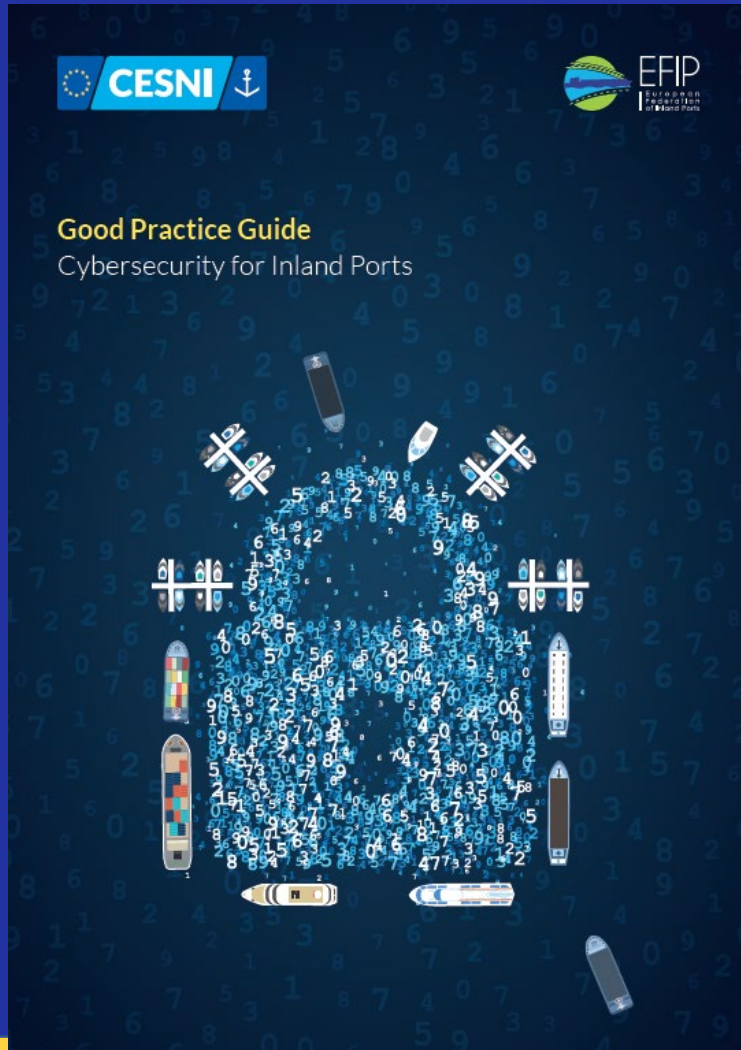


# GOOD PRACTICE GUIDE

## Good Practice Guide Cybersecurity for inland ports

21/03/2023





**CESNI in a few words**



**Overview of the guide**



**Application of measures**

# 01

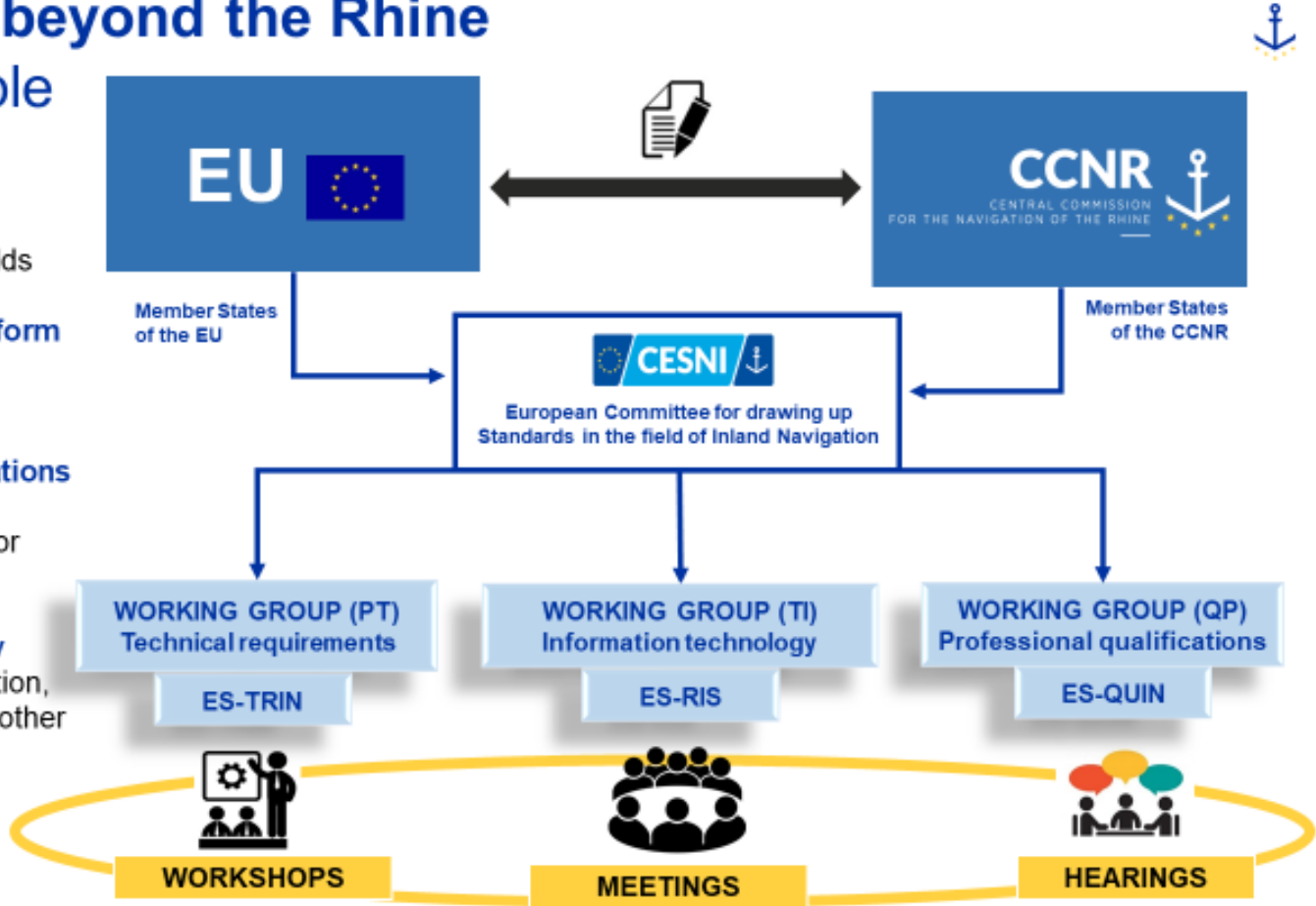
**CESNI in a few words**



# CESNI, a CCNR Committee with all EM and CCNR MS

## Cooperation beyond the Rhine CESNI example

- » adopting technical standards in various fields
- » deliberating on their uniform interpretation and application
- » deliberating on derogations and equivalences of technical requirements for specific crafts
- » deliberating on priority topics (safety of navigation, environment protection, other areas).



# Step-by-step approach

- **Cybersecurity is part of the work-programme of CESNI**
  - It is a complex and vast subject, with reglementary, technical aspects...
  - It will not be addressed all at once
- **CESNI identified two inland navigation targets more exposed to cyber-threats**
  - Inland Ports and vessels
- **With the support of EFIP, Inland ports were chosen as a first step**
  - The guide aims to be an accessible framework for cybersecurity good practices for every type of inland navigation ports
  - In 4 languages, free download
  - Expected 1<sup>st</sup> semester 2023
- **When this guide will be published, CESNI will discuss on next steps**

# 02

## Overview of the guide



# Guide composed of 3 parts

## Part 1

### Cybersecurity threat landscape of ports

- General cybersecurity trends and consequences for ports
- IT security of ports, their principal assets, and of inland navigation craft
- Port threat taxonomy
- Sample port attack scenarios

## Part 2

### Mitigating cybersecurity risks for ports

- Organisational policies and procedures
- Information technology/Operational technology policies for port
- Technical cybersecurity measures for ports

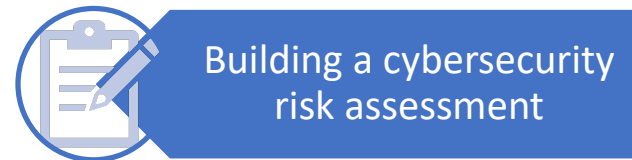
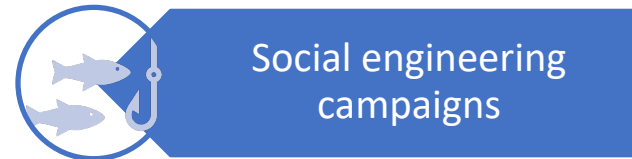
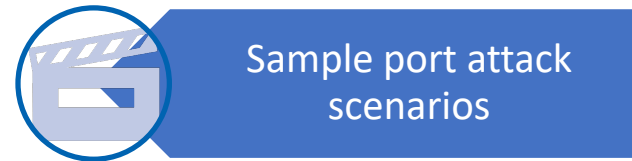
## Part 3

### Tips for the implementation of risk mitigation measures

- Maturity evaluation framework
- Applicability table for measures

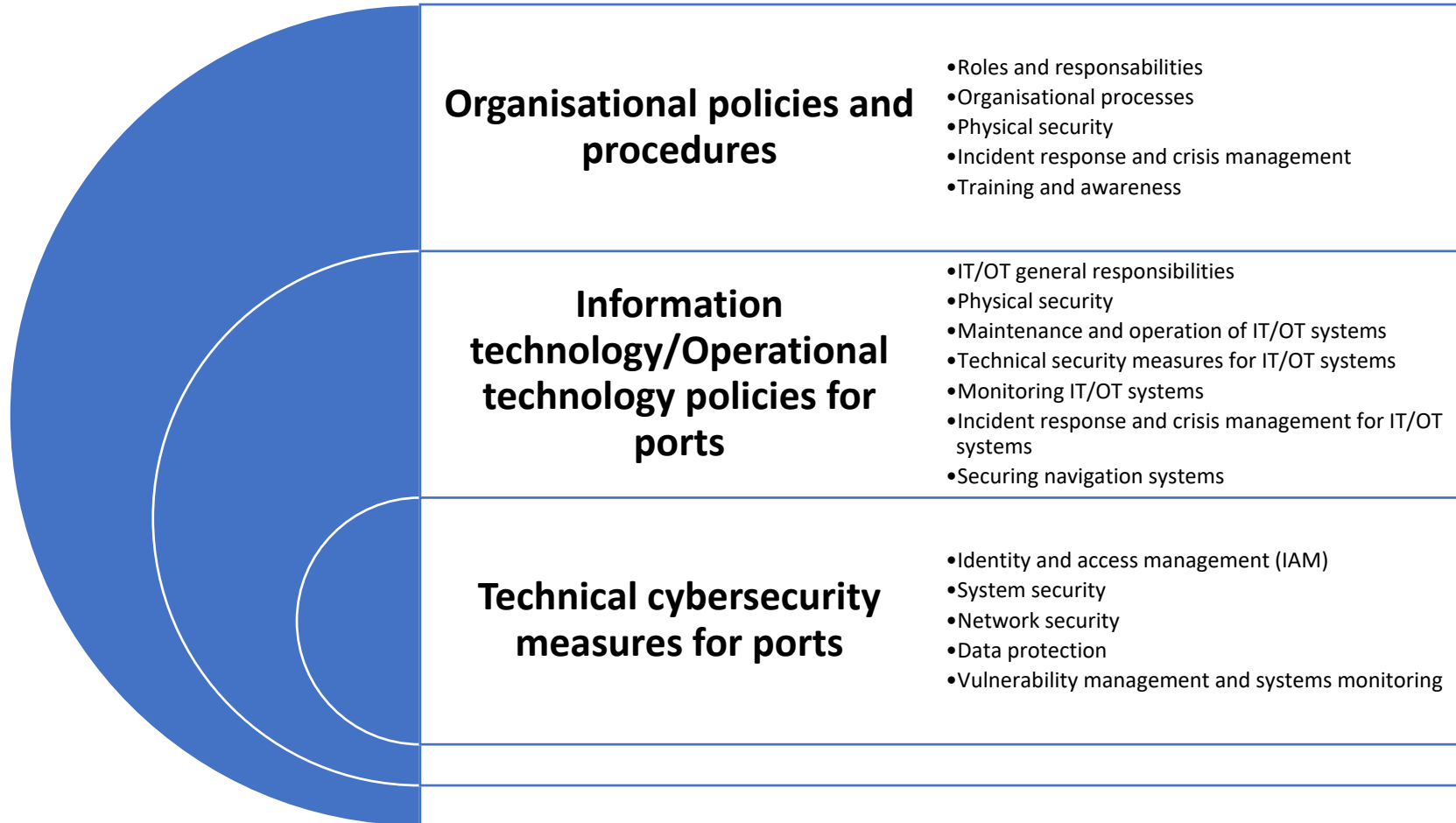
## And 5 case studies

- **Case studies are illustrated with example and advices**
- **Simple steps are given to put in practice**





# 3 types of measures

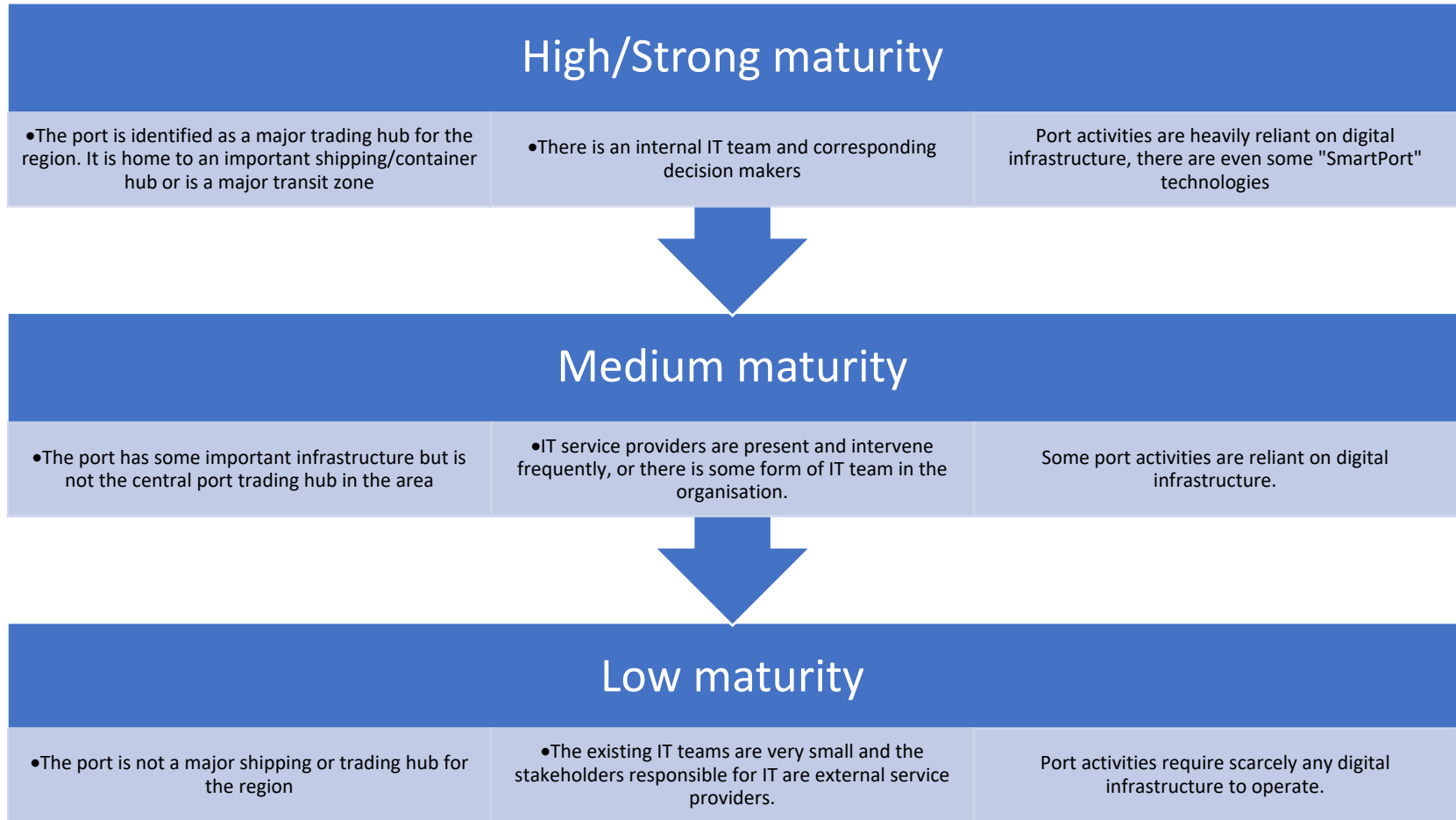


# 03

## Application of measures




# Maturity Level of inland ports regarding cybersecurity



# Maturity Evaluation Framework

- **Self-assessment method**
  - A score is given to each measure depending if the measure is currently enforced
  - The scores are given by a panel of key (internal) actors, including as a minimum:
    - an executive manager
    - a manager of IT
    - and an operational manager
  - The final aggregated score gives the level of maturity

## About 80 graduated measures (depending on the level of maturity)



Measure ID	Measure
[ITOT] 5.1	Access to the internet from critical industrial systems (such as lock bridge management systems, power stations, drinking water stations) should be limited to the minimum.
[ITOT] 5.2	Development tools should not be installed on active and running machines. Only production systems should be active on IT/OT installations.
[ITOT] 5.3	With regard to operational systems, unsecured protocols (e.g. HTTP, Telnet, FTP) should be disabled in favour of secured protocols (e.g. HTTPS, SSH, SFTP).
[ITOT] 5.4	Separate networks_zones should be used for the connection of operational systems, for any IoT devices, for professional use Wi-Fi, and for public Wi-Fi.
[ITOT] 5.5	Industrial Control Systems (ICSs) should be divided into consistent functional or technical zones. These zones should be separated from each other.
[ITOT] 5.6	A filtering policy between zones and at administrative gateways should be implemented following a defined strict protocol (i.e. protocol regarding data streams, activity logging, IP address logging, etc.)
[ITOT] 5.7	Where possible, a VPN should be deployed to gateways, blocking outside traffic to operational system zones.
[ITOT] 5.8	Workstations that are authorised to log on to parts of the network with high privilege levels (administration) should, as far as possible, be separated from the main network. These workstations should be controlled and should not be used for other purposes. They should be frequently updated and reinforced using hardening policies.
[ITOT] 5.9	When the remote control of operational systems is required, remote connections should be certified, connection passwords should be managed in the context of the password policy defined by the organisation, logging should be enabled, secure communication protocols should be in place, and remote connection sessions should be automatically ended after a period of inactivity.
[ITOT] 5.10	Mechanisms should be in place to secure machine-to-machine exchanges (including EDI messages and API mostly used with external stakeholders, such as shipping companies) and provide mutual authentication, integrity, and confidentiality with the port systems, especially when exchanges are carried out on the Internet. Examples of these mechanisms are encryption, PKI or digital certificates, integrity checks, digital signature, and timestamping.

# Applicability Matrix

Maturity	Concerned IT Teams	Operational Managers	Executive Management
Low	[TSM] 1.1 + 1.2 + 1.3 + 1.4 + 1.5 + 1.6 + 2.1 + 3.1 + 3.2 [ITOT] 5.3	[OPP] 3.1 + 3.2 + 3.3 + 3.4 + 3.5 + 3.6 + 3.7 + 3.8 + 3.9 + 4.0 + 4.1 + 5.1 + 5.2 + 5.3 + 5.4 + 5.5 + 5.6 + 5.7 + 5.8 + 5.9 + 6.0 + 6.1 + 6.2 + 6.3 + 6.4 + 6.5 + 6.6 + 6.7 + 6.8 + 6.9 + 7.0 + 7.1 + 7.2 + 7.3 + 7.4 + 7.5 + 7.6 + 7.7 + 7.8 + 7.9 + 8.0 + 8.1 + 8.2 + 8.3 + 8.4 + 8.5 + 8.6 + 8.7 + 8.8 + 8.9 + 9.0 + 9.1 + 9.2 + 9.3 + 9.4 + 9.5 + 9.6 + 9.7 + 9.8 + 9.9 + 10.0 [ITOT] 2.1 + 2.2 + 2.3 + 2.4 + 2.5 + 2.6 + 2.7 + 2.8 + 2.9 + 3.0 + 3.1 + 3.2 + 3.3 + 3.4 + 3.5 + 3.6 + 3.7 + 3.8 + 3.9 + 4.0 + 4.1 + 4.2 + 4.3 + 4.4 + 4.5 + 4.6 + 4.7 + 4.8 + 4.9 + 5.0 + 5.1 + 5.2 + 5.3 + 5.4 + 5.5 + 5.6 + 5.7 + 5.8 + 5.9 + 6.0 + 6.1 + 6.2 + 6.3 + 6.4 + 6.5 + 6.6 + 6.7 + 6.8 + 6.9 + 7.0 + 7.1 + 7.2 + 7.3 + 7.4 + 7.5 + 7.6 + 7.7 + 7.8 + 7.9 + 8.0 + 8.1 + 8.2 + 8.3 + 8.4 + 8.5 + 8.6 + 8.7 + 8.8 + 8.9 + 9.0 + 9.1 + 9.2 + 9.3 + 9.4 + 9.5 + 9.6 + 9.7 + 9.8 + 9.9 + 10.0 3.3 + 5.1 + 5.2	[OPP] 1.1 + 2.1 + 2.2 + 2.3 + 5.6 [TSM] 4.1
Medium	[OPP] 2.5 [ITOT] 1.1 + 1.2 + 4.2 + 5.4 + 5.5 + 5.6 + 5.7 + 5.8 + 5.9 + 6.0 + 6.1 + 6.2 + 6.3 + 6.4 + 6.5 + 6.6 + 6.7 + 6.8 + 6.9 + 7.0 + 7.1 + 7.2 + 7.3 + 7.4 + 7.5 + 7.6 + 7.7 + 7.8 + 7.9 + 8.0 + 8.1 + 8.2 + 8.3 + 8.4 + 8.5 + 8.6 + 8.7 + 8.8 + 8.9 + 9.0 + 9.1 + 9.2 + 9.3 + 9.4 + 9.5 + 9.6 + 9.7 + 9.8 + 9.9 + 10.0 2.5 + 3.3 + 3.4 + 3.5 + 3.6 + 4.2 + 4.3 + 4.4 + 5.1 + 5.2 + 5.3 + 5.4	[OPP] 2.4 + 3.6 + 4.6 [ITOT] 2.4 + 2.5 + 4.1 + 4.3 + 4.4 + 4.5 + 4.6 + 4.7 + 4.8 + 4.9 + 5.0 + 5.1 + 5.2 + 5.3 + 5.4 + 5.5 + 5.6 + 5.7 + 5.8 + 5.9 + 6.0 + 6.1 + 6.2 + 6.3 + 6.4 + 6.5 + 6.6 + 6.7 + 6.8 + 6.9 + 7.0 + 7.1 + 7.2 + 7.3 + 7.4 + 7.5 + 7.6 + 7.7 + 7.8 + 7.9 + 8.0 + 8.1 + 8.2	[OPP] 1.1 + 3.4 + 3.5 + 4.2 + 4.3 + 4.4 + 4.5
High	[OPP] 4.11 [ITOT] 1.3 + 1.4 + 5.9 + 5.10 + 6.3 + 6.4 [TSM] 1.10 + 1.11 + 1.12 + 2.6 + 2.7 + 2.8 + 2.9 + 2.10 + 3.7 + 3.8 + 3.9 + 4.5 + 4.6 + 4.7	[ITOT] 2.6 + 4.5 + 8.3 + 8.4	[OPP] 1.3 + 1.4 + 1.5 + 1.6 + 2.6 + 2.7 + 4.7 + 4.8 + 4.9 + 4.10 + 5.8 + 5.9 [ITOT] 4.6

# Conclusions

- **Cybersecurity is a complex subject**
  - This guide is only a contribution, not an end
  - Maybe it needs to be enlarged beyond the context of ports
- **The importance of this subject will certainly increase with time**
  - Automation of navigation
  - More digitalisation in inland navigation
- **Cybersecurity is not only about IT, it needs a holistic approach**
  - Vessels, crew, ports, equipment, remote control center
  - Technical perspective, management and operational



THANK YOU FOR YOUR ATTENTION

[CESNI.EU](http://CESNI.EU)

**Raphaël Le Guillou**

CESNI Administrator, Information Technologies

r.leguillou@ccr-zkr.org