

Figure 16. Main data sources in insurance process

Based on relevant information and data gained the underwriter has a task to assess carefully the risk and to evaluate likelihood of a substantial loss. To assess the risk the underwriter uses a list contained in the application form to screen the company to be insured from possible hazards and threats. The underwriter also uses a historical data base to check on the risk exposure, possible past claims, or declined applications in the past. Underwriters follow general rules for the risk classification. For proper risk management some companies assign to their risk management group a selected team of industry experts understanding relevant aspects of the risk analysis that could affect the company financial stability.

Modern insurers that use advanced evaluation methods make final decisions based on an individual risk profile as illustrated in *Figure 17*. The specific (own) risk profile is drawn using quantitative data, preferably plant specific, for defined accident scenarios. The risk results obtained enable more sophisticated decision making in risk management being more tailored to the situation considered. Some methodological aspects of the insurance audit and predictive risk analysis for influence factors identified are presented in monographs [15].

The evaluation of the *probable maximum loss* (PML) and the *estimated maximum loss* (EML) can be of interest rather for plants of moderate complexity. Presently used methods to evaluate risks that are based on the PML or EML do not provide sufficient information about risk profile for underwriting process, because these methods do not take sufficiently into account the probabilities of damages. It is the reason why the risk of less severity damages but occurring more frequently is often underestimated. In the insurance practice the EML or PML can be evaluated by dividing the risk profile to be evaluated into so called complexes [15].

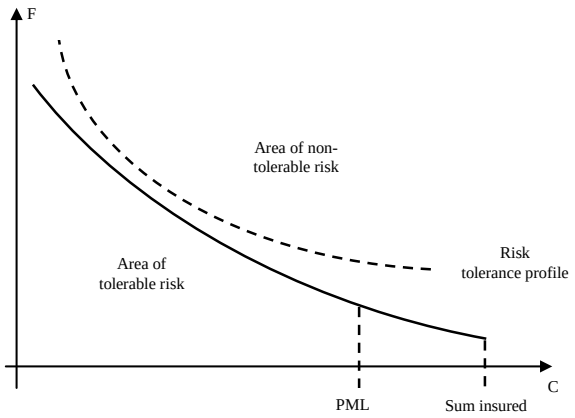

Figure 17. Illustration of the risk profile concept

A new method has been developed for insurance purposes called the *Insurance Risk Analysis Method* (IRAM) [15]. IRAM is a semi-quantitative method of risk analysis based on generic data, knowledge of experts and data gathered during survey. A wide range of specific data concerning the risk factors makes the analysis more specific and therefore, the risk level evaluated is more objective. The presented approach relies on insurance audit done by experts e.g. risk engineers on the site of insured organization and allows to translate specific engineering knowledge into economic language which is more useful for underwriting purposes.

Results of the risk profile for property damage categories distinguished in an industrial plant are illustrated in *Figure 18*. Due to the fact that there are some points of risk above the profile at risk, higher premium should be considered by the *underwriter*, because one of points (no. 2) is localized above risk tolerable profile. It means that some activities must be undertaken in order to reduce risk. Risk engineer is responsible for preparation of recommendations for the case considered taking into account the technical and organizational aspects with support of the cost-benefit analysis (CBA).

The information and data gained during the risk analysis process based on the survey on site, which is to be conducted by risk engineers / experts before preparing the insurance offer, have fundamental meaning. The approach involves also expert opinions based on a systemic acquired in a framework developed that should be as much objective and professional as possible. Expert knowledge concerning personnel operation activities, quality of procedures and using them in practice, facility specification, environmental context, etc. are crucial for risk evaluation.

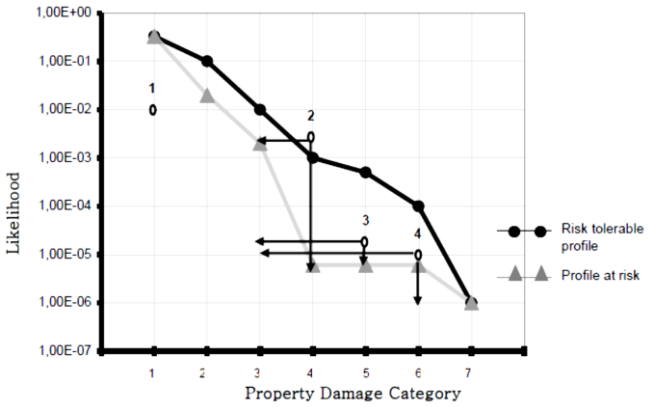

Figure 18. Risk profile and evaluation results for property damage categories

The knowledge of factors influencing significantly the risk level of particular plant to be insured is important for defining the *term of conditions* in the context of the *insurance products* available in the insurance company. If the intrinsic risk level of the hazardous plant is too high, especially as regards risk due to potential major accident and its consequences, the insurer can decline to insure company responsible for operation of such plant. Avoiding of negative selections of such companies / industrial plants of relatively very high level of risk is crucial to limit the insurer own risk, especially in the situation of competitive insurance market.

7. Conclusions

The oil ports play an important role in the energy sector economy and *critical infrastructure* (CI) of the country. There are many requirements, recommendations and guidelines how to design and

operate *hazardous plants* including *oil port installations and oil terminals*. There are also general requirements concerning risk evaluation to support safety related decision making and guidelines concerning competences of persons responsible for safety and security of such systems. An approach is proposed in this report oriented towards *proactive reliability and safety management* and *predictive risk* analysis within *integrated safety and security management* to be compatible with systemic MTE (*man-technology-environment*) concept.

It is especially important in case of hazardous plants and CI systems operating in changing conditions and should include *preventive maintenance* strategy to be elaborated for specific installation and site. The problem should be considered in life cycle from the design stage, and then evaluated periodically during operation, with possible modifying *preventive maintenance strategy* or modernizing installations, especially when innovative technologies are available.

The *industrial automation and control systems* (IACS) contribution to safety and security were of special interest in the report because they play at present an important role in mitigation of risks. These issues have been considered in relation to the Industry 4.0 idea oriented on innovative technologies with advanced OT / IT (*operational technology / information technology*) convergence, and creative initiatives of specialists and activities of supporting staff. The reliability and *business continuity management* (BCM), as well as *integrated safety and security management* are of prime importance in this idea.

The role of *functional safety* and *cyber security* solutions in mitigating relevant risks has been emphasised. The integrated analyses of safety and security related aspects in life cycle management of hazardous plants and oil ports was proposed with regard to the security levels distinguished in Maritime (ISPS Code) Regulations 2014. The influence of technical and organisational factors should be carefully considered in relevant analyses and decision making.

The *integrated proactive safety and security management* system was described that involves systematic application of *polices*, *processes* and *procedures*, and *practices* to activities of communicating and consulting, establishing the context, and monitoring for recording performances of interest to be oriented on evaluating *key performance indicators* (KPIs) relevant to the reliability and safety management. Nine categories KPIs of class A were distinguished and six categories of class B. It was emphasised that KPIs should be informative, consistent and their number should be minimised to reduce effort of proactive reliability safety management.

An approach was also outlined how to evaluate *performance shaping factors* (PSFs), originated from the analysis of the human and organisational factors, and the *environmental influence factors* (EIFs) to obtain aggregated influence factors (IFs) to be of interest in *predictive risk evaluation.* It is also important for the insurer carrying out the insurance audit and risk evaluation of particular hazardous plant / installation for specific performance characteristics and conditions. The insurance company, having experience, statistical data and knowledge about good engineering practices at various sites, can significantly support the safety and security management suggesting more reliable and resilient solutions to hazards / threats identified.

A long term professional cooperation of the company to be insured and the insurer and should contribute to effective mitigating and controlling risks in relevant time horizons. The objective is to evaluate and mitigate risks, and control them proactively, through undertaking appropriate activities within a *process based management system* according to elaborated policy and strategy that includes organisational and technical aspects. Careful planning in this strategy of preventive maintenance activities of sensitive equipment, including tests of protecting equipment, and improving the training programmes should be of high priority.

Careful evaluating and controlling risks is also crucial for any insurance company. Basic activities of the risk engineers and underwriters in the insurance process are outlined in the context of identified hazards/threats and defined factors that significantly influence risks to be considered in evaluating the insurance premium in the context of terms and conditions specified.

Acknowledgments

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] BS EN 15341 (2007). Maintenance - Maintenance Key Performance Indicators. British / European Standard.
[2] Brown M. (2009). Developing KPIs that drive process safety improvement. Hazards SSI, Symposium series No. 155, IChemE. Lloyds Register EMEA, Aberdeen.
[3] CRO Forum (2014). Cyber resilience, The cyber risk challenge and the role of insurance. KMPG Advisory, Amstelveen.
[4] 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 (in Polish). 16.12.2011, Dz.U. No. 276, pos. 1663.
[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[6] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).
[7] Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).
[8] DNV (2001). Marine risk assessment. Offshore technology report 063. HSE books prepared by DNV.
[9] DNV (2013). Risk level and acceptance criteria for passenger ships. European Maritime Safety Agency (EMSA/OP/10), DNVGL.
[10] DNV (2016). Cyber security resilience management for ships and mobile offshore units in operation, Recommended practice, DNVGL-RP-0496.
[11] ENISA (2016). Communication network dependencies for ICS/SCADA Systems, European Union Agency for Network and Information Security.
[12] FSA (1996). Formal Safety Assessment. A methodology for FSA of shipping. International Maritime Organisation.
[13] GE (2016). Top 10 Cyber Vulnerabilities for Control Systems, GE Oil & Gas Digital Solutions, General Electric Company.
[14] 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, pp. 683-687.
[15] Gołębiewski D. (2010). Insurance Audit, Practical methods of risk analysis (in Polish). Poltext Publishers, Warsaw.
[16] Gołębiewski D., Kosmowski K.T. (2017). Towards process based management system for oil port infrastructure in context of insurance. Journal of Polish Safety and Reliability Association, Vol. 8, No. 1, pp. 23-37.
[17] HSE (2000). ADNOC Group Health, Safety and Environmental Management Guidelines. HSE Risk Management.
[18] HSE (2006). Developing process safety indicators, A step-by-step guide for chemical and major hazard. Health and Safety Executive.
[19] HSE (2015). Cyber Security for Industrial Automation and Control Systems (IACS), Health and Safety Executive (HSE) interpretation of current standards on industrial communication network and system security, and functional safety.
[20] HSE (2016). Cyber Security for Industrial Automation and Control Systems (IACS), HSE report for Chemical Explosives and Microbiological Hazard Division (CEMHD) and Energy Division, Electrical Control and Instrumentation (EC&I) Specialist Inspectors.
[21] IAEA (2015). Development and implementation of a process based management system. Nuclear Energy Series Report NG-T-1.3. International Atomic Energy Agency, Vienna.
[22] IEC 61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Parts 1-7. International Electrotechnical Commission, Geneva.
[23] IEC 61511 (2015). Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva.
[24] IEC 62443 (2013). Security for industrial automation and control systems. Parts 1-13 (undergoing development). International Electrotechnical Commission, Geneva.
[25] ISGOTT (1996). International Safety Guide for Oil Tankers & Terminals, International Chamber of Shipping, London.
[26] ISO 9001 (2016). Quality management systems - Requirements. International Organisation for Standardisation.
[27] ISO 14001 (2015). Environmental management systems - Requirements with guidance for use. International Organisation for Standardisation.
[28] ISO 22301 (2012). Societal security - Business continuity management - Requirements. The International Organisation for Standardisation.

[29] ISO 22400 (2014). Automation systems and integration - Key performance indicators (KPIs) for manufacturing operations management, Parts 1 and 2. International Organisation for Standardisation.
[30] ISO 31000 (2018). Risk management - Principles and guidelines. International Organization for Standardization, Geneva.
[31] ISPS Code (2013). Maritime Regulations 2014, Legal notice No. 102, Maritime Transport Decree No. 20 of 2013.
[32] Kosmowski K.T. (2003). Risk analysis methodology for reliability and safety management of nuclear power plants (in Polish). Gdańsk University of Technology Publishers.
[33] 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.
[34] Kosmowski K.T. (2013). Functional safety and reliability analysis methodology for hazardous industrial plants. Gdańsk University of Technology Publishers.
[35] Kosmowski K.T. et al. (2015). Basics of functional safety (in Polish). Gdańsk University of Technology Publishers.
[36] 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, Vol. 6, No. 2, pp. 31-45.
[37] Kosmowski K.T. (2015). Methodological issues of functional safety and reliability assessment of critical systems in hazardous plants. Journal of Polish Safety and Reliability Association, Vol. 6, No. 2, pp. 59-69.
[38] Kosmowski K.T., Śliwiński M. (2016). Organizational culture as prerequisite of proactive safety and security management in critical infrastructure systems including hazardous plants and ports. Journal of Polish Safety and Reliability Association, Vol. 7, No. 1, pp. 133-145.
[39] Kosmowski K.T., Śliwiński M., Piesik E., Gołębiewski D. (2016). Procedure based proactive functional safety management for the risk mitigation of hazardous events in the oil port installations including insurance aspects. Journal of Polish Safety and Reliability Association, Vol. 7, No. 1, pp. 147-156.
[40] Kosmowski K.T. (2017). Cognitive engineering and functional safety technology for reducing risks in hazardous plants. Journal of Polish Safety and Reliability Association, Vol. 8, No. 1, pp. 73-85.
[41] Kosmowski K.T. (2017). Safety Integrity Verification Issues of the Control Systems for Industrial Power Plants. In Advanced Solutions in Diagnostics and Fault Tolerant Control. Springer International Publishing AG 2017 (ISSN 2194-5357), p. 420-433.
[42] Lebecki K. et al. (2013). Integrated methods of occupational, social and environmental risk management for hazards of major industrial accidents (in Polish). Central Mining Institute (GIG - Główny Instytut Górnictwa), Katowice.
[43] LOPA (2001). Layer of Protection Analysis, Simplified Process Risk Assessment. Center for Chemical Process Safety. American Institute of Chemical Engineers, New York.
[44] Mahan R.E. et al. (2011). Secure Data Transfer Guidance for Industrial Control and SCADA Systems. PNNL-20776, Pacific Northwest National Laboratory, Richland.
[45] Markowski A.S. (2017). Safety of industrial processes (in Polish). Lodz University of Technology Publishers.
[46] MARPOL (2005). International Convention for the Prevention of Pollution from Ships, Lloyd's Register Rulefinder.
[47] OGP (2011). Process Safety - Recommended Practice on Key Performance Indicators. International Association of Oil & Gas Producers, Report No. 456.
[48] OGP (2016). Process Safety - Leading Key Performance Indicators. International Association of Oil & Gas Producers, Report No. 556, Supplement to Report 456.
[49] Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).
[50] STCW (1996). International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, International Maritime Organization, London.
[51] UN (2006). Maritime security: elements of an analytical framework for compliance measurement and risk assessment. United Nations, New York and Geneva.