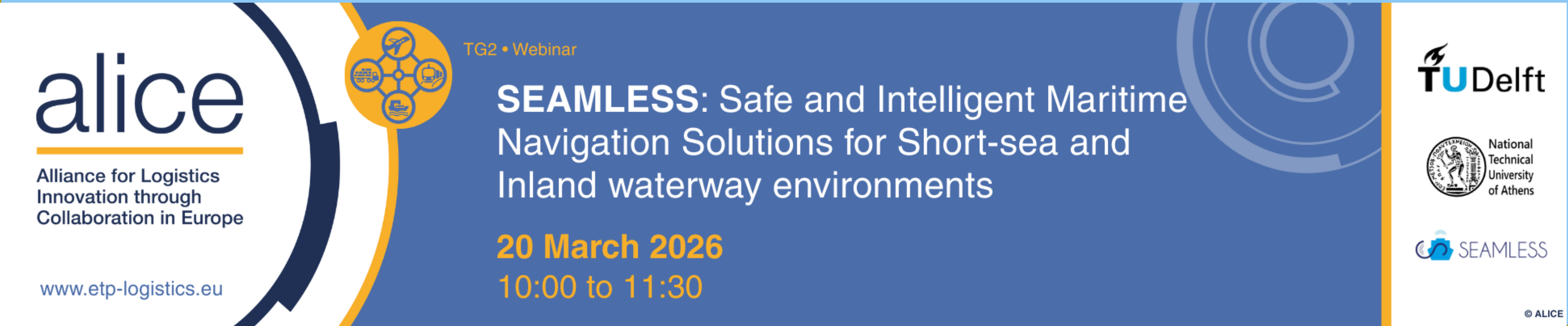
WARRANT
Dependable Waterborne Digitalisation

IDENTIFYING RISKS FOR WATERBORNE DIGITAL SYSTEMS

THE CHALLENGES OF USING ESTABLISHED TECHNIQUES IN NEW SETTINGS



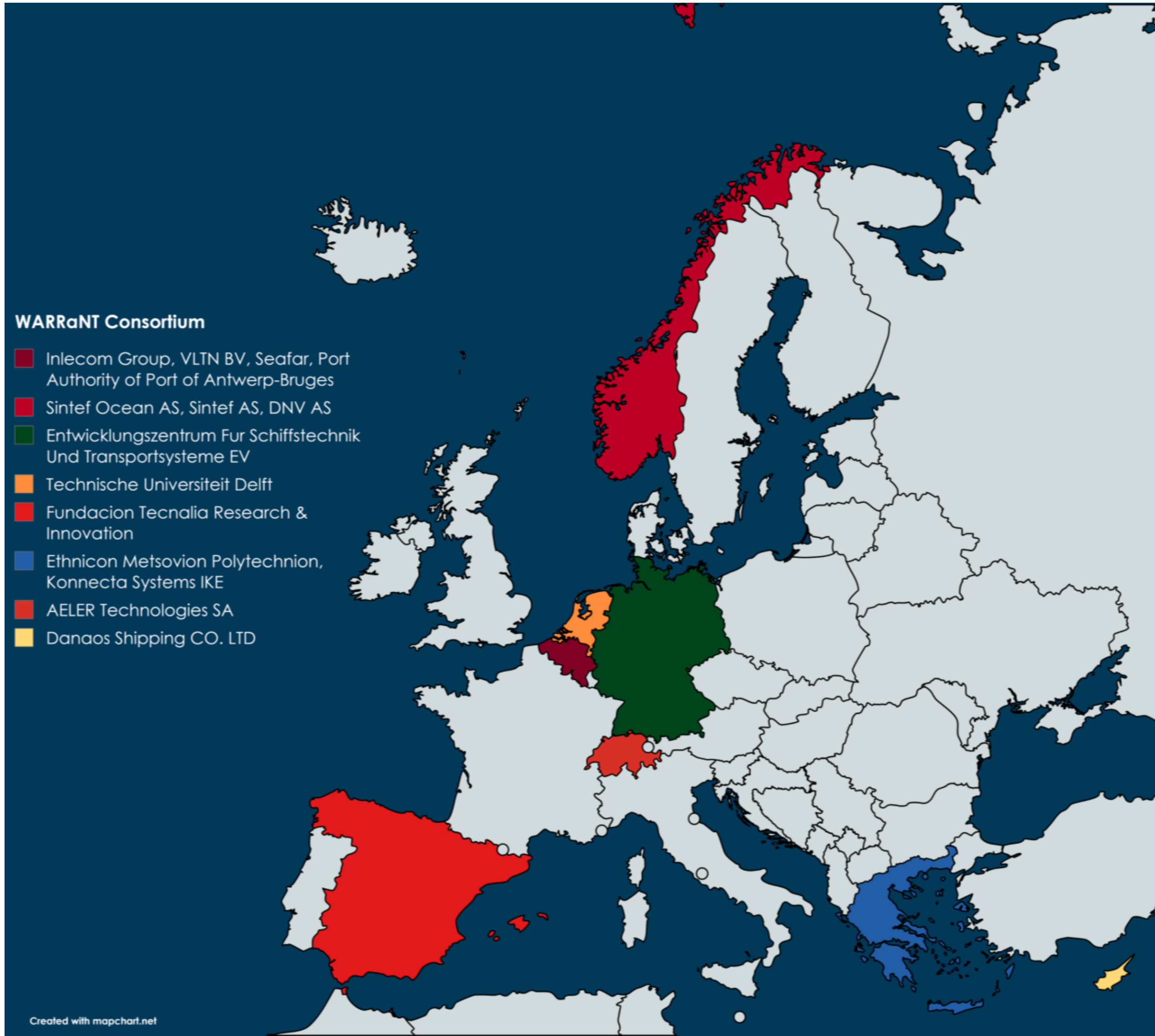
Funded by the European Union

SOME FACTS ABOUT THE PROJECT

WAterborne fedeRated systems and models for secuRe and resilieNt operations

Duration: 36 months

Total eligible costs: 4,251,557.50 €



WARRANT
Dependable Waterborne Digitalisation

MOTIVATION

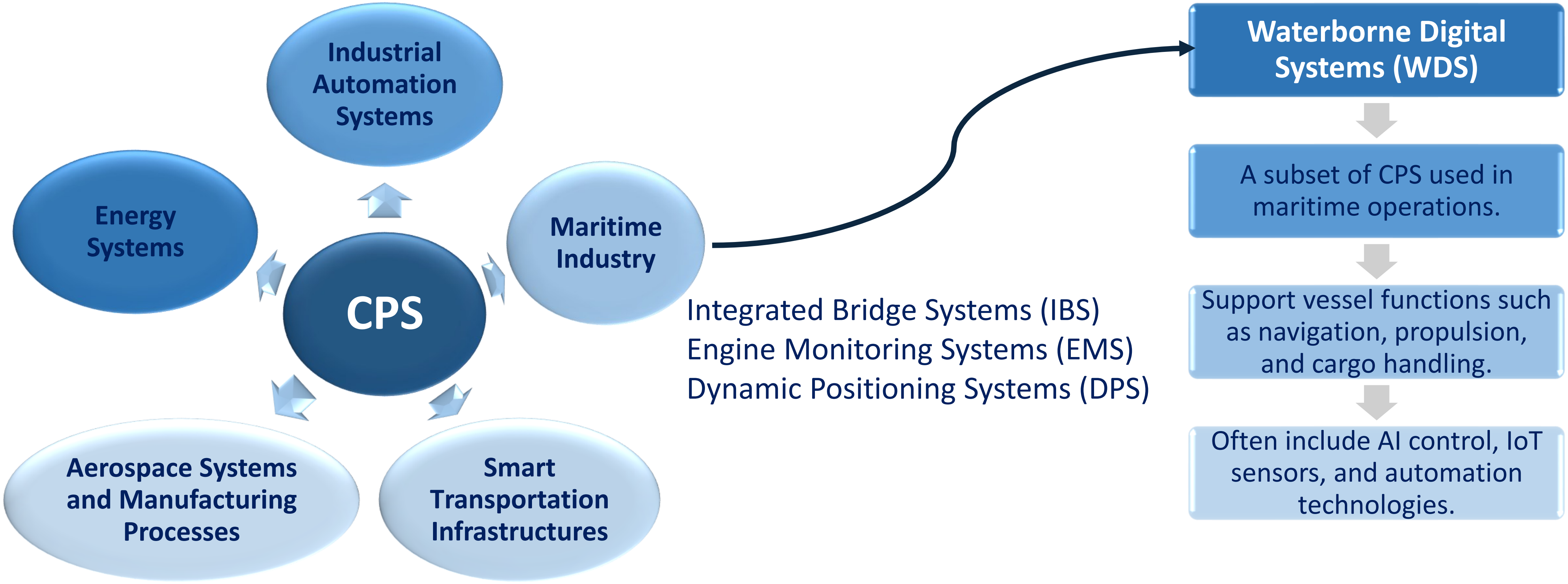
Waterborne Digital Systems (WDS) are **smart**, **interconnected** systems with **shared human/machine (possibly AI) control and IoT sensors** that exhibit complex behaviour in off-nominal conditions.

OBJECTIVE

Adapt and extend the conventional Hazard and Operability (HAZOP) analysis for reducing unidentified hazardous scenarios and improve the effectiveness of safety assurance for **Waterborne Digital Systems (WDS)**.

CHARACTERISTICS OF CYBER-PHYSICAL SYSTEMS (CPS)

- Integrate physical processes with computational components and communication networks.
- Rely on continuous interaction between sensors, controllers, actuators, and communication infrastructures.

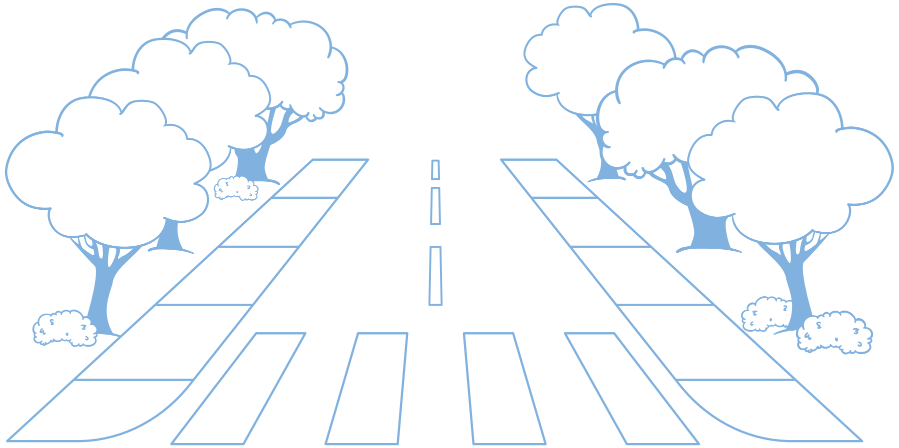


(Lyu et al., 2019; Progoulakis et al., 2021; Nourian & Madnick, 2015)

WARRANT
Dependable Waterborne Digitalisation

SAFETY AND SECURITY CHALLENGES

The increasing adoption of WDS improves operational **efficiency** and **automation** capabilities.



Why is CPS risk assessment more complicated ?

Challenges

New hazards and failure modes emerge from the **interaction of components** (e.g. communication delays, incorrect sensor data).

Cyber threats can directly **trigger safety-critical failures** in physical systems (e.g. navigation, propulsion, cargo management).

CPS may include machine learning/AI, and distributed control systems with **dynamic and possibly "black-box" behaviour**.

(Nourian & Madnick, 2015; Progoulakis et al., 2021; Qi et al., 2022)

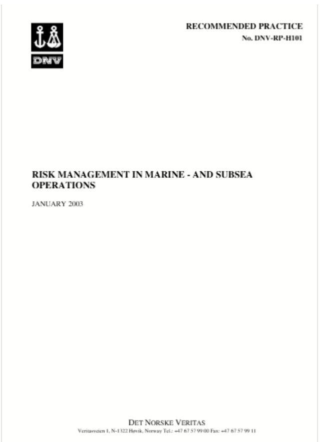
HAZARD AND OPERABILITY (HAZOP)

- HAZOP is an established hazard identification technique originally for the chemical process industry.
- **Its fundamental principle is that hazards arise when the system deviates from its design intent**.

1. Formation of a multidisciplinary expert team.
2. Review of system architecture and workflow.
3. Division of the system into nodes representing process segments or operational functions.
4. Application of guidewords such as "**No**", "**More**", "**Less**", "**Part of**", or "**Other than**" to identify abnormal conditions.
5. Identification of deviations, causes and consequences.

ISO/IEC 61882:2016
Standardized methodology for HAZOP studies

DNV-RP-H101
'Risk Management in Marine and Subsea Operations'
Recommends HAZOP as a method for risk assessment in marine and subsea environments.



(Rausand and Haugen, 2020; Qi et al., 2022)

WARRANT
Dependable Waterborne Digitalisation

LIMITATIONS OF TRADITIONAL HAZOP FOR CPS

Traditional HAZOP

Maritime system examples

- Inert Gas System
- Ballast Pump System
- Fuel Supply Systems

Systems-of-Systems complexity and risk propagation	Cyber-security risks	Complex component interactions	Human/Machine interactions
Is designed for less complex, predominantly hardware-driven systems	Does not inherently account for software and cyber attacks	Fails to capture hazards arising from interactions between system components	Not easy to determine deviation from design intent of complex, adaptive systems

(Qi et al., 2022; Fenelon & Hebbron; Nourian & Madnick, 2015)

HAZOP EXTENSIONS FOR CPS FROM THE LITERATURE

Cyber-HAZOP	Control HAZOP (CHAZOP)	Hierarchical HAZOP approaches	Model-based hazard analysis
• Integrates cybersecurity threats into deviation analysis, linking cyber attacks with process deviations (Wang et al., 2026).	• Analyses hazards related to control systems, including software, communication networks, hardware, and human–machine interfaces (Clarke, 2016).	• Analyse CPS at multiple levels, such as system architecture, software lifecycle, and internal algorithm behaviour (Qi et al., 2022).	• Uses mathematical models or simulations to identify hazardous system states (Golabi et al., 2022).

WARRANT HAZOP-BASED METHODOLOGY

Component Layer propagates to Function Layer

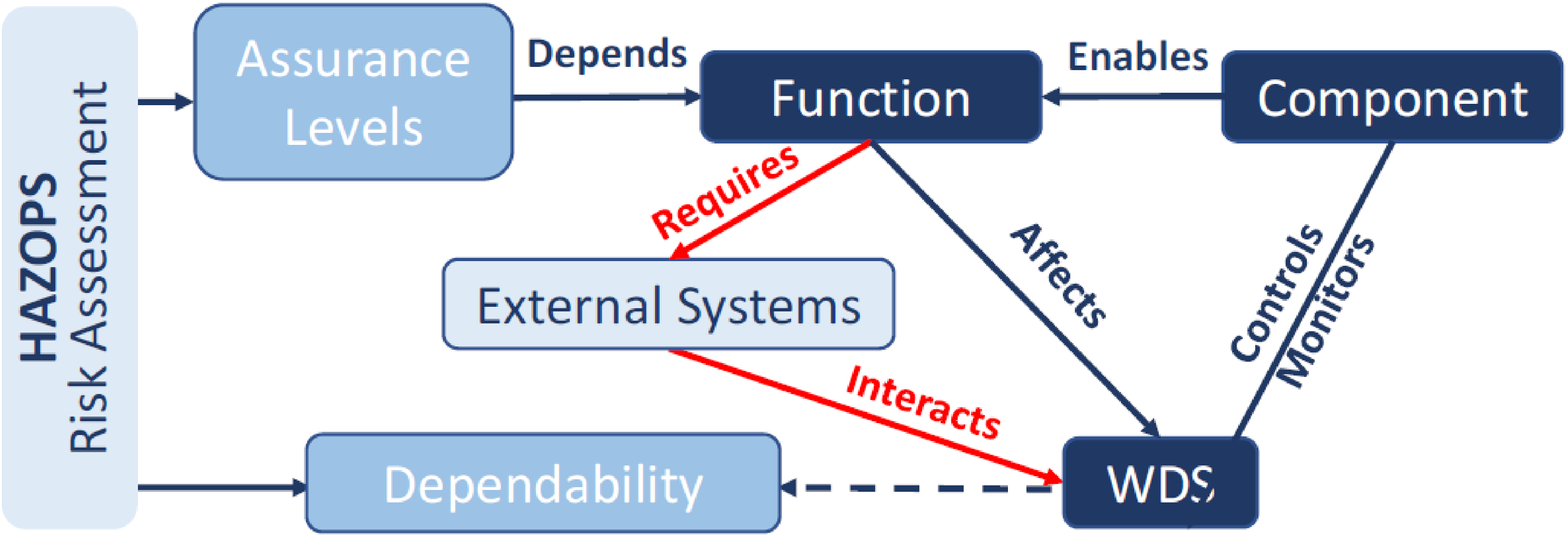


Figure 1 Schema of the envisioned KG

Source: INLECOM Whitepaper (2025)

HAZOP case studies for different WDSs will be conducted in the WARRANT Living Labs.

CASE STUDY: REMOTE OPERATIONS

WARRANT Living Lab 4

Dependable Remote Operation Systems (SEAFAR)

Operational Environment:
Remote-controlled barges in the Rhine and Antwerp regions.

Objective:
Apply WARRANT methodology to ensure remote operations are safe, cybersecure and resilient under real-world conditions.

HAZOP activities:

- Select risks of interest to stakeholder.
- Implement HAZOP variations to identify methodological gaps.

CASE STUDY: REMOTE OPERATIONS

- **Initial study object →** Handover procedure.
- **Method →** Procedure HAZOP conducted through workshops with SEAFAR.
- **Nodes →** Steps of the procedure.

Nodes:

- ROC Request for initiation of remote control
- Ship Preparation for remote control
- Ship requesting local control
- ROC request to give the control back on board
- ROC emergency procedure
- Ship emergency take over in local control

Guidewords	Meaning
No	None of the design intent is achieved.
As well as	An additional activity occurs.
Part of	Only some of the design intent is achieved.
Reverse	Logical opposite of the design intention is achieved.
Other than (other)	Complete substitution-another activity takes place OR an unusual activity occurs or uncommon condition exists.
Before/after	The step (or some part of it) is effected out of sequence.
Early/late	The timing is different than intended.
Faster/slower	The step is done/ not done with the right timing.

CASE STUDY: REMOTE OPERATIONS

For each deviation (i.e. step + guideword) the following have been examined:

Causes

- Hardware failures (e.g., button failure).
- Human factors (e.g., stress, fatigue, lack of due diligence).
- Operational conditions (e.g., time pressure).

Consequences

- Impacts on safety, assets, environment and operations.
- Possible effects on other nodes

Safeguards

- System redundancy.
- Monitoring and alarm systems.
- Shutdown or control mechanisms.

Risk Ranking

Category		Consequence Severity				
Asset		No shutdown, costs less than $10,000 to repair	No shutdown, costs less than $100,000 to repair	Operations shutdown, loss of day rate for 1-7 days and/or repair costs of up to $1,000,000	Operations shutdown, loss of day rate for 7-28 days and/or repair costs of up to $10,000,000	Operations shutdown, loss of day rate for more than 28 days and/or repair more than $10,000,000
Environmental Effects		No lasting effect. Low level impacts on biological or physical environment. Limited damage to minimal area of low significance.	Minor effects on biological or physical environment. Minor short-term damage to small area of limited significance.	Moderate effects on biological or physical environment but not affecting ecosystem function. Moderate short-medium term widespread impacts e.g. oil spill causing impacts on shoreline.	Serious environmental effects with some impairment of ecosystem function e.g. displacement of species. Relatively widespread medium-long term impacts.	Very serious effects with impairment of ecosystem function. Long term widespread effects on significant environment e.g. unique habitat, national park.
Community/ Government/ Media/ Reputation		Public concern restricted to local complaints. Ongoing scrutiny/ attention from regulator.	Minor, adverse local public or media attention and complaints. Significant hardship from regulator. Reputation is adversely affected with a small number of site focused people.	Attention from media and/or heightened concern by local community. Criticism by NGO's. Significant difficulties in gaining approvals. Environmental credentials moderately affected.	Significant adverse national media/public/ NGO attention. May lose license to operate or not gain approval. Environment/ management credentials are significantly tarnished.	Serious public or media outcry (international coverage). Damaging NGO campaign. License to operate threatened. Reputation severely tarnished. Share price may be affected.
Injury and Disease		Low level short-term subjective inconvenience or symptoms. No measurable physical effects. No medical treatment required.	Objective but reversible disability/impairment and/or medical treatment, injuries requiring hospitalization.	Moderate irreversible disability or impairment (<30%) to one or more persons.	Single fatality and/or severe irreversible disability or impairment (>30%) to one or more persons.	Short or long term health effects leading to multiple fatalities, or significant irreversible health effects to >50 persons.
		Low (1)	Minor (2)	Moderate (3)	Major (4)	Critical (5)
Likelihood	Almost Certain (E) Occurs 1 or more times a year	High	High	Extreme	Extreme	Extreme
	Likely (D) Occurs once every 1-10 years	Moderate	High	High	Extreme	Extreme
	Possible (C) Occurs once every 10-100 years	Low	Moderate	High	Extreme	Extreme
	Unlikely (B) Occurs once every 100-1000 years	Low	Low	Moderate	High	Extreme
	Rare (A) Occurs once every 1000-10000 years	Low	Low	Moderate	High	High

Source: **ABS GUIDANCE NOTES ON RISK ASSESSMENT APPLICATIONS FOR THE MARINE AND OFFSHORE INDUSTRIES, 2020**

CASE STUDY: REMOTE OPERATIONS (INDICATIVE RESULTS)

Study title:	HAZOP				
Procedure title:	Remote/local Control handover procedure	**Revision number:**	0	**Sheet:**	
Team composition:		**Instruction 1:**	Preparation for ship local control	**Date:**	
Part considered:				**Meeting date:**	

No.	Property	Guideword	Deviation	Possible causes	Consequences	Existing Controls	Severity	Likelihood	Risk	Actions required	Severity	Likelihood	Risk
1	Checks including steering gear, propulsion and bow thrusters are on neutral position.	1. No	1. Checks not performed	Lack of proper crew training, Lack of crew familiarisation, Fatigue, Stress, Lack of due diligence, Lack of company procedures or inadequate procedures	Underestimated safety risk, Partial situational awareness, Uncontrolled vessel movement, Loss of control, Collision, Grounding, Crew injury.								
		2. Part of	2. Checks performed partially	Lack of proper crew training, Lack of crew familiarisation, Fatigue, Stress, Inattention to detail, Lack of due diligence, Lack of company procedures or inadequate procedures	Underestimated safety risk, Partial situational awareness, Uncontrolled vessel movement, Loss of control, Collision, Grounding, Crew injury.								
		3. Faster	3. Checks performed faster and therefore some elements are omitted.	Lack of proper crew training, Lack of crew familiarisation, Fatigue, Stress, Inattention to detail, Lack of due diligence, Lack of company procedures or inadequate procedures	Underestimated safety risk, Partial situational awareness, Uncontrolled vessel movement, Loss of control, Collision, Grounding, Crew injury.								

Design intent:
Before control is handed over, ship controls (steering gear, propulsion) need to be on neutral position.

Designed Safeguard:
Check that ship controls are actually on neutral position.

WARRANT
Dependable Waterborne Digitalisation

WARRANT HAZOP-BASED METHODOLOGY (FUTURE WORK)

- Evaluate **how different HAZOP variations can be integrated** (and if this is necessary) to reduce unidentified hazardous scenarios that relate to the “CPS-like” characteristics of Remote Operations Systems.

- **Conduct similar case studies** in the other WARRANT Living Labs for different Waterborne Digital Systems (WDS).

- **Support the structure of the WARRANT Knowledge Graph** with knowledge of chains of events (Causes → Deviations → Consequences → Impact on system functionality).

- Examine how the methodology can support the **safety assurance process** for different types of WDS.

Thank you very much for your attention!

Any questions?

Konstantinos Louzis

PhD Candidate, Research Engineer
School of Naval Architecture & Marine Engineering
National Technical University of Athens (NTUA)
klouzis@mail.ntua.gr