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

PRESENTATION AT HAZARD WORKSHOP ORGANIZED BY PSRA ON 15.02.2019 IN GDYNIA

Project Partner:
Polish Safety and Reliability Association (PL)

Kosmowski Kazimierz T. (GUT)
Gołębiewski Dariusz (PZU)
Oil port installations and the DCS / SCADA system and the control system with implemented safety functions
Scope of presentation

- Functional safety requirements after Buncefield accident
- Legal requirements concerning security of networks and information systems
- OT / IT convergence
- Vulnerability of ICS components
- Risk analysis and management in organisations (ISO 31000)
- Individual and societal risk criteria
- Safety and security evaluation - towards integrated approach
- Functional safety and cyber security analysis
- Systemic MTE approach in safety and security analysis and management
- Towards process based management system
- A and B categories of Controls / Barriers (C/B) for defining KPIs
- Examples of performance indicators to be assessed in insurance audit
- Conclusions
1. The Competent Authority and Operators should develop a common methodology to determine SIL requirements for overfill prevention systems of tanks in line with the principles of EN 61508 / 61511.

2. Protection against loss of containment is required that is physically and electrically separated and independent from the tank gauging system.

3. The safety-related systems should be designed, operated and maintained to achieve and maintain required SIL (safety integrity level) in accordance with the requirements of the standard EN 61511.

4. All elements of an overfill prevention system should be proof tested in accordance with the validated arrangements and procedures sufficiently frequently to ensure that specified SIL is maintained in practice in accordance with the requirements of Part 1 of EN 61511.

5. The sector should put in place arrangements to ensure the receiving site has ultimate control of tank filling. The receiving site should be able to safely terminate or divert a transfer (to prevent loss of containment or other dangerous conditions) without depending on the actions of a remote third party, or on the availability of communications to a remote location.
Legal requirements concerning security of networks and information systems in EU including cyber security of ports

NIS Directive

**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.

- **Maritime (ISPS Code) Regulations** 2014, Legal notice No. 102, **Maritime Transport Decree** No. 20 of 2013.


**NIS**
Network and Information Security

**CERT**
Computer Emergency Response Team

**CSIRT**
Computer Security Incident Response Team

csirt.gov.pl (Poland)
The persons carrying out the assessment shall have appropriate skills to evaluate **security of the port facility**, taking into account 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.

**SOC**

Security Operations Center

**SIEM**

Security Information and Event Management
Assets and infrastructure that should be considered as important to protect (Regulation EC No 725/2004)

- Accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;
- Cargo facilities, terminals, storage areas, and cargo handling equipment;
- Systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks;
- Port vessel traffic management systems and aids to navigation;
- Power plants, cargo transfer piping, and water supplies;
- Bridges, railways, roads;
- Port service vessels, including pilot boats, tugs, lighters, etc.;
- Security and surveillance equipment and systems; and
- The waters adjacent to the port facility.

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.
Typical levels in an industrial process plant and its control system (IACS) in the context of IT / OT convergence

**Company**
- ERP
- MES
- DCS / SCADA / HSI / AS
- PLC / RTU / HMI
- Sensors / Actuators / Conduits
- Industrial equipment
  - Production lines / installations

**Technology evolution - Industry 4.0 concept**
- **INDUSTRY 1.0** Mechanization, steam power, mechanical
- **INDUSTRY 2.0** Mass production, assembly lines, electrical energy
- **INDUSTRY 3.0** Automation, computers, and electronics
- **INDUSTRY 4.0** Cyber Physical Systems, Internet of Things, networks

**OT / IT convergence**
- Manufacturing Execution System
- Distributed Control System / Supervisory Control and Data Acquisition / Human System Interface / Alarm System
- Programmable Logic Controllers / Remote Terminal Units / Human Machine Interface
- Within Industrial Automation and Control System (IACS) e.g. safety related BPCS or SIS

**Main production equipment and auxiliary equipment**
(electrical supply subsystems with protections)

**IT (Information Technology) / OT (Operational Technology)**

**Key terms**
- ERP: Enterprise Resource Planning
- Business analytics, production optimising and intelligence
- MES: Manufacturing Execution System
- DCSC / SCADA / HSI / AS: Distributed Control System / Supervisory Control and Data Acquisition / Human System Interface / Alarm System
- PLC / RTU / HMI: Programmable Logic Controllers / Remote Terminal Units / Human Machine Interface
- Sensors / Actuators / Conduits: Within Industrial Automation and Control System (IACS) e.g. safety related BPCS or SIS
Typical Industrial Control System (ICS) for a large site and Demilitarized Zone (DMZ)

Source: Cyber Security for Industrial Automation and Control Systems (IACS). HSE report for Chemical Explosives and Microbiological Hazards Division (CEMHD) and Energy Division, Electrical Control and Instrumentation (EC&I) Specialist Inspectors.
Problems of ICS computers being attacked in Europe

Percentage of attacked ICS computers in Europe H2 2017 vs H1 2017 (Kaspersky Lab)

Malware classes, percentage of ICS computers attacked, H2 2017 (Kaspersky Lab)
Vulnerability of ICS components

Number of vulnerable products used in different industries ICS-CERT 2017

Distribution of vulnerabilities identified by Kaspersky Lab ICS CERT in 2017 by types of components analyzed

Distribution of vulnerabilities identified by ICS components
Risk analysis and management in organisations (ISO 31000)

PRINCIPLES
Value Creation and Protection

FRAMEWORK
Leadership and Commitment

PROCESS
Scope, Context, Criteria
Risk Assessment
Risk Treatment

Relations between principles, framework and process in the risk management

Risk management process in life cycle

Communication and consultation in context of legal system, good practices, expectations of stakeholders, and criteria for risk evaluation including BCM aspects

Establishing Scope and Context of the risk management processes

Risk assessment
Hazards & threats identification
Preliminary ranking of risks
Risk analysis
Risk evaluation
Risk treatment

Monitoring, recording, reporting and reviewing for proactive safety management with consideration of defined KPIs, PSFs and IFs
Prevention and mitigation controls for reducing risks: probabilities / frequencies and consequences of scenarios (categories for representation of potential accidents)

Based on ISO 31010
Functional safety and cybersecurity analysis within process based management system

Risk analysis and assessment with regard to accident scenarios
Risk acceptance criteria for individual and/or societal risk
Defining the safety functions and determining their required safety integrity
Other risk reduction facilities

Necessary risk reduction / safety of functions
Safety function

- #1
- #2
- #3
E/E/PE safety-related system

- #E1
- #E2
- #E3
Required SIL or HFT of the E/E/PE and SIS subsystems

Verification and validation of consecutive safety functions being implemented by the E/E/PE systems or SISs
Including hardware, software and human factors with regard to potential dependencies and systematic failures

1. Knowledge & methods for hazards analysis and risk evaluation, process safety management (PSM), business continuity management (BCM)

2. Knowledge & methods suitable for the development and usage the quality, environment and safety / security management systems

3. Knowledge & methods for identification of hazards, analyses and assessments of risks; designing the protection layers and rings

4. Knowledge & methods for security analysis of computer systems / networks and software quality/safety management

5. Knowledge & methods suitable for designing interactive HMI/HSI, the control room and alarm system with relevant diagnostics tools

6. Knowledge & methods for assessment of human factors, cognitive task analysis (CTA) and human reliability analysis (HRA)

7. Knowledge & methods supporting cost-benefit analysis (CBA) of risk reduction measures, and scheduling preventive maintenance and overhauls

Sources of knowledge and selected standards

- EN ISO 9241, EN ISO 9001
- EN ISO 14001, EN/IEC 27001, ISO/IEC 27002
- ANSI/ISA 18.02
- EN ISO 31000, 31010
- ISO 45001
- OSHA 3132
- EN ISO 18001
- ISO 22031
- OHSAS 18001
- ISO 28000
- EN/IEC 27001
- EEMUA
- ANSI/ISA 18.02
- NUREG-0700
- HCR, CREAM, HEART
- THERP, SPAR-H
- ALARP
- R^2P^3, TOR
- RCM, RBI, RIMAP
Threshold levels of individual risk considered in ALARP (as low as reasonably practicable) analysis

Based on: ADNOC Group Health, Safety and Environmental Management Guidelines. HSE Risk Management, 2000
### Risk matrix for societal risk assessment and management in the context of functional safety (SIL)

#### Consequences*

<table>
<thead>
<tr>
<th>People – health</th>
<th>Assets</th>
<th>Environment</th>
<th>Reputation</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple fatalities (&lt; 10⁻⁵ a⁻¹)</td>
<td>Extensive damage (≥ $100M)</td>
<td>Massive effect</td>
<td>Catastrophic (international impact)</td>
<td>5</td>
</tr>
<tr>
<td>Single fatality (&lt; 10⁻⁴ a⁻¹)</td>
<td>Major damage (&lt; $100M)</td>
<td>Major effect</td>
<td>Severe (national impact)</td>
<td>4</td>
</tr>
<tr>
<td>Major injury (&lt; 10⁻³ a⁻¹)</td>
<td>Local damage (&lt; $10M)</td>
<td>Localised effect</td>
<td>Considerable impact</td>
<td>3</td>
</tr>
<tr>
<td>Minor injury (&lt; 10⁻² a⁻¹)</td>
<td>Minor damage (&lt; $1M)</td>
<td>Minor effect</td>
<td>Minor impact</td>
<td>2</td>
</tr>
<tr>
<td>Slight injury (&lt; 10⁻¹ a⁻¹)</td>
<td>Slight damage (&lt; $100k)</td>
<td>Slight effect</td>
<td>Slight impact</td>
<td>1</td>
</tr>
<tr>
<td>No injuries</td>
<td>No damage</td>
<td>No effect</td>
<td>No impact</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Probability / frequency [a⁻¹]

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>F_a &lt; 10⁻⁴</td>
<td>Improbable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F_b &lt; 10⁻³</td>
<td>Remote</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F_c &lt; 10⁻²</td>
<td>Occasional</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F_d &lt; 10⁻¹</td>
<td>Probable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F_e ≥ 10⁻¹</td>
<td>Frequent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Required risk reduction

<table>
<thead>
<tr>
<th>RR</th>
<th>Probability of Failure on Demand – average for considered safety function</th>
<th>Safety Integrity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>PFD_{avg} = 10⁻¹</td>
<td>SIL1</td>
</tr>
<tr>
<td>100</td>
<td>PFD_{avg} = 10⁻²</td>
<td>SIL2</td>
</tr>
<tr>
<td>1000</td>
<td>PFD_{avg} = 10⁻³</td>
<td>SIL3</td>
</tr>
<tr>
<td>10000</td>
<td>PFD_{avg} = 10⁻⁴</td>
<td>SIL4</td>
</tr>
</tbody>
</table>

#### Intolerable too high risk

Conditionally tolerable risk - reduction required (ALARP & CBA)

Tolerable risk (periodically reassessed)
The design, operation, periodical testing and maintenance of E/E/PES: Electric / Electronic / Programmable Electronic (E/E/PE) Systems
1. Define the safety functions for reducing relevant risks taking into consideration the results of identification and evaluation of hazards.

2. Determine required safety integrity level SIL (1÷4) of consecutive safety functions based on the results of risk assessment using quantitative risk analysis method or semi-quantitative method, e.g. calibrated risk graph for defined consequences.

3. Design appropriate architecture of E/E/PE safety-related systems or SISs for implementing relevant safety functions.

4. Verify SIL / SAL of safety-related systems using quantitative probabilistic modeling methods for architectures of E/E/PE or SIS designed with regard to architectural constrains - the interval probabilistic criteria for SILs are defined in EN 61508 and EN 61511 standard.

5. Consider security related aspects for the control safety-related systems operating in computer networks with regard to IEC 62443.
The outer ring may include: lighting, fences, entrance/exit points, bollards, intrusion detection sensors and smart alarming, guards on patrol at property fence line, etc.

The middle ring may include: escort of visitors, locked doors, receptionist, access control system, window bars, parcel inspection, turnstiles, etc.

The inner ring may include technical and organizational solutions as: door and cabinet locks, visitor escort policies, emergency communications, secure computer rooms, network firewalls and passwords policy, etc.
Examples of Key Performance Indicators (KPIs) for BPCS, AS and SIS

**Basic Process Control System (BPCS)**

**BPCS-1:** Mean time to dangerous failure (MTTF\(_D\))

**BPCS-2:** Mean time to abnormal performance requiring correction (MTTF\(_O\))

**BPCS-3:** Safe failure fraction (S\(_{FF}\)) for architectures performing safety function

**BPCS-4:** Mean time to spurious operation failure (MTTF\(_S\))

**BPCS-5:** Period of the control room audit and review of functional safety procedures.

**Alarm system (AS)**

**AS-1:** Alarm rates in normal operation per day (maximum and average),

**AS-2:** Number of alarms following an upset situation per hour,

**AS-3:** Percentage of hours containing more than 30 alarms,

**AS-4:** Percentage of 10-minute periods containing more than 5 alarms,

**AS-5:** Percentage of time the alarm system is in a flood condition,

**Safety Instrumented System (SIS)**

**SIS-1:** The number of demands on the SIS with implemented safety function,

**SIS-2:** The time intervals of partial and overall testing of the redundant SIS,

**SIS-3:** The number of failures of channels on tests in redundant SIS per month,

**SIS-4:** Spurious operation rate of SIS channels per months,

**SIS-5:** Safe failure fraction (S\(_{FF}\)) for subsystems of the safety-related system.
**Security level (SL)** concept provides a qualitative approach to addressing security for a **ICS zone**:

**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.

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.
Security Assurance Levels (SALs) in the context of Fundamental Requirements (FRs): target and achieved

**Level Definitions**

1. Casual or Coincidental Violation
2. Intentional Violation Using Simple Means
3. Intentional Violation Using Sophisticated Means
4. Intentional Violation Using Sophisticated Means & Extended Resources

**Foundational Requirements**

- **AC**: Access Control
- **UC**: Use Control
- **RA**: Resource Availability
- **DI**: Data Integrity
- **TRE**: Timely Response to an Event
- **RDF**: Restrict Data Flow
- **DC**: Data Confidentiality

**SAL Vector Format**

\[ SAL ? ([FR], domain) = \{ AC, UC, DI, DC, RDF, TRE, RA \} \]

- **Examples**
  - SAL-T(Control System Zone) = \{2 2 0 1 3 1 3\}
  - SAL-C(Engineering Workstation) = \{3 3 2 3 0 0 1\}
  - SAL-C(RA, Safety PLC) = 4

- **Definition & usage still under development**

Security Assurance Levels (SALs) in the context of Fundamental Requirements (FRs): Target and Achieved (cont.)

If Achieved SAL < Target SAL some additional countermeasures have to be considered in the implementation process.

The countermeasures to be implemented 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.),

- **security management** (rights management, patch management for system & application, security incident management, training, etc.).

One of countermeasures to be considered is a **demilitarized zone (DMZ)** that aims to enforce the control network’s policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the control network from outside attacks.

Integrated functional safety and cyber security analysis of critical systems

**System safety analysis and management**
- Preliminary hazard and risk analysis
- Safety-related requirements and criteria
- Designing / redesigning safety-related functions / protections
- Assessment / reassessments of risk, dependence and importance measures
- Monitoring and data acquisition of failures, procedures of the system operation, planning of tests and maintenance

**System security analysis and management**
- Preliminary threats and vulnerability analysis
- Security-related requirements and criteria
- Designing / redesigning security-related functions / countermeasures
- Assessment / reassessments of risk, vulnerability and interaction measures
- Monitoring and data acquisition of threats, procedures of the system operation, planning of tests and corrections

**Identification of safety and security environments**
- System-oriented approach

**Specification and integration**
- Comparative risk analyses
- Evaluating of operation process - monitoring and assessing in life cycle

**Assessment / reassessments of risk, vulnerability and interaction measures**
- Monitoring and data acquisition of threats, procedures of the system operation, planning of tests and corrections

**SIL & SAL for risk levels**

<table>
<thead>
<tr>
<th>Probability</th>
<th>Minor</th>
<th>Low</th>
<th>Major</th>
<th>Severe</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>MR</td>
<td>HR</td>
<td>VHR</td>
<td>VHR</td>
</tr>
<tr>
<td></td>
<td>SIL 2</td>
<td>SIL 3</td>
<td>SIL 4</td>
<td>SIL 4</td>
</tr>
<tr>
<td></td>
<td>SAL 2*</td>
<td>SAL 3*</td>
<td>SAL 4</td>
<td>SAL 4</td>
</tr>
<tr>
<td>Medium</td>
<td>MR</td>
<td>HR</td>
<td>VHR</td>
<td>VHR</td>
</tr>
<tr>
<td></td>
<td>SIL 2</td>
<td>SIL 3</td>
<td>SIL 4</td>
<td>SIL 4</td>
</tr>
<tr>
<td></td>
<td>SAL 2*</td>
<td>SAL 3*</td>
<td>SAL 4</td>
<td>SAL 4</td>
</tr>
<tr>
<td>Low</td>
<td>LR</td>
<td>MR</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td></td>
<td>SIL 1</td>
<td>SIL 2</td>
<td>SIL 3</td>
<td>SIL 3</td>
</tr>
<tr>
<td></td>
<td>SAL 1*</td>
<td>SAL 2*</td>
<td>SAL 3*</td>
<td>SAL 3*</td>
</tr>
<tr>
<td>Rare</td>
<td>LR</td>
<td>LR</td>
<td>MR</td>
<td>HR</td>
</tr>
<tr>
<td></td>
<td>SIL 1</td>
<td>SIL 1</td>
<td>SIL 2</td>
<td>SIL 3</td>
</tr>
<tr>
<td></td>
<td>SAL 1*</td>
<td>SAL 1*</td>
<td>SAL 2*</td>
<td>SAL 3*</td>
</tr>
</tbody>
</table>
Towards process based management system for an oil port infrastructure

Conditions and sources of requirements influencing a process based management system

A hierarchy of decisions, information flow, documents and activities in a process based management system
Examples of processes to be considered for developing the process based management system (PBMS) e.g. for the oil port infrastructure

Executive Processes (EP):
EP1 Managing the organization and business continuity,
EP2 Managing the processes and procedures,
EP3 Evaluating in time and improving defined KPIs,
EP4 Coordinating external relations including regulators, 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 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.
Examples of procedures (PR) of interest in practical realization of relevant management processes

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, social and operational risks for oil port terminal,
PR4 Evaluation of long distance piping operational risks,
PR5 Evaluation of functional safety in life cycle of the control / protection systems for planning tests and preventive maintenance of equipment,
PR6 Evaluation of protection layers including alarm system and HMI,
PR7 Periodic human task analysis in context of communication and interfaces for supporting Human Reliability Analysis (HRA) and planning training to limit human error probability (HEP),
PR8 Periodic integrated functional safety and cyber security evaluation for life cycle IACS management including testing and preventive maintenance of components,
PR9 Staff and personnel recruitment, training and competence management,
PR10 Audit of organizational culture for shaping safety and security culture,
PR11 Evaluation and ranking KPIs and aggregated factors for development strategy and tactic of the risk management (to specify risks for reduction, retention and transfer to the insurance company).

Remark: Procedures are used as specified and have to periodically reviewed as defined in PBMS, e.g. immediately when changes are introduced.
Key performance indicators (KPIs) for proactive safety & security management

- **Key Performance Indicators (KPIs)** are used to help organizations understand how well they are performing in relation to their strategic goals and objectives.

- KPIs provide the most important performance information that enables organizations and their stakeholders to understand whether the organization keeps track in realization of relevant activities and processes or not.

- The goal is to develop a set of KPIs for given organization to reduce the complex nature of organizational performance to a small number of key indicators in order to make the management problem more understandable and transparent for decision making.

- KPIs can be counted and compared; it provides evidence of the degree to which an objective is being attained over a specified time. The issue is whether to use *qualitative or quantitative metrics*.

- Due to complexity of real technical systems the evaluations are often most powerful for decision making when the analysts use *both qualitative and quantitative metrics*. 
Category A of Controls / Barriers (C/B) for defining KPIs

A1. Leadership and integrated management - based on systemic MTE approach,
A2. Organisational culture - human resources and competencies, permits to work and change management, procedures and training,
A3. Design, modernisation and performance of installations - including infrastructure and protections, redundancy and separation of equipment,
A4. Operational Technology (OT) - operational control and interfaces, OT performance, safety and security,
A5. Information Technology (IT) - information storage, transfer and interfaces, IT performance, safety and security,
A6. IACS design and performance - requirements / criteria for functional safety (PL/SIL) and security (SL, SAL) solutions,
A7. Alarm system (AS) - design concept and performance, procedures and operator interface and training,
A8. Maintenance - including calibrations, functional tests and preventive maintenance based on statistics available and plant specific reliability data,
A9. Evaluation of near misses and abnormal states of minor consequence registered (MCR), injuries / fatalities,
A10. Fire monitoring and protection system - design concept, inspections, tests and preventive maintenance.
For hazardous plants (e.g. SEVESO / COMAH type) additional C/B categories are proposed to be considered for defining relevant KPIs:

**B1. Safety and security culture in organisation,**

**B2. Integrated management system (IMS)** - 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; ISM audits and improvement plan,

**B3. Leading and lagging indicators** - for tiers: 1, 2, 3 and 4,

**B4. Emergency and evacuation procedures and exercise plan.**
Examples of KPIs for B3 subcategory

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 case).

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 (process safety event) and restricted area of admission.

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.
Examples of security related performance indicators to be assessed in an insurance audit of oil port infrastructure

**Physical Security (PS)**
- physical security policy,
- enforcing a clear desk policy at sites, etc.

**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, etc.
- intrusion prevention, detection or data loss prevention software deployed on workstations and laptops,
- monitoring and reviewing intrusion logs (how often),
- expected response time for a critical alert,

**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?

**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 safety and 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?
Towards systemic MTE approach in safety and security analysis and management in life cycle

- **KPIs => AKPI**
  - Hardware and software related factors (Technology)

- **IFs => AIF**
  - Contextual / systemic evaluation of factors

- **EIFs => AEIF**
  - Environmental and external factors (Environment)

**Predictive risk evaluation and treatment** for considered scenarios in technical system / hazardous plant (specific model)

**FAILURES / ACCIDENTS**

- **Man**
- **Technology & Software**
- **Environment**

**Failure influences**

**Direct Level**
- **Factor D1**
- **Factor D2**
- **Factor D3**
- **Factor D4**

**Organisational Level**
- **Factor O1**
- **Factor O2**
- **Factor O3**
Evaluation of risks to be transferred to the insurance company (in context of insurance products available)

**Risk engineering report**
- Generic data
- Plant specific data
- Insights (KPIs, PSFs, IFs)

**Risk acceptance (or not)**
- Rate of coverage provided
- Terms & conditions
- Risk retention

**Scenarios considered**

---

![Diagram showing risk acceptance profile and scenarios considered]
The oil port reliable operation is crucial for the energy sector economy and state critical infrastructure (CI). There are numerous requirements, recommendations and guidelines how to design and operate hazardous plants and oil ports, with relevant installations and infrastructure, integrating in decision making the safety and security aspects.

Due to complexity of systems considered and many factors involved it is necessary to apply in practice a process based management system (PBMS) including business continuity management (BCM) and integrated safety & security (S&S) aspects.

The PBMS takes advantage of evaluating risks and KPIs with regard to quantitative and qualitative information (aggregation of expert opinions) to support effectively decisions concerning reliability, safety and security in an integrated way.

The methodology proposed is focused on the evaluation of IACS (Industrial Automation and Control Systems) and IT/OT convergence indicating how to integrate in evaluations the functional safety (EN 61508) and cyber security (IEC 62443) aspects. The approach is compatible with the Industry 4.0 concept being implemented nowadays in practice.

The insurance company point of view has been also considered, because nowadays the insurer, interested in decreasing risks, offers the expertise how to limit effectively some risks in life cycle from the design conceptual stage of hazardous plant, through its reliable and safe operation, until decommissioning.
Details are given in Journal of Polish Safety and Reliability Association – JPSRA, Special Issue on HAZARD Project, Volume 10, No 1, April 2019

Slides below illustrate Laboratory LINTE^2 at Gdańsk University of Technology (GUT) 
https://eia.pg.edu.pl/linte/main

designed and available at present for making experiments in the domain of critical infrastructure - electric power systems using advanced DCS/SCADA system for verifying and validating control/protection algorithms with regard security aspects to limit the network vulnerability
Basic information about the project

- **Finanse source:** POIG
- **Budget:** funding POIG 46,220 mln PLN, overall costs **50,953 mln PLN**
- **Goal:** construction of a new laboratory for R&D in area of electric power systems
- **Completion of the investment:** 31 December 2015
- **Starting operation:** 12 April 2016
Elements of the research installation

Control system and communication conduits

- 9 control rooms with operator workstations and SCADA software (remote supervising, development and initiating algorithms, on-line control, configurations, etc.)
- Controllers of functional units (SJF) remotely programmed from engineering stands (Simulink Real Time)
- 70 digital protection relays programmed from engineering stands
Main hall of the laboratory
Functional units

- Autonomus energy sources:
  - Solar power station 33 kW
  - 2 generating sets 80 kW with Diesel engines
  - gas microturbin 65 kW
Design of experiments