INTEGRATED APPROACH FOR FUNCTIONAL SAFETY AND CYBER SECURITY MANAGEMENT IN MARITIME CRITICAL INFRASTRUCTURES

PRESENTATION AT HAZARD WORKSHOP ORGANIZED BY PSRA ON 15.02.2019 IN GDYNIA

PROJECT PARTNER:

POLISH SAFETY AND RELIABILITY ASSOCIATION (PL)

MARCIN ŚLIWIŃSKI (GUT)

EMILIAN PIESIK (GUT)

Overview

- Introduction.
- Challenges and topic overview.
- Procedure of functional safety and cyber security management in selected maritime critical infrastructure.
- Functional safety analysis including cyber security aspects:

  - determining safety integrity level with cyber security;

  - verifying safety integrity level including security aspects.
- Case study e.g. critical maritime infrastructure:

  - functional safety analysis with regard cyber security on example distributed industrial control system ICS;

  - project control and protection systems - verifying SIL including cyber security aspects.
- Summary.

Probabilistic criteria

Probabilistic criteria for the E/E/PE safety-related functions/systems:

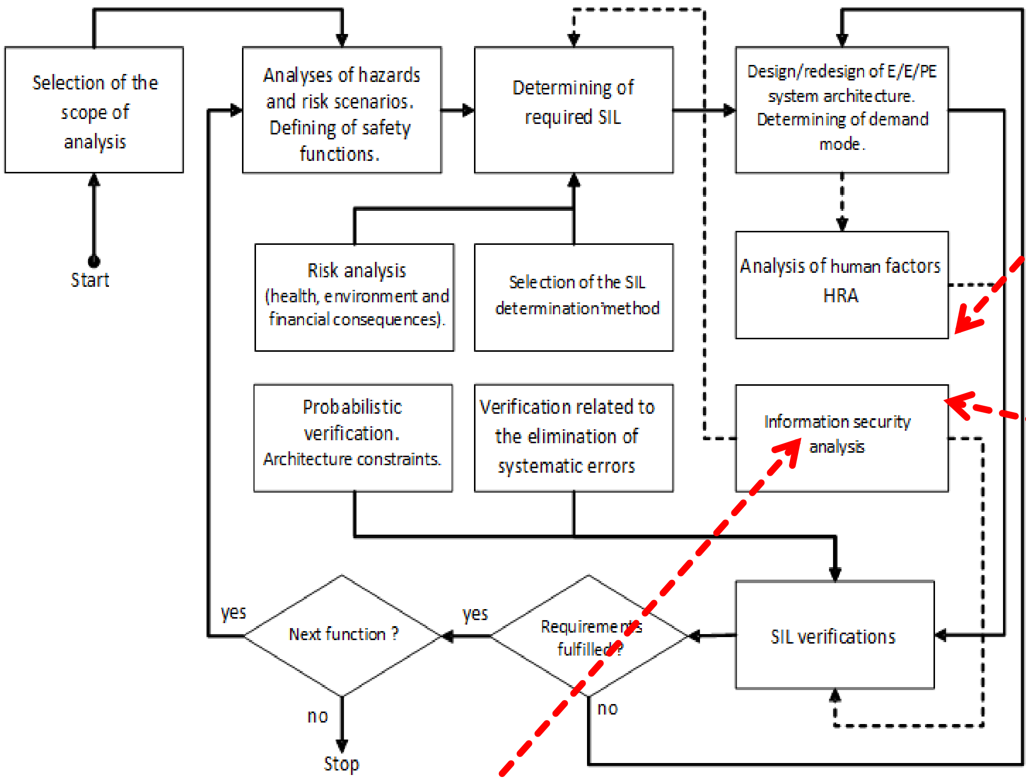
SIL	PFD_{avg}	PFH
4	$[10^{-5}, 10^{-4})$	$[10^{-9}, 10^{-8})$
3	$[10^{-4}, 10^{-3})$	$[10^{-8}, 10^{-7})$
2	$[10^{-3}, 10^{-2})$	$[10^{-7}, 10^{-6})$
1	$[10^{-2}, 10^{-1})$	$[10^{-6}, 10^{-5})$

SIL – safety integrity level;

PFD_{avg} – average probability of failure to perform the design function on demand for the system operating **in low demand mode of operation**;

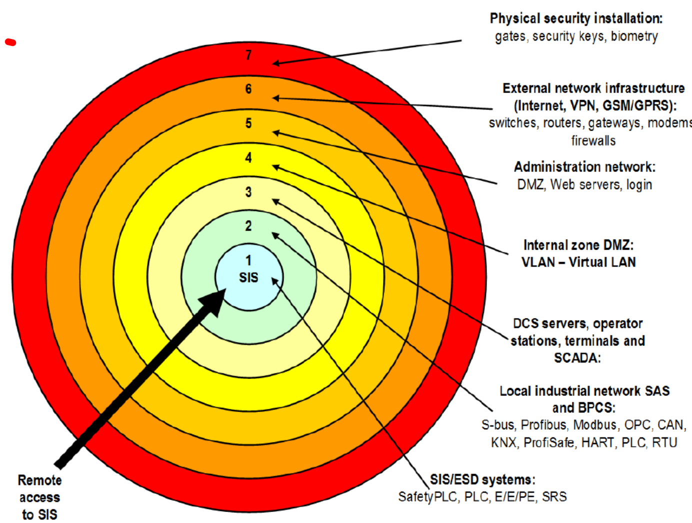
PFH – probability of dangerous failure per hour (the frequency) for the system operating **in high demand mode operation or continous.**

Functional safety analysis procedure with the cyber security aspects



Levels of security and corresponding EALs

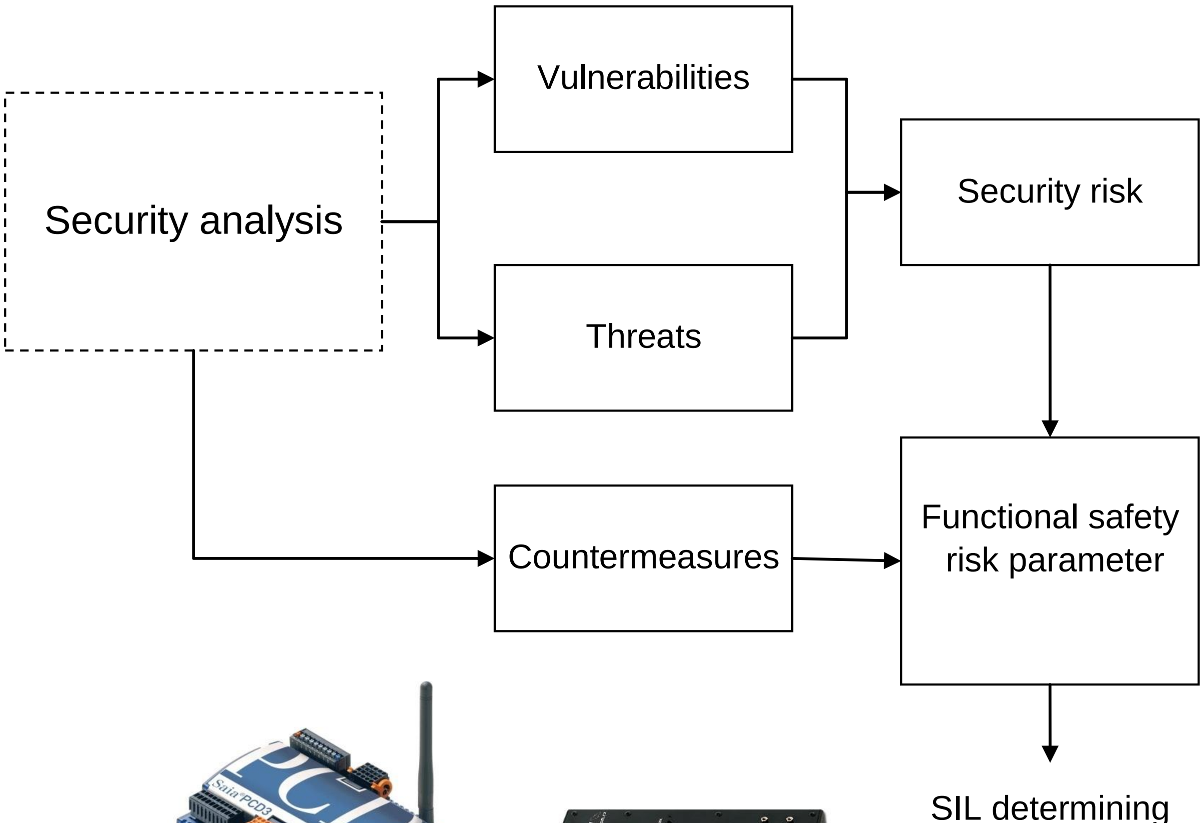
Evaluation assurance level	Level of security
EAL1	Low level
EAL2	Low level
EAL3	Medium level
EAL4	Medium level
EAL5	High level
EAL6	High level
EAL7	High level



$$SAL = \{ AC \quad UC \quad DI \quad DC \quad RDF \quad TRE \quad RA \}$$

AC - identification and authentication control; UC - use control; DI - data integrity;
DC - data confidentiality; RDF - restricted data flow; TRE - timely response to event; RA - resource availability.

Procedure using cyber security factors in functional safety analysis



Categories of distributed process control and protection systems

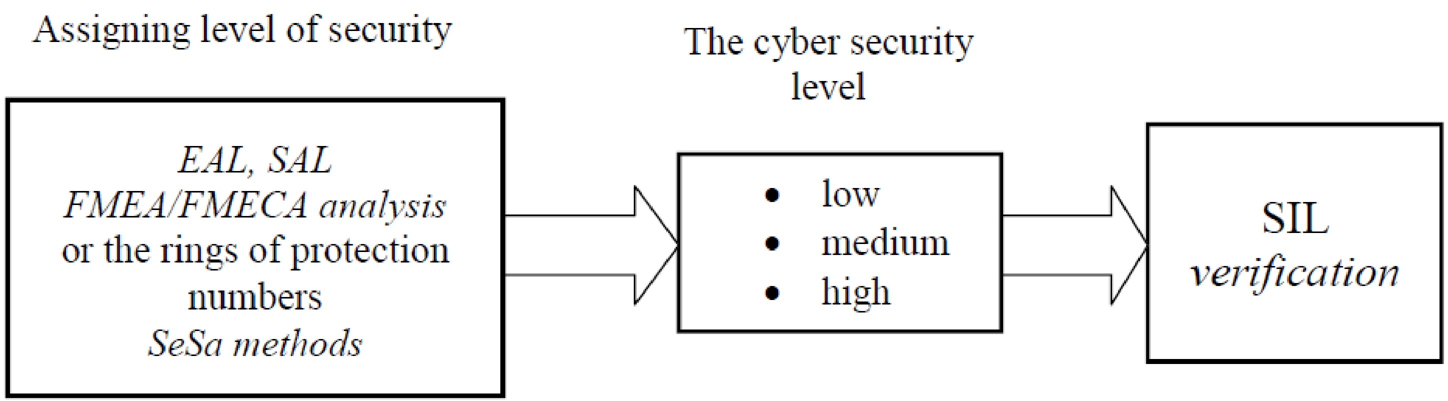
Classification of the process control and protection systems:

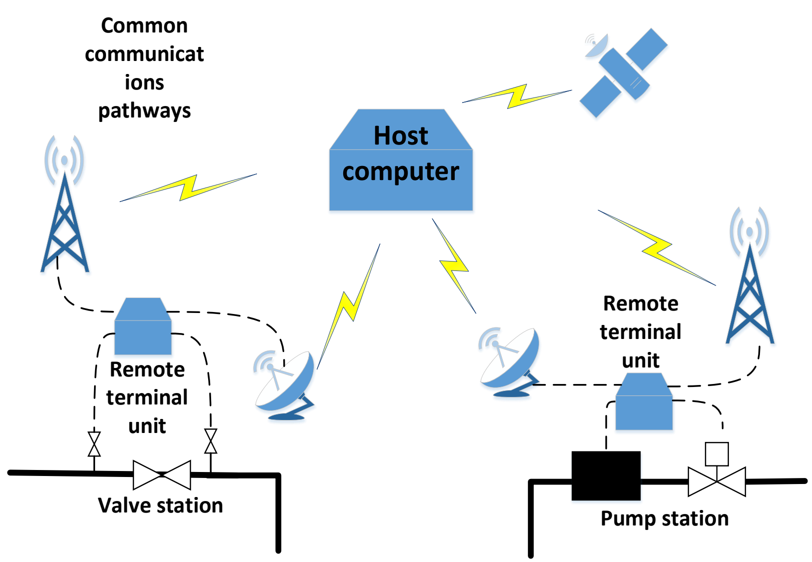
I. Systems installed in concentrated critical objects using only the internal communication channels (e.g. local network LAN),

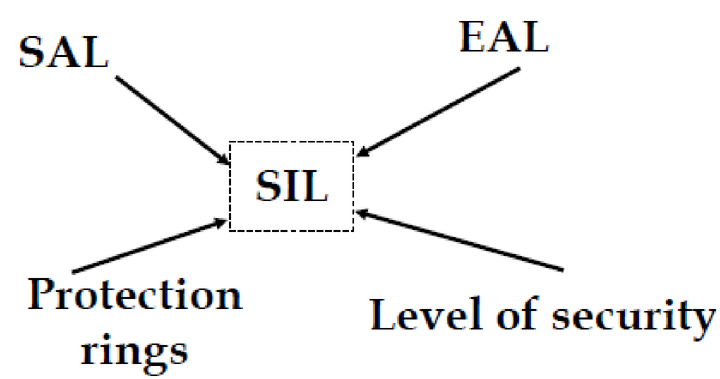
II. Systems installed in concentrated or distributed critical plants, where the protection and monitoring system data are sent by internal communication channels and can be sent using external channels,

III. Systems installed in distributed critical instalations, where data are sent mainly by external communication channels.

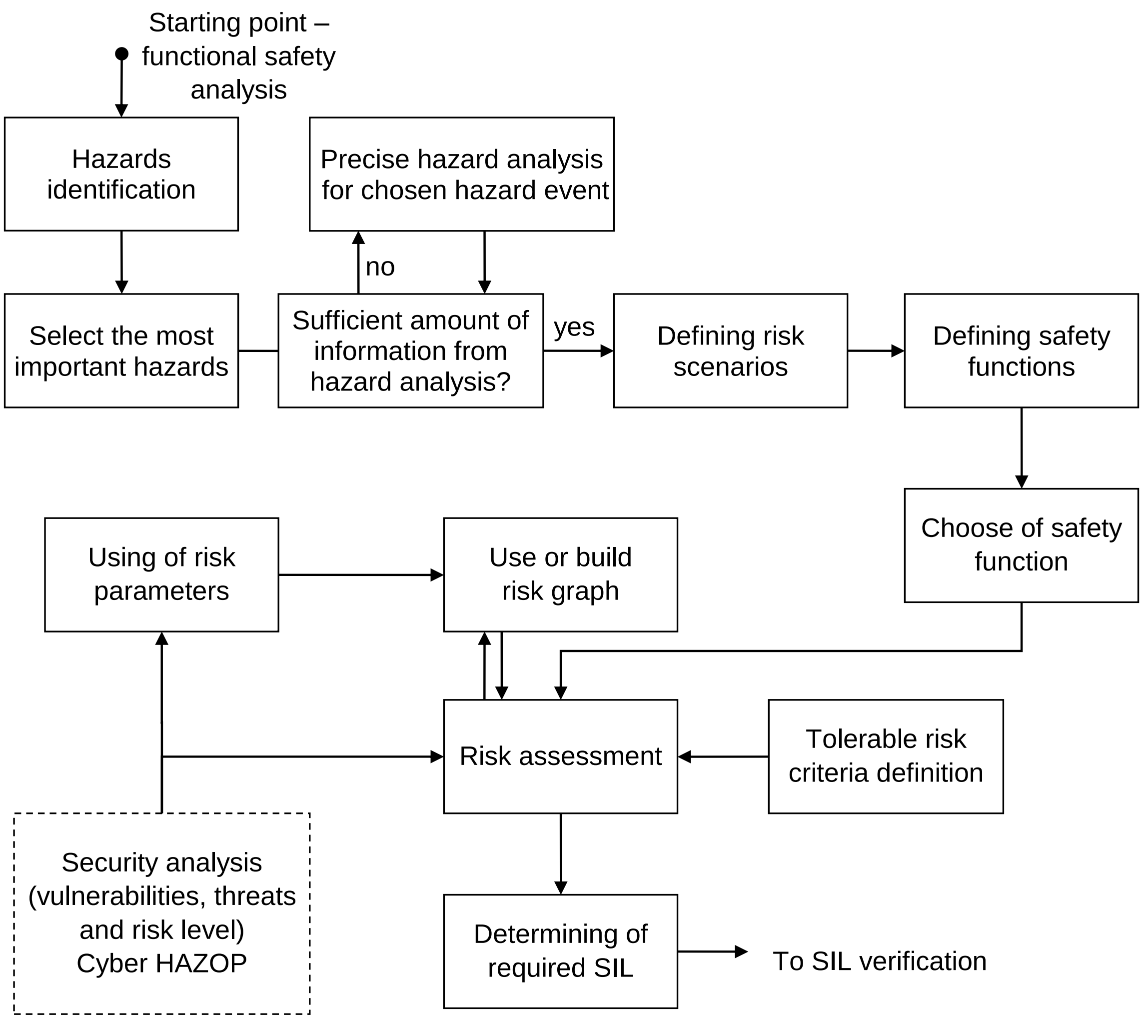
Assigning level of cyber security in industrial network







A general procedure of SIL determining with cyber security

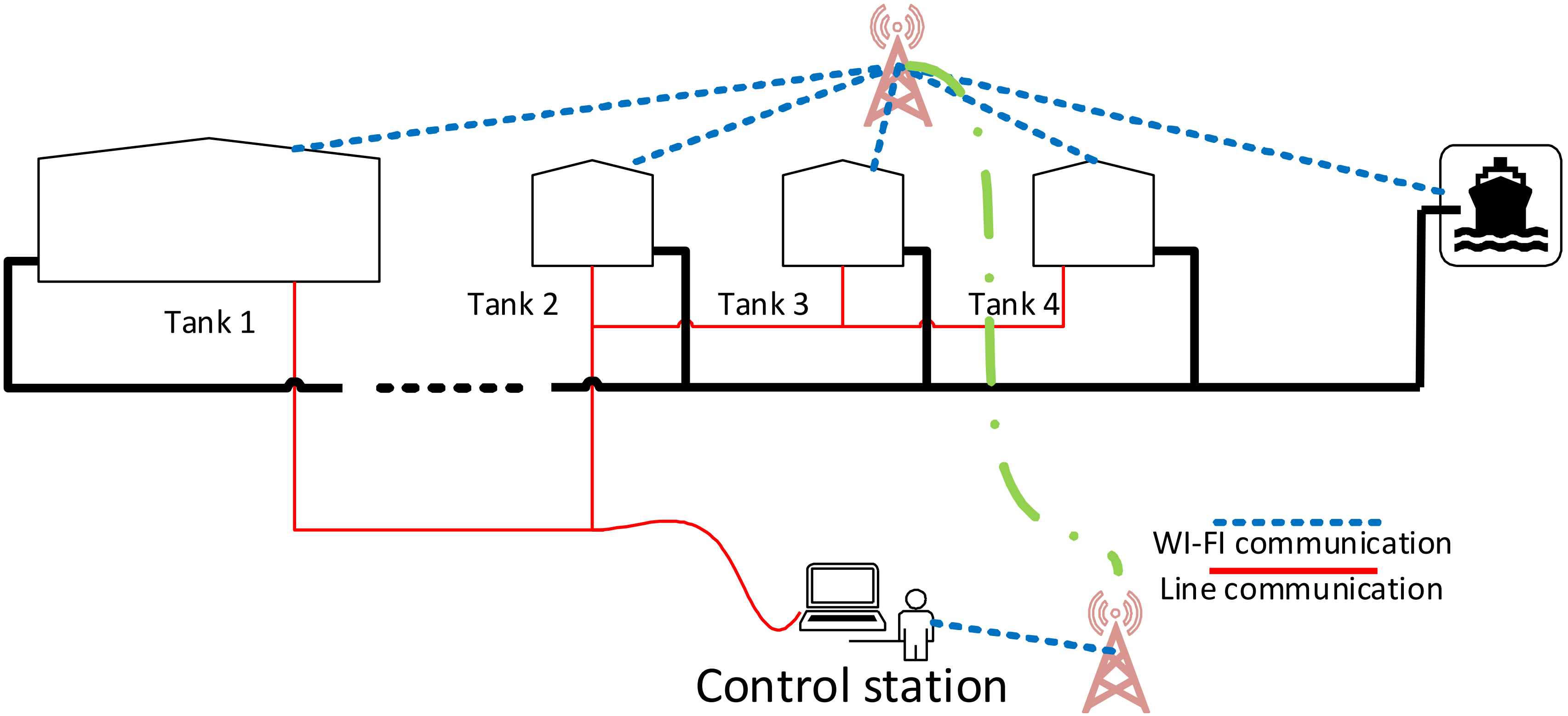


Concept of Central Sea Port Gdańsk(2019-2027) e.g. Critical maritime infrastructure

source: www.gospodarkamorska.pl/

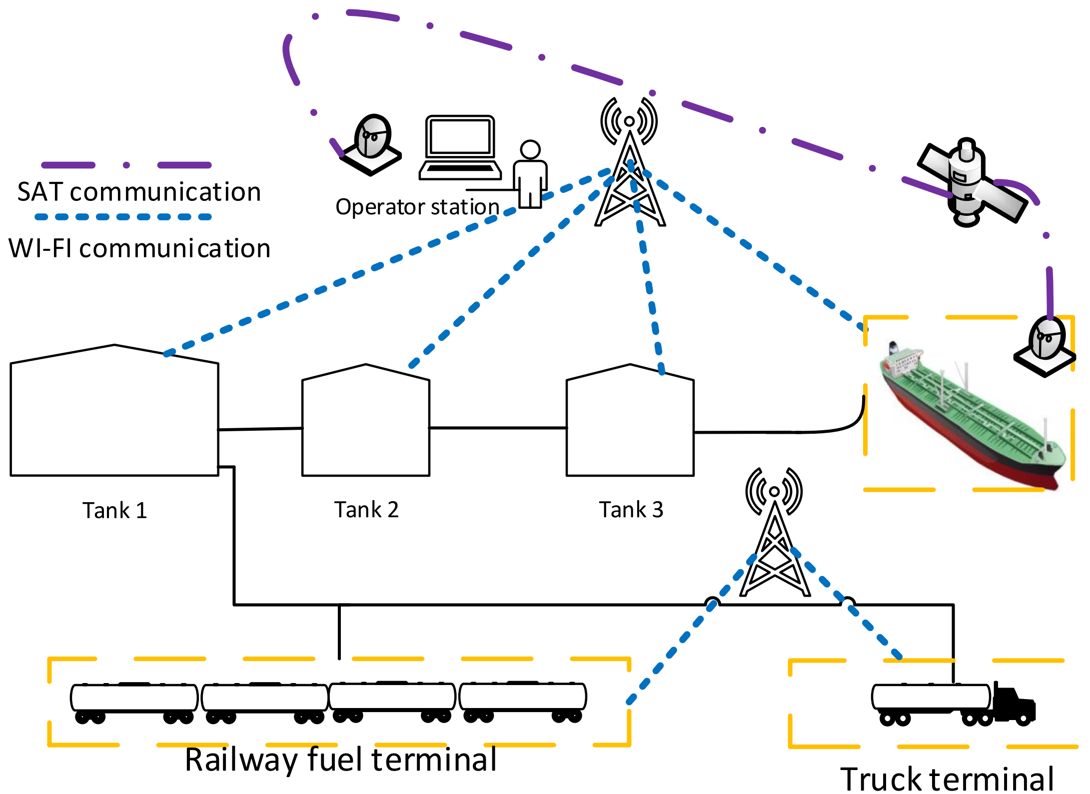
source: www.rynekinfrastruktury.pl/

Data transfer in distributed industrial control and protection systems



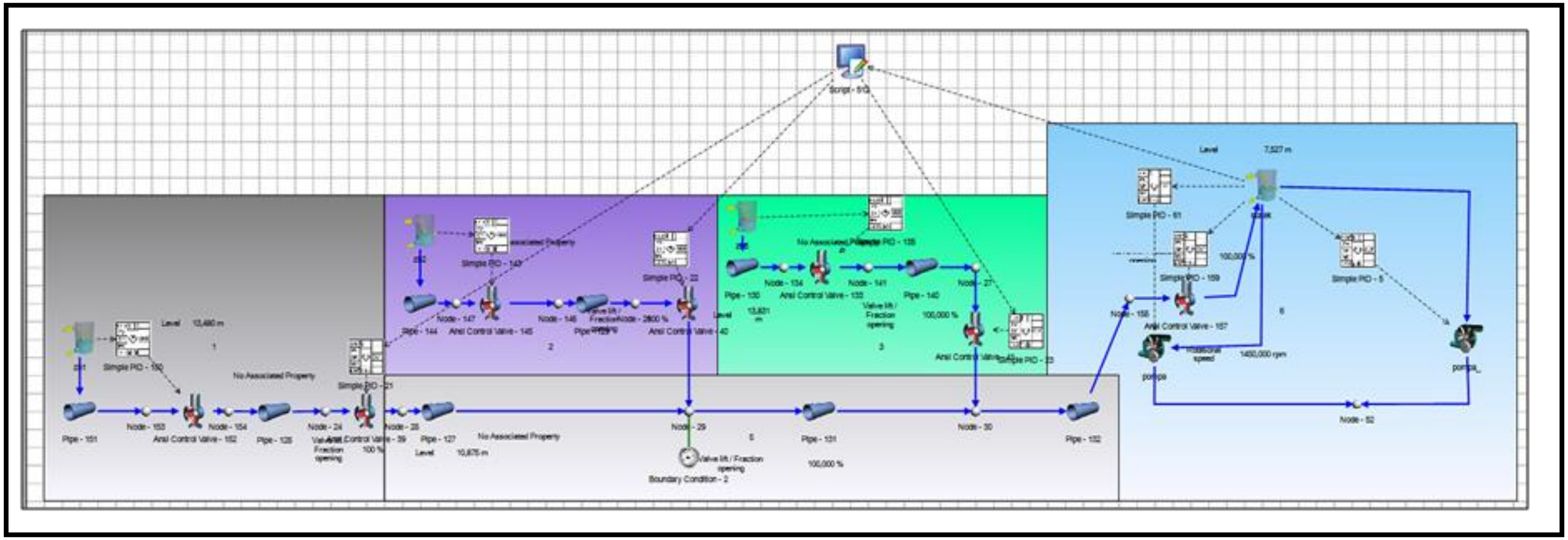
The control and protections system's in the oil sea port infrastructures may be connected by different internal and/or external communication channels.

Data transfer in distributed ICS maritime critical infrastructures



Main reason is that some parts of the large distributed installation are without option to use the line connection. Presented installation is distributed and control and protection system is III category (wireless and satellite).

Flownex CFD model for the oil sea port pipeline infrastructures



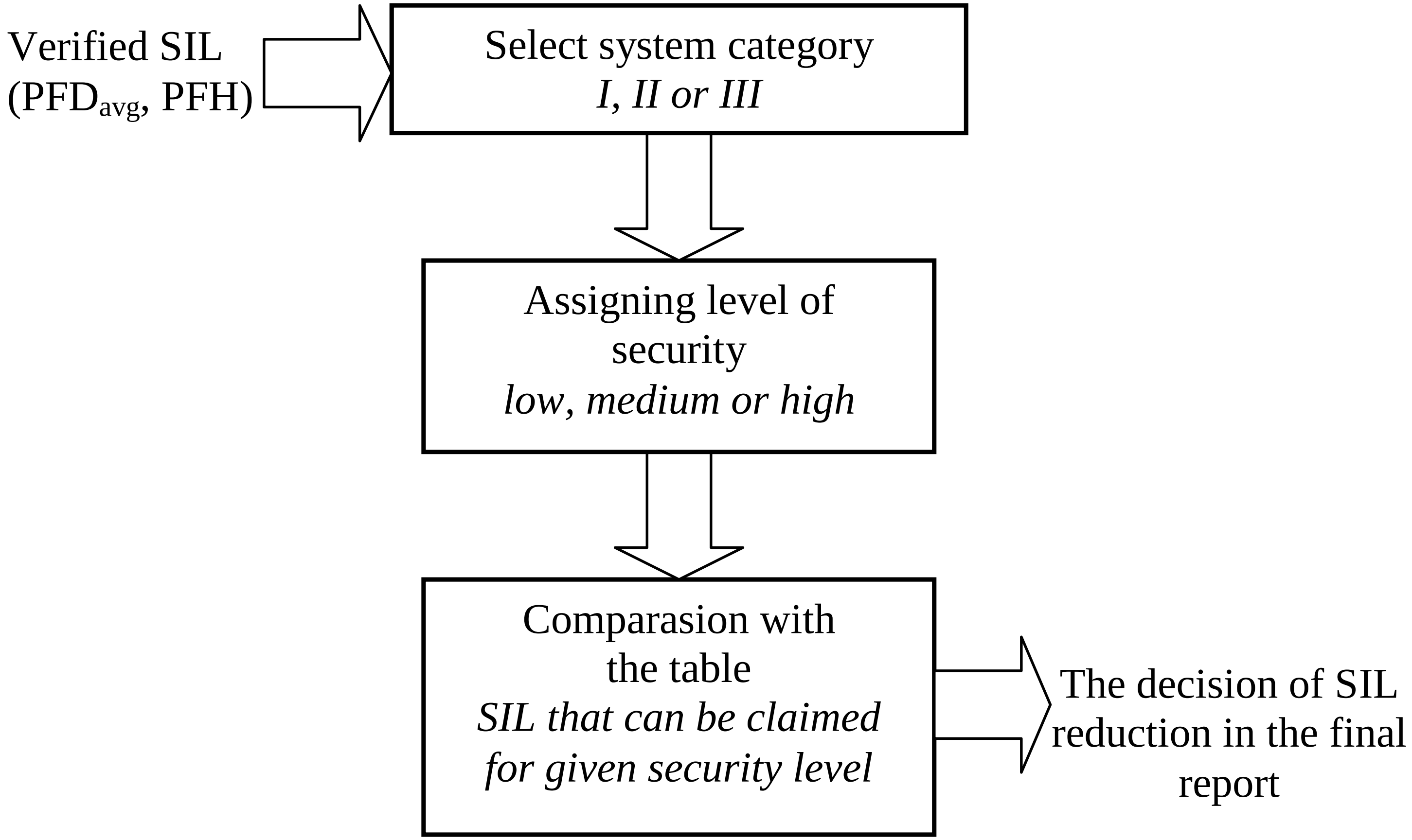
There are a lot of problems in that kind of installations. Main of the problem is high pressure oil transfer, overfill prevention tanks, pipeline leak, human errors, and common communication errors.

SIL that can be claimed for given EAL, SAL or sesa protection rings for ICS systems category II and (III)

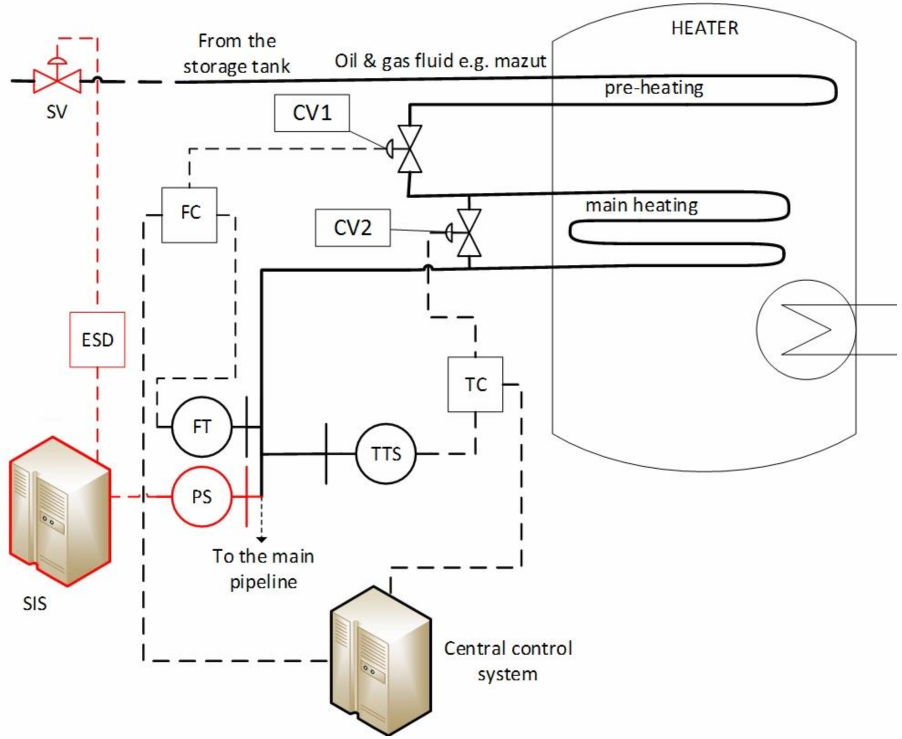
Determined				Verified SIL for systems of category II & (III)			
cyber security				*functional safety*			
EAL	SAL	Protection rings	Level of security	1	2	3	4
1	1	1	low	- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
2	1	2		- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
3	2	3	medium	SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
4	2	4		SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
5	3	5	high	SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
6	4	6		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
7	4	7		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)

The low level of security might reduce the safety integrity level when the SIL is to be verified.

Procedure of the SIL verification including security aspects

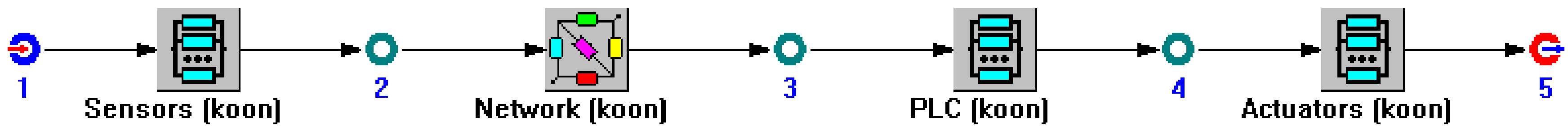


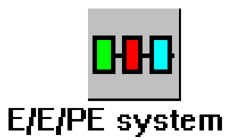
Example of oil sea port installation with critical infrastructure including BPCS and SIS systems



From the risk assessment the safety integrity level for given safety function overpressure protection pipeline was determined as **SIL3**.
In industrial practice such level requires usually to be designed SIS using a more sophisticated configuration.

Reliability block diagram model safety instrumented system SIS with industrial network





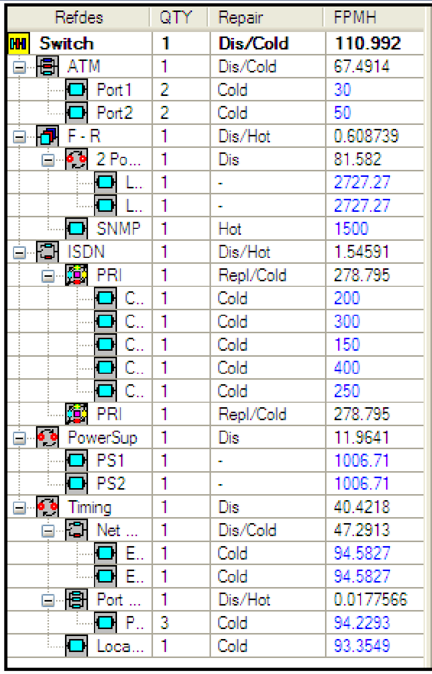
$$PFD_{avgSYS} \cong PFD_{avgS} + PFD_{avgNet} + PFD_{avgPLC} + PFD_{avgA}$$

with network

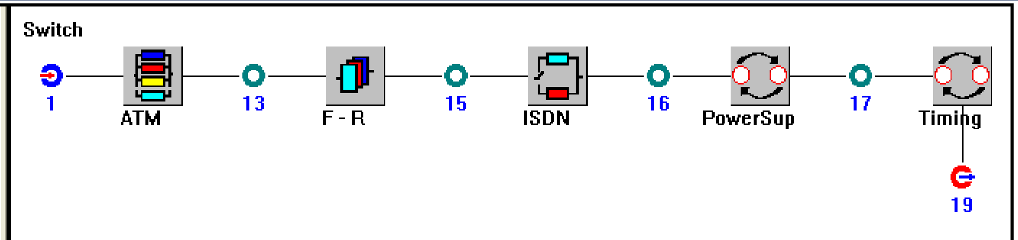
$$PFD_{avgSYS} \cong PFD_{avgS} + PFD_{avgPLC} + PFD_{avgA}$$

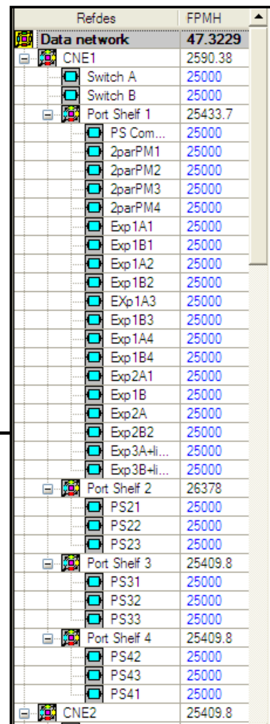
without industrial network !!!

RBD model industrial network

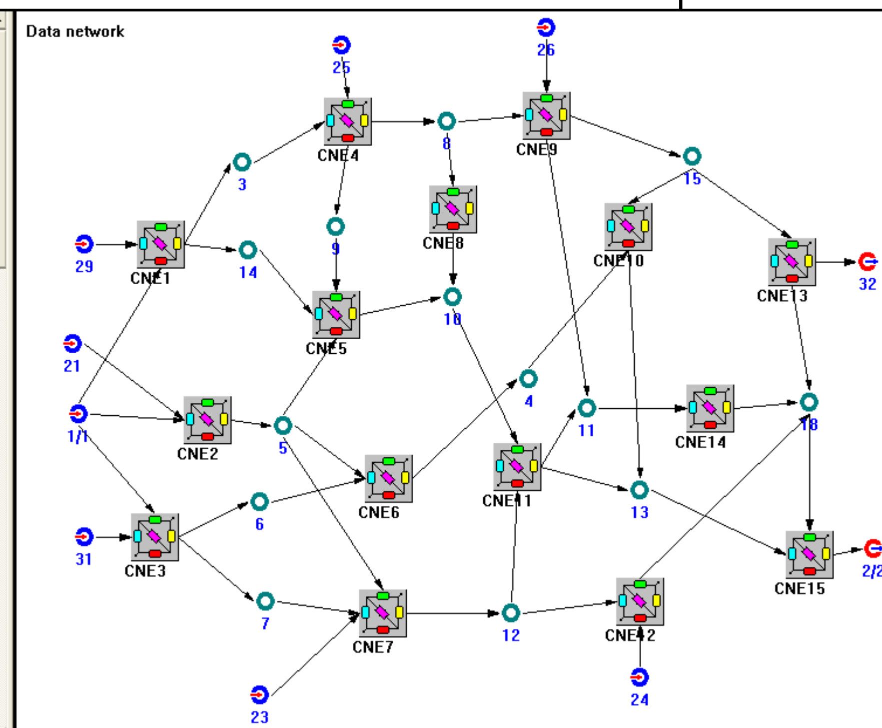


Refdes	QTY	Repair	FPMH
Switch	**1**	**Dis/Cold**	**110.992**
ATM	1	Dis/Cold	67.4914
Port1	2	Cold	30
Port2	2	Cold	50
F - R	1	Dis/Hot	0.608739
2 Po...	1	Dis	81.582
L..	1	-	2727.27
L..	1	-	2727.27
SNMP	1	Hot	1500
ISDN	1	Dis/Hot	1.54591
PRI	1	Repl/Cold	278.795
C..	1	Cold	200
C..	1	Cold	300
C..	1	Cold	150
C..	1	Cold	400
C..	1	Cold	250
PRI	1	Repl/Cold	278.795
PowerSup	1	Dis	11.9641
PS1	1	-	1006.71
PS2	1	-	1006.71
Timing	1	Dis	40.4218
Net ...	1	Dis/Cold	47.2913
E..	1	Cold	94.5827
E..	1	Cold	94.5827
Port ...	1	Dis/Hot	0.0177566
P..	3	Cold	94.2293
Loca...	1	Cold	93.3549





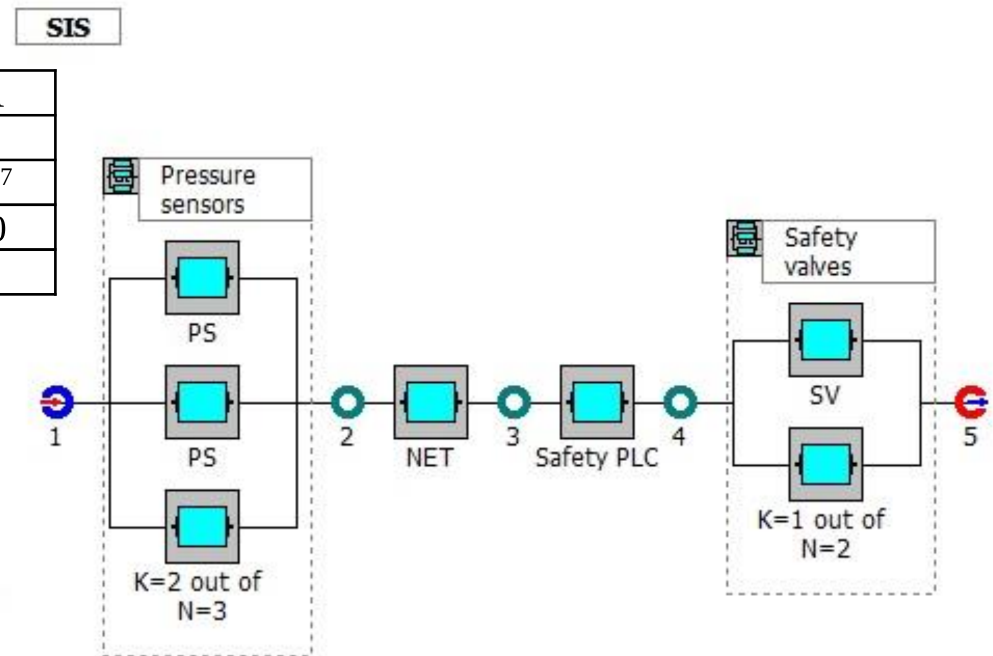
Refdes	FPMH
Data network	**47.3229**
CNE1	2590.38
Switch A	25000
Switch B	25000
Port Shelf 1	25433.7
PS Com...	25000
2parPM1	25000
2parPM2	25000
2parPM3	25000
2parPM4	25000
Exp1A1	25000
Exp1B1	25000
Exp1A2	25000
Exp1B2	25000
EXp1A3	25000
Exp1B3	25000
Exp1A4	25000
Exp1B4	25000
Exp2A1	25000
Exp1B	25000
Exp2A	25000
Exp2B2	25000
Exp3A+li...	25000
Exp3B+li...	25000
Port Shelf 2	26378
PS21	25000
PS22	25000
PS23	25000
Port Shelf 3	25409.8
PS31	25000
PS32	25000
PS33	25000
Port Shelf 4	25409.8
PS42	25000
PS43	25000
PS41	25000
CNE2	25409.8



SIS - overpressure protection system

Reliability data for elements SIS system:

	PS	NET	SafetyPLC	SVA
DC [%]	54	99	90	95
λ_{DU} [1/h]	$3\cdot10^{-7}$	$8\cdot10^{-8}$	$7\cdot10^{-7}$	$8\cdot10^{-7}$
T_I [h]	8760	8760	8760	8760
β	0.02	0.01	0.01	0.02



where: *DC – diagnostic coverage,*
λ_{DU} *– dangerous undetected failure rate*
T_I *– test interval,*
β *– beta factor (common couse failure)*

RBD model overpressure protection safety instrumented system in the critical installation

The average probability of failure on demand PFD_{avg} is calculated according to formula:

where: PFD_{avgSYS} - average probability of failure on demand for the SIS system, PFD_{avgS} - for the sensor, PFD_{avgNet} - average probability of failure on demand for the network, PFD_{avgPLC} - for the PLC, PFD_{avgA} - for the actuator.

The SIL verification report for SIS

System /subsystems/elements		k oo n	β [%]	PFD_{avg}	SIL
SIS	**0**	**-**	**-**	**$9.15 \cdot 10^{-4}$**	**3**
PS	**.1**	**2 oo 3**	**3**	**$4.46 \cdot 10^{-5}$**	**4**
PS	..2	-	-	$1.34 \cdot 10^{-3}$	2
PS	..2	-	-	$1.34 \cdot 10^{-3}$	2
PS	..2	-	-	$1.34 \cdot 10^{-3}$	2
NET	**.1**	**1 oo 1**	**-**	**$3.5 \cdot 10^{-4}$**	**3**
NET	..2	-	-	$3.5 \cdot 10^{-4}$	3
PLC	**.1**	**1 oo 1**	**-**	**$4.38 \cdot 10^{-4}$**	**3**
Safety PLC	..2	-	-	$4.38 \cdot 10^{-4}$	3
SVA	**.1**	**1 oo 2**	**2**	**$8.22 \cdot 10^{-5}$**	**4**
SVA	..2	-	-	$3.5 \cdot 10^{-3}$	2
SVA	..2	-	-	$3.5 \cdot 10^{-3}$	2

Thus, the PFD_{avg} is equal $9.15 \cdot 10^{-4}$ fulfilling formally requirements for random failures on level of SIL3. But PFD_{avg} value is near probabilistic criterion SIL2.

The omission of some subsystems or communication network can lead to too optimistic results, particularly in case of distributed control and protection systems of category II and III.

Safety integrity level **SIL3** for **III category** systems in those case required **high level of security** (**EAL ≥ 5** or **SAL ≥ 3**).

$$PFD_{avgSIS} \cong PFD_{avgPS(2oo3)} + PFD_{avgNET} + PFD_{avgSafetyPLC} + PFD_{avgSV(1oo2)} \cong$$

$$\cong 4.46 \cdot 10^{-5} + 3.5 \cdot 10^{-4} + 4.38 \cdot 10^{-4} + 8.22 \cdot 10^{-5} \cong 9.15 \cdot 10^{-4} \Rightarrow SIL3$$

Conclusion

- The control and protection systems of maritime critical infrastructure are potentially vulnerable to cyber attacks, as they are distributed and perform complex functions supervisory control and data acquisition SCADA.
- Based on risk assessment results the safety integrity level SIL is determined for safety functions.
- These functions are implemented within industrial control system ICS that consist of BPCS and/or SIS.
- Determination of required SIL related to the risk mitigation is based on semi quantitative evaluation method.
- Verification of SIL for considered architectures of BPCS and/or SIS is supported by probabilistic modelling for appropriate data and model parameters including security-related aspects.
- Security related analyses of the ICS during its design and operation as distributed control system DCS are very important in maritime critical infrastructures.

Conclusion

- A comprehensive integration of the functional safety and cyber security analysis in maritime critical infrastructures is very important and it is currently a challenging issue.
- In this project an attempt to integrate the functional safety and security issue was presented.
- The security aspects, which are associated with e.g. communication between equipment or restrictions in access to the system and associated assets, are usually omitted during this stage of analysis. However, they can significantly influence the final results.
- Further research works have been undertaken to integrate outlined above aspects of safety and security in the design and operation of the programmable control and protection systems to develop a relatively simple methodology to be useful in industrial practice.
- The next step of evaluation the proposed approach safety & cyber security integrated it to include human as a hazard factor.

REFERENCES

Details are given in Journal of Polish Safety and Reliability Association – JPSRA, Special Issue on HAZARD Project, Volume 10, No 1, April 2019

Interreg
Baltic Sea Region

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND

HAZARD

GDAŃSK UNIVERSITY OF TECHNOLOGY

HISTORY IS WISDOM
FUTURE IS CHALLENGE