

D3.1 DETAILED PLANNING AND COORDINATION OF LLS



Disclaimer

This document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Document Information

Grant Agreement	101202581
Full Title	Waterborne fedeRated systems and models for secuRe and resilieNt operations
Acronym	WARRANT
Deliverable	D3.1: Detailed planning and coordination of LLs
Deliverable Due Date	30.09.2025
Deliverable Submission date	15.10.2025
Work Package	WP3
Lead Partner	NTUA
Leading Author	Konstantinos Louzis
Dissemination Level	Public

Document History

Version	Date	Author	Description of change
0.1	11.08.2025	Konstantinos Louzis	Table of Contents
0.2	19.09.2025	Konstantinos Louzis Dimitris Kaklis Gadi Benmoshe Frederic Kracht Maria Chiara Bodda Argyris Mavrakos Vasso Reppa	Draft text included in Sections 1 - 6
0.3	25.09.2025	Per Håkon Meland	Draft text on resilience engineering and LL1 in section 3.
0.4	25.09.2025	Viviana Seguel	Drafted text on LL2: section 4.1, 4.1.1, 4.1.2
0.5	06.10.2025	Konstantinos Louzis Sofia Koufou	Editing and streamlining sections
0.6	08.10.2025	Dimitris Kaklis Viviana Seguel Frederic Kracht	Revisions by LL Leaders
0.7	09.10.2025	Konstantinos Louzis	Revisions by LL Leaders
0.8	10.10.2025	Konstantinos Louzis Georgia Tsiochantari	Final draft sent to internal reviewers
0.85	13.10.2025	Lars-Andreas Wengersberg Antonis Antonopoulos	Review comments delivered by internal reviewers
0.9	13.10.2025	Konstantinos Louzis	Revisions based on reviewer comments
1.0	14.10.2025	Georgia Tsiochantari	Final version to be submitted

Table of Contents

EXECUTIVE SUMMARY.....	9
1 INTRODUCTION	10
2 LIVING LABS PLANNING AND STRATEGY	13
3 LL1 “DEPENDABLE CONTAINERSHIP DIGITAL SYSTEMS”	18
4 LL2 “DEPENDABLE SMART CONTAINER SYSTEMS WITH ADVANCED SHIP COMMUNICATIONS”	25
5 LL3 “INCREASING THE RESILIENCE OF AUTOMATION IN AUTONOMOUS GREEN VESSELS”	35
6 LL4 “ENHANCED DEPENDABILITY OF REMOTE OPERATION SYSTEMS”	48
7 CONCLUSIONS.....	59
REFERENCES.....	62

List of Figures

FIGURE 1: OVERVIEW OF WARRANT LIVING LABS COMMON WORKFLOW.....	11
FIGURE 2: STRATEGY FOR THE IMPLEMENTATION OF THE WARRANT LLS.	14
FIGURE 3: WP3 TIMELINE IN PROJECT MONTHS INCL. MILESTONES, DELIVERABLES, AND WORKSHOPS.....	17
FIGURE 4: STRUCTURE OF NOVA.	39
FIGURE 5: SIGNAL LEVEL OF NOVA.....	40
FIGURE 6: STRUCTURE OF ELLA.....	41
FIGURE 7: SIGNAL LEVEL OF ELLA.	41
FIGURE 8: SOFTWARE LEVEL OF ELLA.....	42
FIGURE 9: STRUCTURE OF VERA.....	43
FIGURE 10: LL4 DEPENDABILITY LEVERS.....	49

List of Tables

TABLE 1: LIVING LAB PHASES AND OBJECTIVES ADAPTED FROM THE ENOLL HANDBOOK (MALMBERG ET AL., 2017).	10
TABLE 2: INITIAL LIST OF KPIS AND TARGETS TO BE USED FOR THE EVALUATION OF THE WARRANT LLS.....	16
TABLE 3: KPI CATEGORIES AND DEFINITIONS FOR LL1.....	21
TABLE 4: IDENTIFIED RISKS RELATED TO THE IMPLEMENTATION OF LL1.....	24
TABLE 5: KPI CATEGORIES AND DEFINITIONS FOR LL2.....	25
TABLE 6: AVAILABLE RESOURCES TO BE USED IN THE IMPLEMENTATION OF LL2.	30
TABLE 7: PLANNED ACTIVITIES BEFORE AND DURING LL2.....	31
TABLE 8: PLANNED ACTIVITIES AFTER THE COMPLETION OF LL2.....	32
TABLE 9: PLANNED ACTIVITIES IN LL2 THAT SUPPORT THE WORK IN OTHER WPS...	32
TABLE 10: IDENTIFIED RISKS RELATED TO THE IMPLEMENTATION OF LL2 AND MITIGATION MEASURES.....	34
TABLE 11: KPI CATEGORIES AND DEFINITIONS FOR LL2.....	36
TABLE 12: SENSORS OF NOVA.....	40
TABLE 13: SENSORS OF ELLA.....	42
TABLE 14: SENSOR DATA OF ELLA.....	42
TABLE 15: SENSOR DATA OF VERA.....	43
TABLE 16: IDENTIFIED RISKS RELATED TO THE IMPLEMENTATION OF LL3 AND MITIGATION MEASURES.....	47
TABLE 17: LL4 DEPENDABILITY ASPECTS.....	49
TABLE 18: LL4 KPIS.	49
TABLE 19: LL4 HIGH-LEVEL WORK BREAKDOWN STRUCTURE.	53
TABLE 20: LL4 RESPONSIBILITIES.....	54



TABLE 21: LL4 CYCLE 2 GANTT CHART.	56
TABLE 22: LL4 STAKEHOLDERS.	57
TABLE 23: LL4 RISK BREAKDOWN STRUCTURE AND MITIGATION MEASURES.	58
TABLE 24: COMPARATIVE OVERVIEW OF THE WARRANT LLS.	60

Acronyms

Acronym	Explanation
AI	Artificial Intelligence
AIS	Automatic Identification System
AIV	Autonomous Inland Vessels
AML	Adversarial Machine Learning
API	Application Programming Interface
BLE	Bluetooth Low Energy
BNWAS	Bridge Navigational Watch Alarm System
CCNR	Central Commission for Navigation on the Rhine
DAL	Design Assurance Levels
DDS	Data Distribution Service
DLT	Distributed Ledger Technologies
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DT	Digital Twin
DTM	Digital Terrain Model
DTLF	Digital Transport and Logistics Forum
ECDIS	Electronic Chart Display and Information System
EMSA	European Maritime Safety Agency
ENoLL	European Network of Living Labs
EU	European Union
FDIR	Fault Detection, Isolation, and Recovery
GA	Grant Agreement

GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPU	Graphical Processing Unit
GSM	Global System for Mobile Communications
HAZOP	Hazard and Operability Study
HE	Horizon Europe
HF	Human Factors
HIL	Hardware-in-the-Loop
HIRA	Hazard Identification and Risk Assessment
HMI	Human-Machine Interface
IACS	International Association of Classification Societies
IDS	Intelligent Dependability Supervisors
IEC	International Electrotechnical Commission
IMO	International Maritime Organization
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
IPR	Intellectual Property Rights
ISM	International Safety Management
ISO	International Organization for Standardization
IT	Informational Technology
KG	Knowledge Graph
LAN	Local Area Network
LiDAR	Light Detection and Ranging

LL	Living Lab
LLM	Large Language Model
LOS	Line Of Sight
NMD	Near-Miss Detection
MASS	Maritime Autonomous Surface Ship
MTBF	Mean Time between Failure
ML	Machine Learning
MLOps	Machine Learning Operations
MTTD	Mean Time to Detect
MTTR	Mean Time to Repair
NGO	Non-Governmental Organizations
OA	Open Access
ODM	Object Detection Model
OEM	Original Equipment Manufacturer
OPEX	Operating Expense
OT	Operational Technology
PLC	Programmable Logic Controller
QoS	Quality of Service
QSHE	Quality, Safety, Health, Environment
R&D	Research & Development
RBAC	Role-Based Access Control
RBS	Risk Breakdown Structure
RLO	Remote Lock Operation
ROC	Remote Operations Centre
ROS	Remote Operations Systems
RTSP	Real-Time Streaming Protocol
SA	Situational Awareness

SBOM	Software Bill of Materials
SCADA	Supervisory Control And Data Acquisition
SCSC	Smart Container-ship Connectivity
SDS	Safety Data Sheet
SIL	Software-in-the-loop
SMC	Sliding Mode Control
SMP	Safety Management Plan
SOP	Standard Operating Procedure
SRODS	Safe, Secure and Resilient Operations of Digitalized Ships
STPA	System-Theoretic Process Analysis
UCA	Unsafe Control Action
VCS	Vehicle Control System
VHF	Very High Frequency
VTs	Vessel Traffic Services
WAN	Wide-Area Network
WBS	Work Breakdown Structure
WDS	Waterborne Digital Systems
WP	Work Package

Executive Summary

This deliverable presents the WARRANT Living Labs (LLs), designed to test and validate the WARRANT Methodology and tools with the objective to improve the dependability of Waterborne Digital Systems (WDS). By establishing a feedback loop between relevant stakeholders and WP1/WP2 technical outputs, the LLs ensure that methodologies and tools are grounded in real operational needs.

Four LLs illustrate the application of the WARRANT methodology:

- **LL1: Dependable Containership Digital Systems** – Focuses on integrated digital ship systems. Using Digital Twin simulations, LL1 tests resilience to faults and cyber threats, defining KPIs such as uptime, recovery time, and incident detection accuracy.
- **LL2: Smart Container Systems** – Examines IoT-enabled, smart containers that enable advanced tracking capabilities. LL2 validates connectivity, hazard detection and operational metrics, aligned with the WARRANT dependability framework.
- **LL3: Resilient Automation in Autonomous Green Vessels** – Investigates automation and monitoring on low-emission, autonomous inland vessels. LL3 integrates digital twins, HIL/SIL simulations, cybersecurity and predictive control to enhance resilience, fault tolerance and performance.
- **LL4: Enhanced Dependability of Remote Operation Systems** – Enhances remote operations within the operational contexts of the Rhine and Antwerp ports. LL4 targets connectivity, situational awareness, vehicle control and HMI, with activities including AI-based object detection, hazard analysis, near-miss detection and remote lock operations.

The deliverable also presents:

- A common Living Lab implementation approach, structured around exploration, experimentation, and evaluation phases.
- Stakeholder engagement methods tailored to each LL.
- Interaction with WPs, highlighting feedback loops and alignment with the WARRANT dependability framework.

This deliverable provides a comprehensive overview of LL objectives, methodologies, interactions and expected outcomes, demonstrating measurable improvements in WDS dependability, resilience and security.

1 Introduction

1.1 Goal and Objectives

The goal of D3.1 is to describe how the WARRANT Living Labs (LLs) will be conducted to establish a feedback loop between stakeholders of the WARRANT methodology and tools for ensuring dependable Waterborne Digital Systems (WDS) and the technical work that will be carried out in WP1 and WP2.

According to the WARRANT Grant Agreement (GA), the specific objectives of the LLs include the following:

- Gathering of essential requirements based on understanding stakeholder needs for guiding the development of the methodology and tools.
- Testing of the technical results from WP1 and WP2, gathering feedback, and refining.
- Quantifying the impact of the WARRANT results with respect to enhancing the dependability of WDS, focusing on safety, security, and resilience.
- Providing a roadmap for ensuring the sustainability of the LLs beyond the project to support post-project exploitation of the WARRANT results.

WARRANT will establish four (4) LLs, each focusing on use cases associated with different WDSs where the WARRANT methodology and tools will be tested and evaluated with respect to the improvement of different aspects of dependability. The activities to be conducted in the LLs will result in the development of Blueprints for dependable WDS, one for each system that will be the object of analysis in each LL (R10 – R13 described for the fulfilment of Project Objective 3 in the WARRANT GA). Each Blueprint will be communicated to relevant external stakeholders in dedicated workshops with at least 20 participants according to the timeline that is described in this document.

As defined by the European Network of Living Labs (ENoLL), a LL actively involves relevant stakeholders in the development process by interacting with the “product” in a real-life setting. According to the Living Lab Methodology Handbook (Malmberg et al., 2017), LLs involve the phases of **exploration, experimentation, and evaluation** where, following the experimental paradigm, a pre-measurement, an intervention, and a post-measurement take place respectively (see Table 1).

Table 1: Living Lab phases and objectives adapted from the ENoLL handbook (Malmberg et al., 2017).

Phase	Objective	Main output
Exploration	Understanding the “current state” and designing possible “future states”	Prototype
Experimentation	Real-life testing of one or more proposed “future states”	Stakeholder feedback
Evaluation	Assessing the impact of the experiment on the “current state”	Value proposition (exploitation)

The workflow that will be used for all WARRANT LLs will follow this 3-phase structure (see Figure 1). The “Exploration” phase will be conducted in WP1 and WP2, where the “prototypes” of the WARRANT methodology and tools will be developed. The testing and validation activities (incl. performance testing, reliability assessments, and safety evaluations) that will be conducted in the “Experimentation” phase will provide feedback to the technical WPs for refinement and ensure that the “prototypes” tested within the LLs are viable for real-world application in waterborne transport. A harmonised list of KPIs will be used during the “Evaluation” phase where the impact of the “experiments” will be quantified with respect to the KPI baseline. The results of the “Evaluation” phase will be used to document the lessons learned from the WARRANT LLs, as well as to draft the plan for sustaining the LLs post-project, which will be included in D3.2 – D3.5.

WP3 will provide input to T4.2 that will determine the value proposition for the WARRANT methodology and tools, as well as inform T4.3, where cybersecurity training material will be developed, in terms of threat awareness of potential malicious interventions/agents.

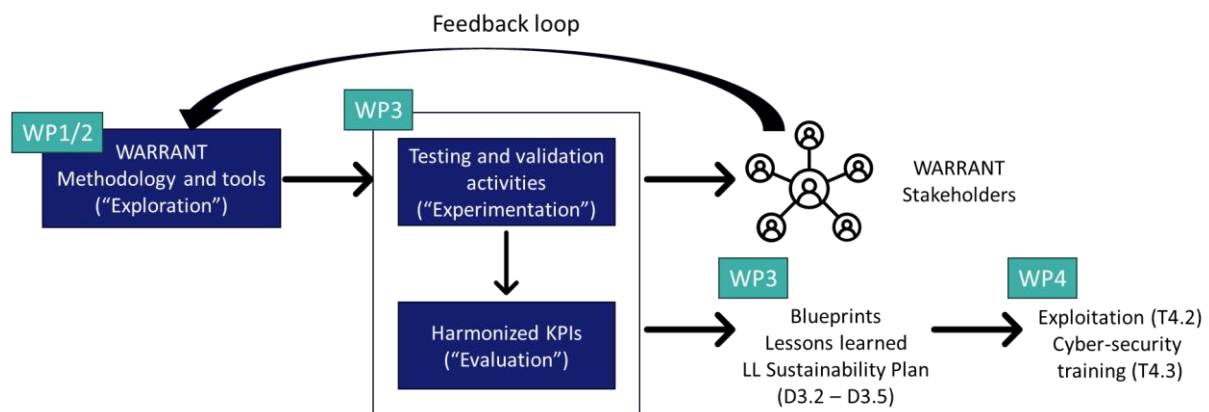


Figure 1: Overview of WARRANT Living Labs common workflow.

1.2 MAPPING WARRANT OUTPUTS

The purpose of this section is to map WARRANT Grant Agreement commitments, both within the formal Deliverable and Task description, against the current document.

WARRANT GA Component Title	WARRANT GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D3.1 Detailed planning and coordination of LLs	This deliverable ensures effective coordination and planning of Living Labs (LLs) to test WARRANT methodologies in real-world maritime environments. It includes a detailed activity roadmap and Key Performance Indicators (KPIs) for evaluation. Success is validated through stakeholder	Sections 3 – 6	Descriptions of LLs 1 – 4 include specific KPIs that will be quantified to show improvements in different aspects of dependability, a timeline of the planned activities

WARRANT GA Component Title	WARRANT GA Component Outline	Respective Document Chapter(s)	Justification
	approval of the plans and alignment with project objectives, as outlined in Task T3.1.		by the involved project partners, and how stakeholders will be engaged in the LL activities.
TASK			
T3.1 Detailed planning and coordination of LLs	This task will ensure that the LLs will be implemented in a unified and coordinated way to achieve WP3 objectives in line with the LL descriptions in section 1.2.5. A suite of techniques will be used with reference to the toolkit for cocreation of the European Network of LLs.	Section 2	D3.1 describes the common methodological approach for the implementation of the LLs, including techniques from the ENoLL handbook.
ST3.1.1 Develop a comprehensive plan for the Living Labs expanding and refining the descriptions provided in section 1.2.5	Develop a comprehensive plan for the LLs, including common testing and evaluation processes, ensuring consistency across all LLs.	Section 2	D3.1 describes the common evaluation framework that will consolidate the KPIs that will be quantified in the LLs.

2 Living Labs Planning and Strategy

2.1 Strategy

Living Labs (LL1–LL4) are the operational backbone of WARRANT. They serve as real-world proving grounds where vessel systems, smart containers, inland automation, and remote operations are tested under authentic conditions. Data and insights from these pilots are continuously fed into the **WARRANT Knowledge Platform (encompassing the Digital Twin infrastructure, Dataspace, and Knowledge Graph).**

This creates a **bi-directional improvement loop** (see Figure 2):

- **From operations to models:** incidents, anomalies, cyber events, and human–machine interaction feedback expand hazard libraries, strengthen cybersecurity toolchains, refine resilience controllers, and update training and procedures.
- **From models back to operations:** validated assurance cases, tuned resilience parameters, regulatory-compliant updates, and improved operator training are redeployed to the Living Labs.

Through federated learning and continuous updating, the WARRANT Knowledge Platform ensures that dependability models and assurance cases evolve in step with **real-world practices, regulatory changes (IMO, IACS, CESNI), and technological innovations (AI assurance, green IT, secure communications).** The result is a methodology that remains not only compliant and dependable today, but also adaptive and future-proof.

WARRANT Continuous Improvement Loop: Living Labs (LL1–LL4) provide operational data to the WARRANT Knowledge Platform. The platform updates hazard libraries, cybersecurity toolchains, resilience controllers, training and procedures, and regulatory solutions. Validated models and assurance cases are then returned to the Living Labs, creating a cycle of continuous evolution.

Hazard Libraries, Cybersecurity Toolchains, Resilience Controllers, and Regulatory/Technological Solutions all connected to and updated via the DT infrastructure.

The DT acts as the backbone enabling federated learning, assurance updates, and continuous evolution across LL1–LL4.

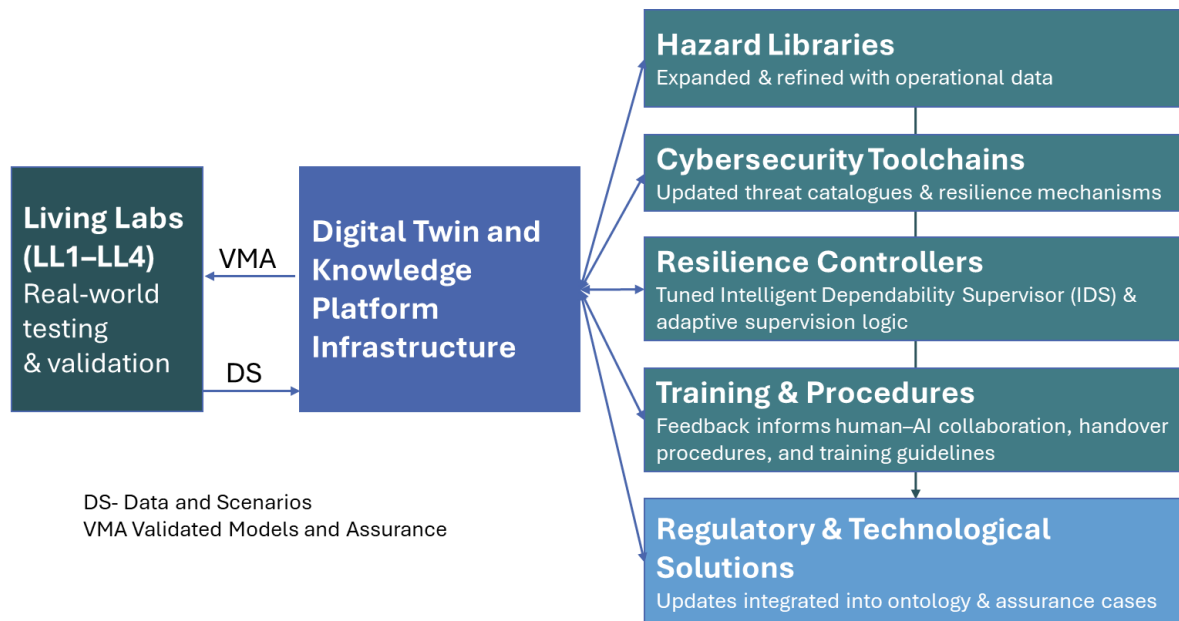


Figure 2: Strategy for the implementation of the WARRANT LLs.

WARRANT Continuous Improvement Loop: Living Labs (LL1-LL4) provide operational data to the WARRANT Knowledge Platform. The platform updates hazard libraries, cybersecurity toolchains, resilience controllers, training and procedures, and regulatory solutions. Validated models and assurance cases are then returned to the Living Labs, creating a cycle of continuous evolution.

Hazard Libraries, Cybersecurity Toolchains, Resilience Controllers, and Regulatory/Technological Solutions all connected to and updated via the DT infrastructure.

The DT acts as the backbone enabling federated learning, assurance updates, and continuous evolution across LL1-LL4.

The Living Labs are tightly integrated with the WARRANT Knowledge Platform, creating **bi-directional feedback loops**:

- **Operational Data → Hazard Libraries:** Incidents, near-misses, and anomalies captured during LL trials expand and refine hazard and risk catalogues, ensuring that HAZOP/STPA analyses remain relevant.
- **Cybersecurity Insights → Toolchains:** Lessons from cyber incident simulations and intrusion testing are translated into improved vulnerability models, updated threat catalogues, and refined detection/response mechanisms.
- **Resilience Controller Tuning → Methodology Refinement:** The performance of Intelligent Dependability Supervisors (IDS) and resilience controllers is evaluated under real-world conditions, with parameters fine-tuned to balance safety, efficiency, and compliance.

- **Human Factors → Training & Procedures:** Feedback from operators and shore-based staff informs improvements in human-AI collaboration, handover procedures, and training guidelines.

Evolution with Regulation and Technology

The maritime regulatory landscape is **continuously evolving**, particularly around cyber resilience (IMO MSC.428, IACS UR E26/E27, EMSA frameworks). WARRANT embeds regulatory updates directly into its feedback cycle:

- New standards are translated into dependability ontology extensions.
- Assurance cases are updated to reflect the latest compliance benchmarks.
- Digital Twins and Knowledge Graphs are enriched with new regulatory attributes, ensuring future-proof certification support.

At the same time, the methodology evolves with **technological innovation**, incorporating advances in AI explainability, federated learning, quantum-resistant cryptography, and green digital infrastructures. In that respect, the expected outcomes are:

- A **continuously improving methodology** that adapts to real-world conditions and regulatory developments.
- **Validated and evolving hazard libraries** that reflect operational reality rather than static assumptions.
- **Cybersecurity toolchains and resilience controllers** strengthened through iterative, LL-driven updates.
- Greater **stakeholder confidence** in WDS and SRODS dependability, supported by transparent evidence of learning and adaptation.

By embedding **continuous feedback and evolution**, WARRANT ensures that its methodology remains not only compliant and dependable today, but also resilient, adaptive, and relevant for the **next generation of digital and autonomous shipping**.

2.2 Harmonised KPI Framework

The objective of the “Evaluation” phase is to quantify the effect on the dependability of the WDSs that will be involved in the WARRANT LLs from the implementation of the WARRANT methodology and tools. To maintain consistency across the LLs and facilitate the drafting of the lessons learned, a common evaluation framework will be developed to ensure that all relevant aspects of dependability will be measured. The main attributes of dependability are the following: reliability, safety, security, resilience, cybersecurity, availability, and maintainability (see Laprie, 1992).

The evaluation framework will consist of the following steps:

1. Creation of a harmonised list of KPIs for each LL, where there is at least one indicator for each aspect of dependability.

2. Determination of the baseline for each KPI in the “current state”.
3. Measurement of the KPIs after the “experiments” in each LL have been conducted.
4. Determination of the effect on dependability by comparing the KPI values with their baseline values.

Table 2 shows the initial list of KPIs, described in the WARRANT GA, which will serve as the basis for the harmonised list to be used for the evaluation of the project LLs.

Table 2: Initial list of KPIs and targets to be used for the evaluation of the WARRANT LLs.

Dimension	KPI	KPI Targets			
		LL1	LL2	LL3	LL4
Availability	Mean Time Between Failures (MTBF)	+15%	+10%	+20%	+15%
Recovery	Mean Time to Recovery (MTTR)	4h → 1h	N/A	2h → 30 min	3h → 1h
Hazard Detection	Time to detect & report hazard	Cyber-attack ≤5 min	Fire/overboard ≤5 min	Failure ≤5 min	Connectivity /AI anomaly ≤5 min
Cybersecurity	Unauthorized access incidents	<1/year	Zero	<1/year	Zero
Regulatory Compliance	% compliance with IMO/IACS/CESNI standards	95%	95%	90%	95%
Efficiency Gains	Cost/operational savings	€5M/year	95% tracking accuracy	+15% fuel/emission efficiency	+10% OPEX reduction
Human Factors / Training Effectiveness	% of operators/crew correctly applying updated procedures in validation trials	90%	85%	90%	95%

2.3 Timeline overview

The results of the WARRANT LLs will be communicated to the stakeholders that will be included in the WDS Alliance, which will be established in M12, through a series of workshops where more than 20 participants from different organization categories will be invited to each event (see Figure 3).

The first workshop in M5 will be conducted with participants from organizations, such as shipping companies, cyber-security solutions providers, and ship digital tools developers. The scope of this workshop will include the detailed plan for the LLs, as well as refined descriptions. The Blueprint for each WDS that will be involved in the LLs will be presented to the WDS Alliance in separate workshops between M14 and M28.

LL3 will produce the following two Blueprints and present them in two separate workshops:

- Blueprint for autonomous green vessels WDS.
- Blueprint for Dependable Smart IW Mobility WDS.

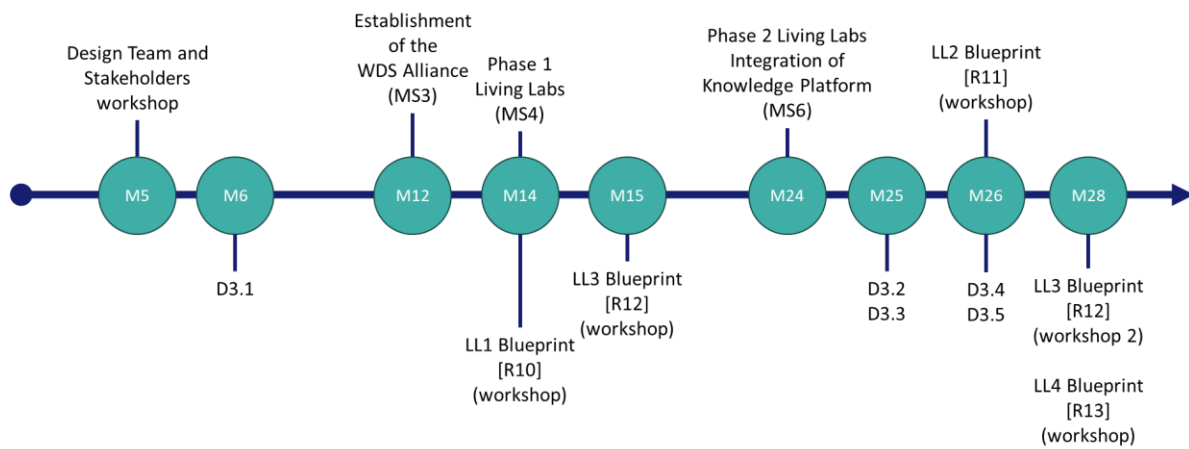


Figure 3: WP3 timeline in project months incl. Milestones, Deliverables, and Workshops.

3 LL1 “Dependable Containership Digital Systems”

3.1 Scope and Specific Objectives

LL1 will be carried out on large containerships operated by Danaos and focuses on their digital systems. These vessels depend on integrated platforms for navigation, engine control and ship-to-shore communication. The aim is to make these systems more dependable and resilient in the face of faults and cyber threats. Using the WARRANT methodology, we will evaluate how vulnerable the systems are, how well they can withstand disruptions, and how fast they can recover. A Digital Twin of the ship’s systems will support this work, allowing us to simulate different failure and attack scenarios without putting the vessel at operational risk. The specific objectives are to assess the ship’s digital resilience, improve fault detection and recovery, and establish clear indicators of dependability such as uptime, response time and accuracy of incident detection.

The specific objectives related to Hollnagel’s four cornerstones of resilience engineering are (Hollnagel, 2009):

- **Anticipating:** Identify potential vulnerabilities, attack paths and mitigations through cyber risk assessment.
- **Responding:** Test how resilient the ship’s digital systems are against cyber incidents.
- **Monitoring:** Improve monitoring and fault detection using Digital Twin technology.
- **Learning:** Define KPIs for dependability, such as system uptime, recovery time after fault occurrence, and accuracy of incident detection.

3.2 Living Lab Challenges

LL1 demonstrates the WARRANT methodology on a large containership, focusing on **cybersecure navigation systems** and the deployment of **assurance Digital Twins (DTs)**. Danaos, as one of the world’s largest containership operators, faces increasing challenges in effectively managing cybersecurity while ensuring compliance with evolving regulatory frameworks (IMO cyber-risk management guidelines, IACS E26/E27).

Current practice exposes several **practical challenges**:

- **Fragmented cybersecurity assurance:** Navigation and propulsion, are often modelled independently, with limited integration across ship subsystems. This complicates compliance reporting and weakens resilience against multi-vector attacks (e.g., GNSS spoofing combined with ECDIS corruption).
- **Gap between models and reality:** WDS dependability models developed in research or design phases often diverge from the actual configuration and operating conditions of LL

ships. Bridging this gap requires systematic mapping between the abstract models of WP1 and the real-world systems aboard Danaos vessels.

- **Reactive security posture:** Many operators rely on post-incident analysis or manual audits to identify vulnerabilities, rather than continuous assurance. This delays detection and mitigation of emerging threats and does not meet the expectations of regulators for proactive cyber resilience.
- **High compliance overheads:** Demonstrating conformity with regulations (e.g., IMO MSC.428, class rules) requires significant manual effort to compile assurance cases, test scenarios, and document resilience measures. Without automated, DT-supported assurance, compliance becomes costly and inconsistent.

Through LL1, Danaos addresses these challenges by:

- **Cybersecure Navigation Focus:** Applying advanced hazard analysis (HAZOPS/STPA) and vulnerability testing (spoofing, jamming, network attacks) to real-world navigation and bridge systems, feeding into a **comprehensive assurance Digital Twin**.
- **Model-Reality Mapping:** Creating traceability between WP1 WDS models and actual LL ship architectures. This mapping ensures that theoretical dependability frameworks are validated, calibrated, and continuously updated with operational data.
- **Resilience Controllers in Action:** Testing the Intelligent Dependability Supervisor (IDS) and adaptive resilience controllers to detect, isolate, and respond to navigation system failures or cyberattacks in real time, maintaining COLREG-compliant operations under degraded conditions.
- **Compliance by Design:** Embedding regulatory requirements into the Digital Twin environment, enabling automatic generation of assurance cases aligned with IACS cyber resilience standards. This reduces the compliance burden while improving audit readiness.
- **Training & procedures:** operator feedback integrated into bridge procedures and crew training guidelines, ensuring safe human-AI handovers and COLREG compliance as part of the assurance toolchain.

In doing so, LL1 delivers not only a **Blueprint for Dependable Containership WDS** but also a practical roadmap for shipping companies to **transform cybersecurity management from reactive compliance to proactive, resilience-driven assurance**.

3.3 Use cases

Cyber-attack on navigation systems: simulate disruptions and test recovery strategies

Objective:

Evaluate and enhance the dependability and resilience of the vessel's navigation and control systems against deliberate cyber intrusions (e.g. GPS/GNSS spoofing, AIS manipulation, ECDIS data corruption, DoS attacks on shipboard networks).

The experiment will analyse how quickly and effectively both automated systems and crew can detect, isolate, and recover from disruptions, ensuring coordinated resilience between ship and port digital infrastructures (e.g., within a port call optimization scenario).

This objective directly supports **KPI-1 to KPI-5** on safety, resilience, detection, and recovery times, and contributes to **KPI-7** (operational efficiency) and **KPI-8** (cybersecurity compliance).

Approach:

Digital Twin-based Simulation Environment

- Develop and deploy a high-fidelity **WDS Digital Twin** for the ZIM LUANDA, replicating real-time navigation data streams (GPS, AIS, ECDIS, radar, GNSS).
- Integrate sensor fusion, hazard identification (HAZOPS, STPA), and dependability enhancement tools based on the **WARRANT methodology** and Knowledge Graph (KG).

Controlled Cyber-attack Scenarios

- Simulate multiple attack vectors: GPS/GNSS spoofing or jamming (Galileo/EGNOS), AIS data falsification, ECDIS data corruption, VTS intrusion, and onboard network denial-of-service.
- Use ethical hacking and vulnerability assessment techniques to validate attack surfaces and system behaviour.
- Incorporate **Generative AI models (LLMs)** to automatically generate and test synthetic threat scenarios within a safe sandbox.

Dependability and Recovery Evaluation

- Measure the **Mean Time to Detect (MTTD)** and **Mean Time to Recovery (MTTR)** for each simulated incident.
- Evaluate system downtime, recovery effectiveness, and compliance with cybersecurity standards (ISO 27001, IMO MSC-FAL.1/Circ.3).
- Use Knowledge Graphs to map interdependencies among navigation subsystems and identify potential cascading failures or single points of failure.

Human–Machine Collaboration Assessment

- Involve crew in simulated response exercises to measure human-in-the-loop decision-making, communication, and response time.
- Assess integration of the **Intelligent Dependability Supervisor (IDS)** to guide optimal recovery actions and human performance under stress.

Cross-LL Collaboration

- Share findings with other LLs focusing on container management and remote operations to refine assurance processes and improve shared resilience models across ship-port digital ecosystems.

Expected outcomes:

- Identification of weak links in navigation data fusion and cyber hygiene.
- Reduction in number of incidents and system downtime improving safety resilience and operational efficiency.
- Assessment of crew and automation response time through human-machine interfacing
- Validation of **recovery strategies**, such as switching to redundant systems or manual navigation modes.

Table 3 demonstrate a detailed list of expected KPIs as referenced in the GA.

Table 3: KPI categories and definitions for LL1.

Category	ID	Description	Metric	Target
Safety and Resilience	KPI-1	Reduction in accident rate attributable to digital system vulnerabilities	% decrease in accidents or incidents	>10% decrease
Safety and Resilience	KPI-2	Mean Time to Recovery (MTTR): average time to restore full functionality after system failure or cyberattack	Hours	4h (2023) → 1h (2028)
Safety and Resilience	KPI-3	System downtime due to cyberattacks on WDS	% of total downtime	5% (2023) → 2.5% (2028)
Safety and Resilience	KPI-4	Reduction in number of cybersecurity incidents detected within WDS	Number of incidents	15 (2023) → 5 (2028)
Safety and Resilience	KPI-5	Mean Time to Detect (MTTD): improved average time to detect cybersecurity incidents	Time (hours/minutes)	2h (2023) → 30min (2028)
Safety and Resilience	KPI-6	Potential cost savings from reduced downtime, fewer accidents, and less reactive maintenance	€ savings	€2M (2023) → €5M (2028)
Operational Efficiency	KPI-7	Improvement in operational efficiency due to more reliable and secure digital systems	% improvement	15% (2023) → 35% (2028)

Category	ID	Description	Metric	Target
Cybersecurity Compliance	KPI-8	Compliance with cybersecurity standards achieved through proposed solutions	% compliance	60% (2023) → 95% (2028)

3.4 Living Lab Structure

The Living Lab will be organised around three phases: exploration, experimentation and evaluation. During the exploration phase, the current state of the ship's digital systems will be analysed to establish a baseline. The experimentation phase will involve controlled trials, within the Digital Twin, where faults and cyber incidents will be introduced. The evaluation phase will then compare the results against the baseline, allowing the methodology to be refined and validated. This cycle will be repeated to ensure improvements are consistent and robust.

- **Exploration** – understand current system design and vulnerabilities.
- **Experimentation** – run pilot tests with simulated faults and cyber threats.
- **Evaluation** – measure KPIs and refine methods with crew and technical experts.

3.4.1 Available Resources

The work will rely on a combination of physical and virtual resources. Danaos Shipping will provide access to a containership and its ship management systems, including navigation, and propulsion systems. The WARRANT frame will employ a Digital Twin environment, for cybersecurity and resilience assessment methods. Crew members and operators will provide practical input to ensure that the solutions tested are grounded in real operational needs. Below we demonstrate briefly the available resources required to realize LL1 UC. Data analytics and monitoring platform provided by Danaos Shipping:

- **Ship management systems** including navigation, engine and propulsion.
- **WDS Digital Twin** continued from DT4GS project (<https://www.dt4gs.eu/>) and redefined within WARRANT. (*ST3.2.1 Cybersecurity and Resilience of Navigation Digital System*).
- **Cyber range and testing environment** for simulating attacks and failures.
- **Crew and operator input** from Danaos for operational validation.

3.4.2 Activities and roles

Danaos will lead LL1 and host the experiments, providing operational expertise and access to vessels. SINTEF and NTUA will carry out cybersecurity and resilience assessments, ensuring the tests are technically rigorous. INLECOM will focus on supporting the integration of the Digital Twin with the ship's systems, by mapping SDS to KG components and generate adversarial attack scenarios to test the mitigation procedures proposed by the DT. DNV will support the dependability evaluation and the definition of key metrics. Together, the partners will plan and execute the experiments, analyse the results and refine the methodology. These activities are further explained below:

- SINTEF and NTUA will implement the risk assessment techniques developed in WP1 and WP2, which are based on HAZOP and STPA, to identify potential hazards related to the ship systems that will be examined in LL1 and develop tailored risk mitigation strategies focused on improving cybersecurity and resilience.
- TECNALIA will conduct comprehensive vulnerability assessments, including GNSS (GNSS, specifically Galileo and EGNOS spoofing/jamming, AIS signal manipulation, ECDIS data corruption, VTS system hacking, and insecure shipboard network communications. Perform penetration testing and ethical hacking exercises. Attack pathways and specific scenarios will be dictated by domain experts and regulatory frames. In a later stage, Generative Models (LLMs) will be trained to combine readily available knowledge with standardized protocols to produce arbitrary scenarios to test and validate in full extent the integrity and transparency of digital systems on-board the vessel.
- KONNECTA and SINTEF Digital will test WDS Dependability Assessment and Enhancement Management. Identify and evaluate optimum enhancements using the WDS KG for navigation systems. Utilize the Library of Innovative WDS Cybersecurity and Dependability Enhancements to address identified vulnerabilities effectively.
- DNV will investigate the assurance process by following WARRANT Methodology guidelines. Develop standardized protocols for sensor data collection and fusion, ensuring compliance with cybersecurity and dependability standards. Conduct periodic reviews and updates based on emerging threats and technological advancements.

3.4.3 Timeline of planned activities

In the first year of the project the focus will be on system mapping, establishing baseline KPIs and developing the Digital Twin. The second year will be dedicated to running the first round of experiments, introducing cyber and fault scenarios to measure the impact on system dependability. The third year will refine these experiments, repeating them with adjustments and validating the outcomes with direct crew involvement. The final months will be used to consolidate the results and report on the lessons learned.

- **M6–M12:** system study, baseline KPIs, and setup of Digital Twin.
- **M12–M18:** first round of experiments (cyber and fault scenarios).
- **M18–M24:** evaluation and refinement of tools.
- **M24–M30:** second round of experiments, validation with crew.
- **M30–M36:** final assessment, results reporting, and input to exploitation tasks.

3.5 Stakeholder Engagement

Stakeholders will be actively involved throughout the Living Lab. Shipowners, operators, classification societies, technology suppliers and cybersecurity providers will be engaged through the WDS Alliance and invited to dedicated workshops. Crew feedback will be gathered during and after the pilot runs to capture operational perspectives by integrating innovative tools for

automated feedback collection and evaluation (see, e.g., <https://unalab.enoll.org/>). Class societies will also be consulted to ensure that the results are aligned with evolving regulatory requirements.

3.6 Implementation Risks

There are some expected challenges in implementing LL1, which are listed along with the mitigation measures in Table 4.

Table 4: Identified risks related to the implementation of LL1.

#	Risk Category	Risk Description	Mitigation Measure(s)
R1	Integration of operating systems	Limited access to real ship systems	Using the Digital Twin as a complementary environment for testing
R2	Confidentiality	Handling of sensitive data related to system vulnerabilities	Strict confidentiality measures
R3	Integration of operating systems	Running experiments on commercial vessels could interfere with operations	Pilots will be carefully scheduled and often shifted to controlled or simulated settings
R4	Integration of operating systems	Integration of new methods with existing ship systems is technically demanding	Phased approach supported by the technical partners

4 LL2 “Dependable Smart Container Systems with advanced ship communications”

4.1 Scope and Specific Objectives

LL2 will be carried out using an AELER smart container, as part of the existing technology, and integrating the live data transmission to the Control Tower, via the containerships system. This will be conducted on a first basis on a digital twin of the vessel's system to be able to test and run hazard scenarios, before being tested on a real vessel.

4.1.1 Objectives

LL2 objectives include establishing a robust baseline for continuous and accurate location tracking of containers throughout their journey. Enabling real-time monitoring and verification of container status during vessel transit and at port operations, including loading and unloading phases.

The objective is to develop:

- Resilient connectivity models that ensure uninterrupted communication across shipboard systems.
- Reliable hazard detection mechanisms capable of identifying threats such as fire or container loss overboard.
- Enhanced operational metrics to assess system performance and response under the most common incident scenarios, fire on board and loss of container overboard

Dependability KPI's

LL2 will establish container vessel and port interoperability, enhancing reliability and resilience under hazard scenarios, ensuring appropriate assurance measures are in place. An initial list of KPIs, as described in the WARRANT GA, is shown in Table 5.

Table 5: KPI categories and definitions for LL2.

Category	ID	Description	Metric	Target
Dependability	1.1	Connectivity Robustness via GSM (on land and international waters via BLE (or any non-proprietary alternative) on board	Percentage of time Smart Container message/ signal is available: before loading, on board, international waters upon arrival	95% signal availability

Category	ID	Description	Metric	Target
Safety Assurance	1.2	Communication Reliability via APIs	Successful data transmissions	99% successful transmissions
	2.1	Fire Detection Response Time	Average time taken to detect and report a fire incident	Within 5 minutes of temperature threshold breach
	2.2	Container Overboard Detection Time	Average time to detect and report a container lost at sea	Within 5 minutes of the incident
Operational Efficiency	3.1	Real-time Tracking Accuracy	Percentage accuracy of container location data	95% of location data fall within a 100m radius
Cybersecurity and Data Integrity	4.1	Unauthorized Access Attempts Mitigation	Number of unauthorized access attempts detected and mitigated	Zero successful unauthorized access incidents
Stakeholder Satisfaction	5.1	User Satisfaction Rating (which will be measured by: ease of use, information obtained from the integration, willingness to adopt when it will be commercialized)	Average satisfaction rating from vessel crew and port personnel	90% satisfaction rate

4.2 Living Lab Challenges

LL2 applies the WARRANT methodology to **smart containers**, with a primary focus on dependable fire detection and container-overboard alerts. A central difficulty arises from current industry practice: container monitoring systems are often **isolated from the ship's LAN and operational infrastructure**. This lack of integration creates critical hazards:

- **Delayed or lost alerts:** If a container fire or overboard event is detected by the container's own sensors but not relayed in real time to the vessel's bridge systems, response time is severely compromised, increasing risks to safety, cargo, and the environment.
- **Fragmented situational awareness:** Crew and automated ship systems (e.g., ECDIS, integrated bridge systems, or emergency management platforms) lack a unified view of container conditions, which can result in overlooked hazards or conflicting data streams.
- **Weak assurance cases:** Because container data remains external to the ship's LAN, classification societies and regulators cannot rely on it as part of formal safety and cybersecurity assurance cases, limiting compliance with IACS E26/E27 and IMO cyber-risk management guidelines.
- **Cybersecurity exposure:** Unconnected or ad-hoc wireless relay channels (e.g., GSM, Wi-Fi, BLE) used by containers may bypass shipboard security layers, creating unmonitored entry points for cyber threats.

The LL2 use case therefore targets **closing this connectivity gap** by embedding container monitoring into the ship's LAN and Digital Twin infrastructure, thereby extending vessel loading

awareness while preserving the integrity and dependability of the vessel's digital systems. This enables:

- **Reliable and dependable real-time alerting** to bridge and crew for fire or overboard events, demonstrating measurable improvement in safety, responsiveness, and human-machine coordination in accordance with the WARRANT KPI framework.
- **Integration of operational data into the WARRANT hazard and dependability libraries**, enabling validation and refinement of the methodology's risk analysis and assurance tools through real-world container-ship interaction scenarios.
- **Implementation of secure and resilient communication architectures**, applying WP2 cybersecurity and resilience mechanisms to ensure that container-to-ship data flows are encrypted, authenticated, and fault-tolerant.
- **Validation of Digital Twin-based assurance processes**, using LL2 experiments to quantify how the inclusion of smart container data improves overall WDS dependability and compliance with emerging IMO/IACS cybersecurity and resilience standards.
- **Illustration of the WARRANT methodology's applicability to multi-layered WDS**, showing how dependability can be systematically enhanced by integrating container-level intelligence into ship-level digital infrastructures through co-simulation, assurance modelling, and KPI-based evaluation.
- **Training & procedures**: crew awareness and emergency response procedures updated to incorporate container-level hazard alerts, supported by training modules linked to the Digital Twin and codified into procedural assurance cases.

4.2.1 Use cases

4.2.1.1 Fire on board or during cargo handling at port

Monitoring of temperature changes, identification of deviation from the allowed threshold and transmission of temperature data together with container number and time stamp to the appropriate system according to the situation.

Detecting fire in smart container systems will be addressed by developing a distributed architecture for ensuring modularity and scalability, developing monitoring agents and intelligent dependability supervisors (Task 1.3) for the container systems. The focus will be the design of a monitoring agent for every container system that will infer the release of a fire by comparing the measurements of temperature and humidity sensors (maybe pressure and oxygen sensors as well) with the expected temperature and humidity estimated using thermodynamic models.

Considering the existence of uncertainties, such as varying environmental temperature in each mission, sensor noise etc, the design of an adaptive threshold will aim to reduce false alarms and missed detections.

The monitoring agent will be designed to detect anomalies in the thermodynamics of a smart container, and to distinguish between faulty temperature sensors and actual fire or indicate that there may be fire in a neighbouring container. The decisions of the monitoring agents for the smart

containers will be aggregated by the global agent that by applying dynamic decision-making AI method (e.g. combinatorial logic) to conclude about the existence of fire or faulty sensors. In the case of faulty temperature sensors, other sensors (e.g. humidity, pressure) will be used to reconstruct the measurements of temperature (virtual sensors) and allow continuous monitoring. Special attention will be given to isolating the container on fire among many containers stacked on board the vessel or on the stacking yard at port. Based on the decision of the monitoring agents, the intelligent dependability supervisor will decide about the best actions to contain the fire, depending on any relevant existing regulation and the transport mode the containers are as listed below:

- **In transit:** to vessel, enabling localization of the potential fire source on board and prevention of its spread.
- **Loading at port:** to vessel and port, enabling them to abort loading or to activate preventive measures.
- **Unloading:** to vessel and port, enabling them to activate preventive measures before unloading.

At the terminal storage area: to port, enabling localization of the potential fire source in the storage area and prevention of its spread (Optional, in addition to the WARRANT GA).

4.2.1.2 Container Lost at Sea Detection and Response

In maritime logistics, container loss at sea poses serious safety, environmental, and economic risks. To address this challenge, AELER smart containers equipped with onboard communication capabilities can play a critical role in early detection and rapid response. This use case outlines a system where the AELER smart containers continuously report their status to the vessel management system. A sudden loss of signal is treated as a potential overboard incident, triggering automated alerts and location tracking to facilitate swift recovery or mitigation.

System functionality:

- **Continuous Status Reporting:** Each smart container is programmed to periodically transmit an “on board” status signal to the vessel management system. This signal confirms the container’s presence and connectivity within the vessel’s network.
- **Incident Detection Logic:** If a container fails to report within a predefined time interval, the system flags it as a potential “container lost at sea” event. This logic is based on the assumption that loss of signal may indicate physical separation from the vessel, such as falling overboard.
- **Last Known Coordinates Logging:** Upon detecting a missing signal, the system automatically retrieves and logs the last known GPS coordinates of the container. This data is critical for narrowing down the search area and initiating recovery efforts before the container drifts further due to ocean currents.
- **Alert and Response Protocol:** The vessel management system generates an alert for the crew and shore-based operations team. The alert includes:
 - Container ID
 - Timestamp of last signal

- Last known coordinates
- Recommended search radius based on drift modelling
- **Integration with Maritime Safety Systems:** The system can optionally interface with maritime safety and environmental monitoring platforms to:
 - Notify nearby vessels of potential floating hazards
 - Alert coastal authorities if the container is carrying hazardous materials

4.2.1.3 The Robust Smart Container-ship Connectivity (SCSC)

The Robust Smart Container-ship Connectivity (SCSC) system is to ensure uninterrupted and secure communication between smart containers and the vessel management system, even under challenging deep-sea conditions. This use case focuses on deploying the SCSC system in the Living Lab (LL) and later on a vessel as a pilot implementation.

Modern maritime logistics will increasingly rely on real-time data exchange between onboard systems and smart cargo units. However, deep-sea environments pose significant challenges to connectivity due to limited access to terrestrial networks and fluctuating signal conditions. The SCSC system addresses these challenges by integrating multiple communication channels—relay, GSM, Wi-Fi, and Bluetooth Low Energy (BLE)—to maintain robust and adaptive connectivity.

DANAOS aims to implement a joint virtual demonstrator with AELER to quantify impact and outcomes by operating and transporting at least one smart 20ft container in a simulated environment. Fully integrated Hardware-in-the-Loop (HIL) or Software-in-the-Loop (SIL) methodologies will be adopted by exploiting the LL1 DT ecosystem and AELERS smart containers IoT systems deriving historical operational data

The use case will revolve around safety and emissions reduction by exploiting innovative container features like advanced insulation ensuring minimum energy demands on sensitive cargo (pharma, food, high-value goods) and sensory measurements for real-time condition monitoring of cargo, as well as more liquid cargo capacity.

Virtual demonstrator will be realized by simulating a round trip cross Atlantic voyage for a candidate DANAOS Living Lab (ZIM LUANDA) transporting sensitive cargo with one of 20ft AELER containers equipped with sensor instalments. Even though the AELER container is already being used by several customers, the data can for now only be collected once the container is back in port. By conducting such voyage, we will be able to stress test the boundaries of the case study under diverse operational conditions (sever weather, parametric rolling identification, cyberattacks, etc), live streaming the data. One main pillar of the use case will revolve around safety by mapping data originated from the container with vessel energy management system and identifying adverse conditions inside the container potentially damaging the cargo and triggering in real-time mitigation measures by instantaneously adapting auxiliaries to address the issue. This automated streamlined procedure will be instantiated by the WARRANT Dependability Supervisor and Digital twin trained on a diverse set of data related to adversarial attacks on ships digital systems and historical data.

In critical conditions where immediate action needs to take place an alerting procedure will be initiated integrated potentially to the ISM manual to engage appropriate personnel on-board to address the issue.

In the logistics chain certain KPIs related to emissions monitoring and cargo transported per TEU need to be established to quantify and extrapolate the impact and savings in financial and environmental terms by exploiting AELER smart container units. Smart sensor system also offers the possibility for DANAOS to better track where containers are, predict when they'll return, and reduce deadhead/ empty repositioning. Furthermore, with better insulation and durability, containers may be usable in more routes without needing special handling or limited to fewer cargo types.

4.3 Living Lab Structure

The Living Lab will operate through a structured cycle comprising three key phases: Exploration, Experimentation, and Evaluation.

- **Exploration:** This initial phase focuses on assessing the Smart container's and the ship's existing digital infrastructure to establish a comprehensive baseline. Explore the thermodynamic models needed for the design of a monitoring agent for the container system. By mapping out the system and identifying vulnerabilities, laying the groundwork for needed improvements.
- **Experimentation:** Controlled trials will be conducted within the Digital Twin environment and later onboard a vessel. The objective for these simulations will be to test system resilience.
- **Evaluation:** Outcomes from the trials will be measured against the established baseline using Key Performance Indicators (KPIs). Additional insights from user's feedback and technical analysis will be used to refine and validate the methodology.

This iterative cycle will be repeated to ensure effectiveness, sustainability and resilience over time.

4.3.1 Available Resources

Table 6: Available resources to be used in the implementation of LL2.

Resource	Provider
Smart container	AELER
Smart container management system	AELER
GSM repeater (if needed)	AELER
Vessel	DANAOS (potential)
Vessel management system	DANAOS (potential)
Port terminal	Terminal operator at Antwerp-Brouge port (potential)
Port terminal management system	Terminal operator at Antwerp-Brouge port (potential)

4.3.2 Activities, roles and timeline

Table 7: Planned activities before and during LL2.

Timeline	Activity and roles	Partner/Stakeholder
M1-M36 4/2025-4/2028	LL Lead	AELER
M6 9/2025	WP3 ST3.1.1: Develop a comprehensive plan for the Living Labs	AELER, NTUA, TU DELFT, INLECOM, DANAOS (potential), Terminal operator at Antwerp-Brouge port (potential)
M7-M13 9/2025-4/2026	Coordination of dates for pilot implementation	AELER, DANAOS (potential), Terminal operator at Antwerp-Brouge port (potential)
M7-M13 9/2025-4/2026	Development needed in the Smart Container system*+**	AELER
M7-M13 9/2025-4/2026	Development needed in the vessel's management system*	DANAOS (potential)
M7-M13 9/2025-4/2026	Development needed in the port's management system**	Port of Antwerp-Brouge (potential)
M7-M13 9/2025-4/2026	Hazard analysis and a cybersecurity vulnerability assessment***	SINTEF, NTUA
M10-M12 1-3/2026	Preparation of Blueprint for Smart container-ship communication system for stakeholder workshop 1	AELER, NTUA, TU DELFT, INLECOM, DANAOS (potential), Terminal operator at Antwerp-Brouge port (potential)
M10-M12 1-3/2026	Coordination of stakeholder workshop 1	AELER, NTUA, TU DELFT, INLECOM, DANAOS (potential), Terminal operator at Antwerp-Brouge port (potential)
M13~ 4/2026	Stakeholder workshop 1	AELER, NTUA, TU DELFT, INLECOM, DANAOS (potential), Terminal operator at Antwerp-Brouge port (potential)
M13 4/2026	Smart container transportation to pilot location	AELER
M13 4/2026	Vessel transport to pilot location	DANAOS (potential)
M14-M15 5-6/2026	Pilot implementation**** 2 Phases: Lab and field	AELER, DANAOS (potential), Terminal operator at Antwerp-Brouge port (potential)
Notes: * API and container<>vessel connectivity via relay or GSM/WIFI/BLE channel open for communication in the deep sea to enable container connectivity via the vessel's Intranet. ** API and container<>port connectivity via relay or GSM/WIFI/BLE channel open for communication in the deep sea to enable container connectivity via ports's Intranet.		

*** To establish a system model for the LL vessel, following a hazard analysis and a cybersecurity vulnerability assessment applying WARRANT methodology and tools to provide robust protection against unauthorized data modification through encryption and secure data transmission to prevent hacking and unauthorized access.

**** Implement digital testing to demonstrate:

1. monitoring of temperature changes, identification of deviation from the allowed threshold and transmission of temperature data together with container number and time stamp to localize the source of (potential) fire on board and prevent its spread.
2. identification of lost containers overboard by updating the coordinates of the last signal to quickly enable the identification of the fallen container before it drifts far from the incident site.
3. the process of real-time temperature notification to the vessel and port systems during loading. If cargo is overheated or the temperature is too close to the limiting threshold, the container will not be loaded, or preventive measures will be applied before loading and departure. (Optional, in addition to the WARRANT GA).
4. the arrival case, transmitting the information about overheated container (e.g. after the transportation on the upper deck on the top of the stack) to the vessel and port systems to activate preventive measures before unloading, e.g. extra inspection or fire-fighting activities. (Optional, in addition to the WARRANT GA).
5. at the terminal storage area case: transmitting the information about overheated container at the terminal storage area to the port systems to activate preventive measures e.g. extra inspection or fire-fighting activities. (Optional, in addition to the WARRANT GA).

Table 8: Planned activities after the completion of LL2.

Timeline	Activity and roles	Partner/Stakeholder
M18-M20 9-11/2026	Update of Blueprint for Smart container-ship communication system for stakeholder workshop 2	Aeler, NTUA, TU DELFT, INLECOM, Danaos (potential), Terminal operator at Antwerp-Brouge port (potential)
M18-M20 9-11/2026	Coordination of stakeholder workshop 2	Aeler, NTUA, TU DELFT, INLECOM, Danaos (potential), Terminal operator at Antwerp-Brouge port (potential)
M21~ 12/2026	Stakeholder workshop 2	Aeler, NTUA, TU DELFT, INLECOM, Danaos (potential), Terminal operator at Antwerp-Brouge port (potential)
M29	D3.3: Report of LL2 Application of the WARRANT Methodology to Smart Container Systems	Aeler, NTUA, TU DELFT, INLECOM, Danaos (potential), Terminal operator at Antwerp-Brouge port (potential)

Table 9: Planned activities in LL2 that support the work in other WPs.

Timeline	Activity and roles	Partner/Stakeholder
M1-M28 4/2025- 7/2027	WP4 ST4.2.1: Innovation, IPR management, and patent applications	AELER, NTUA, TU DELFT, INLECOM, DANAOS (potential), Port of Antwerp-Brouge (potential)
M6-M30 9/2025- 9/2027	WP2 ST2.3.2 DWDS Digital Twinning framework. (M6-M30)	AELER, NTUA, TU DELFT, INLECOM, DANAOS (potential), Port of Antwerp-Brouge (potential)

Timeline	Activity and roles	Partner/Stakeholder
M19-M32 10/2025- 11/2027	WP4 ST4.2.2 Commercialisation strategy	AELER, NTUA, TU DELFT, INLECOM, DANAOS (potential), Port of Antwerp-Brouge (potential)
M22 1/2027	R6 Presentation of a study on the improvement of computational efficiency for risk scenario generation, with demonstration in LL2	AELER, SINTEF, TU DELFT, INLECOM, DANAOS (potential), Port of Antwerp-Brouge (potential)
M6-M30 9/2025- 9/2027	Exploitation Strategy and Methodology, KER 4: WDS Dependability Assessment and Continuous Assurance and Enhancement Management	AELER, NTUA, TU DELFT, INLECOM, DANAOS (potential), Port of Antwerp-Brouge (potential)

4.4 Stakeholder Engagement

Stakeholder categories generally relevant to LL2

- Vessel operators: shipping/charter companies, shipmasters/associations.
- Terminal operators: Port of Antwerp-Bruges (in consortium and potentially in LL).
- Authorities/regulators: Port authorities, IMO.
- Maritime trade organisation: BIMCO.
- Classification societies/insurers: DNV (in consortium), other classes, insurers/risk assessors.
- Service Provider: Vessel/Port management system manufacturers, communication providers, cybersecurity vendors.
- Research/academia: universities/research institutes
- Standardisation bodies: ISO, UNCEFACT

Engagement methods and frequency

As described in the WARRANT GA, the stakeholder engagement will be done through R11: Presentation of Blueprint for Smart container-ship communication system to stakeholder workshop with 20+ participants from container ship companies and containerized transport stakeholders.

One workshop before to the pilot execution (M13 instead of M14 as planned in the proposal) and another after the elaboration of the pilot results (M21 instead of M26 as planned in the proposal). Feedback from the direct users will be collected during and after the pilot.

The workshops will be hybrid, with the opportunity to attend in person or online.

4.5 Implementation Risks

Table 10: Identified risks related to the implementation of LL2 and mitigation measures.

#	Risk Category	Risk Description	Mitigation Measure(s)
R1	Vessel Integration	Not reaching an agreement with a ship owner to allocate a vessel for pilot implementation	Pilot implementation through simulation of a vessel
R2	Vessel Integration	Not reaching an agreement with a ship owner to develop API: vessel management system <> smart container	Pilot implementation through installation of Smart Container management system on a standalone computer on the vessel
R3	Vessel Integration	Not reaching an agreement with a ship owner on the communication method: vessel management system <> smart container	Pilot implementation through installation of Smart Container management system on a standalone computer on the vessel
R4	Terminal Integration	Not reaching an agreement with a terminal operator for pilot implementation	1. Pilot implementation through simulation of a terminal 2. Not implementing this use case (optional)
R5	Terminal Integration	Not reaching an agreement with a terminal operator to develop API: port management system <> smart container	1. Pilot implementation through installation of Smart Container management system on a standalone computer on the terminal 2. Not implementing this use case (optional)
R6	Terminal Integration	Not reaching an agreement with a terminal operator on the communication method: port management system <> smart container	1. Pilot implementation through installation of Smart Container management system on a standalone computer on the vessel 2. Not implementing this use case (optional)

5 LL3 “Increasing the resilience of automation in autonomous green vessels”

5.1 Scope and Specific Objectives

Vision and Motivation

LL3 addresses the design, validation, and operation of resilient automation functions on (semi-) autonomous, low-emission inland vessels. The focus is on the DST ecosystem:

- **NOVA (“Smart & Green Ship”)** as an electrically driven demonstrator for autonomous functions and green propulsion.
- **ELLA** as a 1:6-scale development platform for manoeuvre automation under real conditions.
- **VeLABi** as a simulation and control centre including HIL/SiL coupling.
- **VERA** as a high-fidelity, ROS2-capable simulation and digital twin environment (UE5) with virtual sensors (camera, LiDAR, radar) and scenario manager.

Technical focus: Resilience across the perception–understanding–decision–action (PUDA) chain, including communication (multi-link), cybersecurity, and verifiable/explainable AI.

Subject of Investigation (WDS of interest)

- Navigation and manoeuvre automation (path planning/following, lock/bridge operations, docking/undocking, collision avoidance).
- Condition monitoring/diagnostics (sensors/propulsion/energy) and data-driven anomaly detection.
- Communication and remote-control paths (4G/5G/satellite/radio), QoS management, and fallback strategies.
- Cybersecure, fault-tolerant IT/OT architecture (PLC/ROS2, DLT-based identities, SBOM/vulnerability analysis).
- Digital twins for design, testing (SiL/HIL), continuous assurance, and knowledge exchange (Dataspace).

Specific Objectives

- **O1:** Complete evidence-based requirements and continuous tests for the WARRANT methodology (hazard/risk models, HAZOP/STPA, usability improvements) on “green & smart ships.”

- **02:** Design, implement, and test an intelligent resilience supervisor with modular sensors/actuators, virtual sensors/actuators, and adaptive, predictive control.
- **03:** Ensure WDS dependencies via a WDS meta-model and knowledge graph; digital twin + dataspace for continuous assurance (including federated learning).
- **04:** Cybersecure operations (identity/trust management, AML robustness, SBOM-based vulnerability analysis) and QoS-guaranteed connectivity (failover, degradation modes).
- **05:** Sim-to-real validation with VERA/VeLABi/ELLA/NOVA and HIL tests.

Measurable KPIs

Table 11: KPI categories and definitions for LL2.

Category	ID	Metric	Target
Path following/ Manoeuvring	1.1	Cross track error for path following	< ± 2 m in steady state (NOVA, ELLA field tests: after transient < ± 4 m)
	1.2	Success rate for docking/undocking and turning	> 85% under defined environmental conditions
	1.3	Maximum rudder angle and actuation frequency as efficiency indicator	(reduction of small high-frequency oscillations vs. baseline) < 50 Hz
Resilience/ Diagnostics	2.1	Mean Time To Detect (MTTD) anomalies	$\geq 50\%$ reduction vs. baseline; false-alarm rate < 5%
	2.2	Mean Time To Recovery (MTTR) after component/link failure	$\geq 50\%$ reduction through supervisor + redundancy/fallback
	2.3	Fail-operational capability: maintain defined core functions under partial failure	< 5 minutes
Communication	3.1	Uptime of communication paths	> 95%; failover switching time < 1 s
	3.2	End-to-end latency for safety-critical channels	< 1 s
Cybersecurity	4.1	SBOM coverage of safety-critical chain	100%
	4.2	MTTD for safety-relevant security events	< 30 min
	4.3	Successful AML evasion tests in approved configurations	0
Energy/ Performance	5.1	Additional energy consumption due to resilience functions	< 5% of mission energy (nominal)

5.2 Living Lab Challenges

LL3 focuses on **autonomous inland waterway vessels and their port operations**, applying the WARRANT methodology to test **resilience controllers, modular sensing strategies, and redundancy mechanisms**. Unlike ocean-going vessels, inland ships operate under **different regulatory frameworks, space constrained manoeuvring environments, and high levels of vessel-port interaction**, which pose distinct dependability and resilience challenges. DST leverages its **SmartShipping Research Program**, test vessels, and the HaFoLa inland port test centre to perform Hardware-in-the-Loop (HIL) experiments linked to extensive WDS model and sensor libraries.

Current challenges in inland waterway automation include:

- **Complex regulatory landscape:** Automation regulations for inland navigation differ from IMO-led ocean regimes. Inland vessels must comply with national riverine authorities, cross-border inland waterway standards, and port-specific operational rules, making assurance cases more fragmented and dynamic.
- **High dependency on port interaction:** Unlike deep-sea ships, inland vessels frequently engage in close-quarters manoeuvring, docking, and cargo transfer operations. Failures in resilience in these operational contexts have immediate safety and economic impacts on ports and local communities.
- **Restricted environments:** Narrow channels, low bridges, locks, and busy mixed-traffic waterways amplify risks of degraded automation, requiring resilient fallback strategies tailored to inland conditions.
- **Sensor and communication constraints:** GNSS reception, connectivity, and redundancy options differ in inland contexts, with heavy reliance on hybrid communication (5G, optical, VHF). Failures can disrupt not just vessel autonomy but coordinated port operations.

LL3 contributions to overcoming these challenges:

- **Deployment of resilience controllers:** Implement and validate Intelligent Dependability Supervisors (IDS) tailored to inland traffic and port-operation contexts, ensuring vessels remain compliant with riverine COLREG equivalents and port-entry protocols even under degraded states.
- **Modular sensing and redundancy integration:** Combine physical and virtual sensors (radar, GNSS, cameras, LIDAR, AIS, INS) to maintain reliable perception in constrained environments. Redundancy strategies (e.g., fallback propulsion, multiple comms channels) are evaluated specifically for inland navigation and port approaches.
- **Exploitation of DST's inland-focused WDS libraries:** Inland-specific models of vessel manoeuvring, port interfaces, and cargo handling are linked to WARRANT's Digital Twin and Knowledge Graph infrastructure, enabling scenario testing across both transit and port interaction phases.
- **HIL testing in port-linked environments:** Use DST's inland testbeds and port simulators to replicate real-world hazards such as lock failures, port traffic congestion, or cyberattacks on Vessel Traffic Services (VTS) and ship-port communication systems. This provides empirical validation of resilience measures under regulatory and operational conditions unique to inland waterways.
- **Regulatory alignment:** Translate resilience and dependability methods into assurance cases adapted for inland navigation rules and European regulatory frameworks (e.g., CESNI standards), complementing IMO-focused approaches.
- **Training & procedures:** Operator and port-staff training integrated into resilience procedures, ensuring effective collaboration during degraded automation and port-entry scenarios, captured within procedural assurance cases for CESNI compliance.

Through LL3, DST will deliver a **Blueprint for Resilient Autonomous Inland Vessel Operations**, demonstrating how modular sensing, redundancy, and adaptive supervision can make **inland waterway automation safe, regulatory-compliant, and port-ready**. This positions inland shipping as a frontrunner for dependable automation in Europe's zero-emission, smart mobility corridors.

5.3 Use cases

5.3.1 Evidence-Based Requirements and Continuous Testing Support

Goal: Specify reference WDS model for “green & smart ships” (automation, control, energy), reference assurance levels, and data fusion; DST ecosystem provides data/test runs.

Activities:

- Derive/validate hazard catalogues (HAZOP/STPA) and risk models for typical inland use cases (narrow passages, bridges/locks, harbour manoeuvres, mixed traffic).
- Apply WARRANT tools: T1.1 (WDS model framework), T2.2 (HAZOP/STPA assistance, risk scenario generator), T2.1 (AML-based data/model integrity), T2.1/T1.4 (security/assurance).
- Digital/HIL tests with VERA/VeLABi/ELLA/NOVA, including defined disturbances (sensor dropouts, GNSS degradation, communication failure).

Results:

- Parameterized, reusable methodology building blocks for LL3; KPI baseline; lessons learned for usability improvements (e.g., semi-automated unsafe-control-action detection, scenario-based risks).

5.3.2 Resilience Control for ‘Smart & Green Ships’

Goal: Design and integrative testing of the supervisor with distributed, adaptive/predictive control; active diagnostics (active interventions for fault discrimination); virtual, physical sensors/actuators.

Activities:

- Design distributed/decentralized controllers (trajectory/heading/DP), mode switching with minimum dwell times; Nomoto-based SMC/LOS combinations; extend with prediction (MPC) for manoeuvres in narrow passages.
- Implement virtual sensors (e.g., GNSS replacement via radar/LiDAR/IMU fusion) and virtual actuators (mask actuator faults) on ROS2 architecture.

- QoS-guaranteed communication failover (cellular/satellite/VHF) and edge computing; define degradation modes (fail-soft/-safe/-operational).
- Integrate supervisor-knowledge graph (WDS dependencies, cascade effects) and digital twin for re-planning and continuous assurance.

Results:

- Demonstrated fail-operational capability in defined disturbance scenarios; reduced MTDD/MTTR; stable manoeuvre support under currents/wind/traffic.

5.4 Living Lab Structure

5.4.1 Available Resources

NOVA – Smart & Green Ship (DST)

- Platform: Dedicated test vessel (catamaran) for autonomy, zero-emission propulsion, and assistance systems.
- Key data: Length ~14.97 m; Width ~7.10 m; Draft ~0.70 m; Propulsion: 2 electric motors (50 kW each); Battery capacity ~320 kWh; v_{max} ~25 km/h.
- Equipment: ECDIS with radar overlay; X-band radar; GPS compass; AIS; VIS/IR cameras (8+), stereo cameras; 4× LiDAR; 4× short-range radar (W-band); ultrasound; IMU; operational data logging; VHF; professional navigation equipment.
- Research: Path planning/control, collision avoidance, bridge/lock protection, context functions; resilience/communication; data collection (annotated image datasets, coverage gaps, operational data).

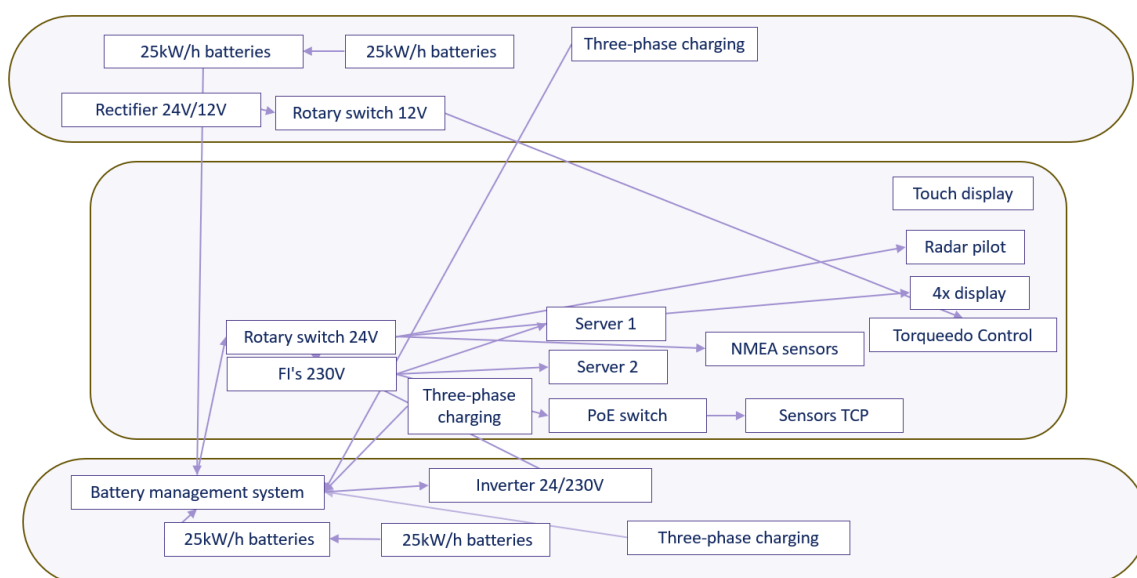


Figure 4: Structure of NOVA.

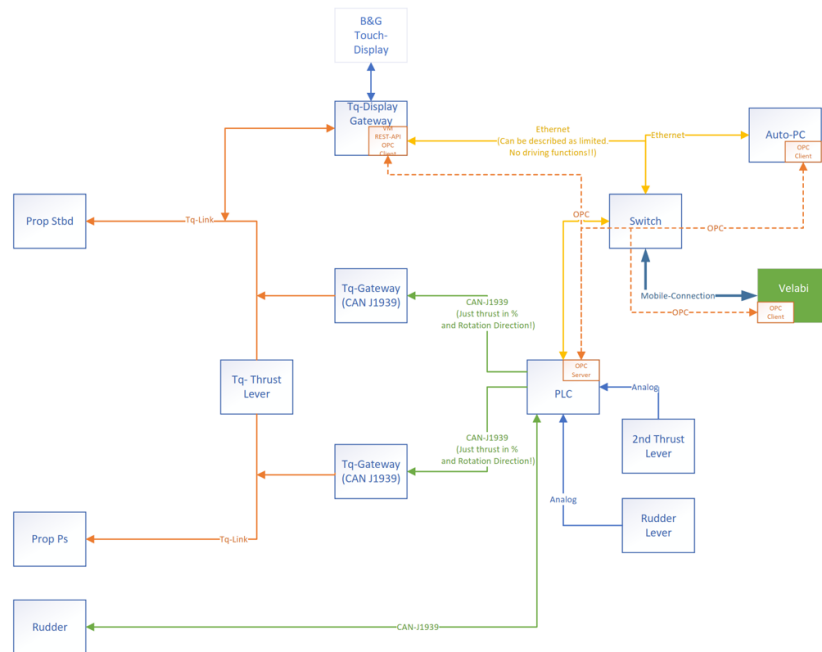


Figure 5: Signal Level of NOVA.

Table 12: Sensors of NOVA.

Sensor	Manufacturer	Data type (ROS2)	Frequency
GPS+IMU	MicroStrain 3DM-GQ7	sensor_msgs/msg/NavSatFix sensor_msgs/msg/Imu microstrain_inertial_msgs/msg/HumanReadableStatus * geometry_msgs/msg/TwistWithCovarianceStamped nav_msgs/msg/Odometry sensor_msgs/msg/Imu	100 Hz
Lidar	Sick MRS6000	sensor_msgs/Pointcloud2	2 Hz
Radar	JRC JMR-611	radar_msgs/RadarScan * ASTERIX CAT240	
AIS	em-trak A200	nmea_msgs/Sentence *	
Camera	Basler ace2	sensor_msgs/msg/CompressedImage	
Weather	Airmar WX120	Still needs to be defined	

ELLA – Scaled Test Platform 1:6 (DST)

- Key data: L 14.88 m; B 1.96 m; T 0.46 m; two main drives; four rudders; 4-channel bow thruster; modular sections.
- Sensors: Multi-LiDAR, radar, stereo camera, monocular camera, thermal imaging, 12× ultrasound, GNSS RTK (e.g., Trimble BX992), IMU; weather station.
- Control/Software: PLC for actuators (real-time/fault-tolerant), automation computer via ROS2; A* path planning (hybrid), LOS guidance with dynamic preview; SMC controller (Nomoto-based); fallback to manual control.

- Validated manoeuvres: Straight driving, turns/U-turns, docking/undocking with documented cross-track/rudder profiles.

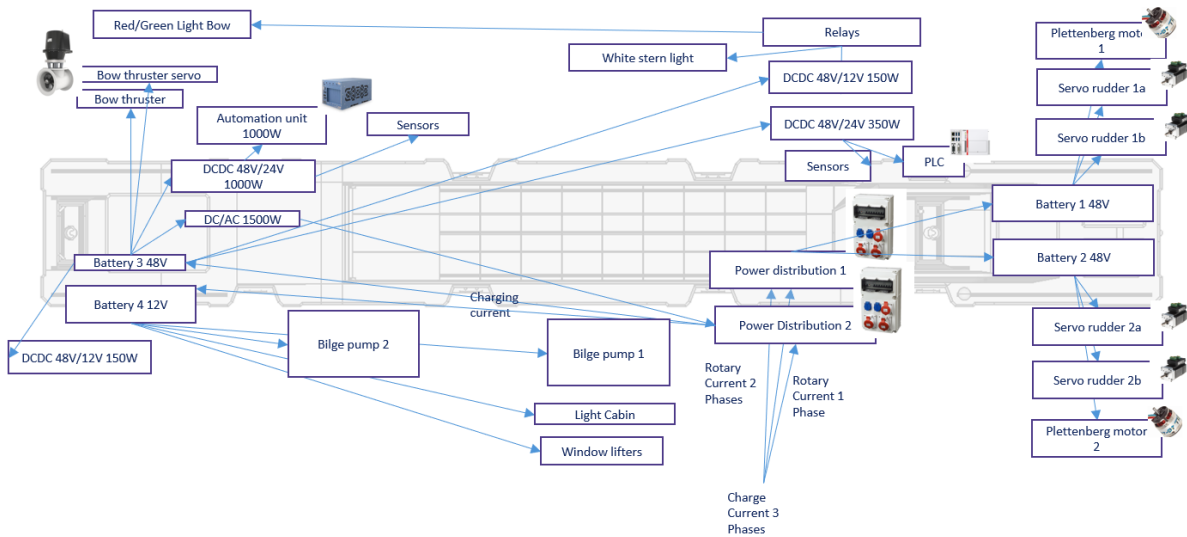


Figure 6: Structure of ELLA.

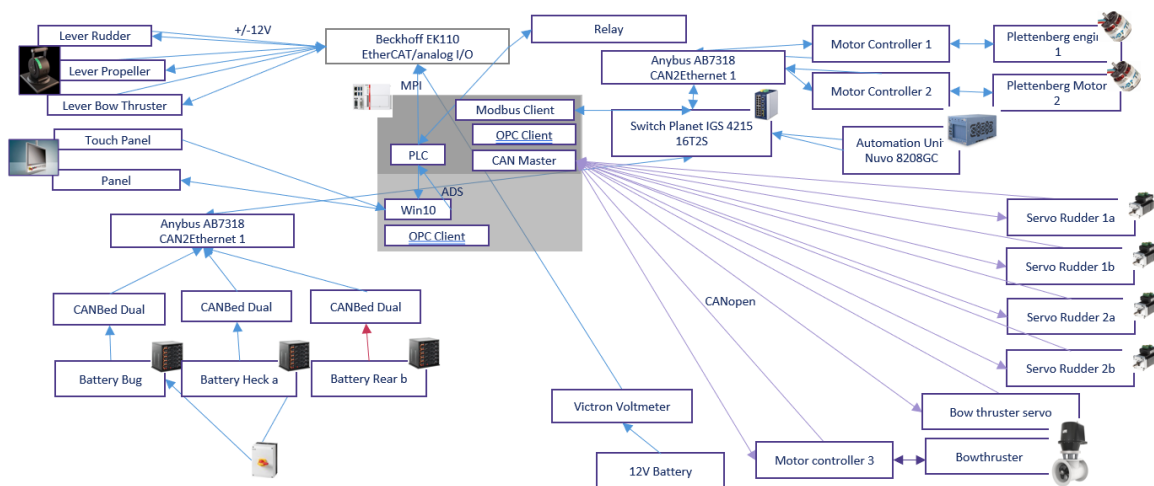


Figure 7: Signal Level of ELLA.

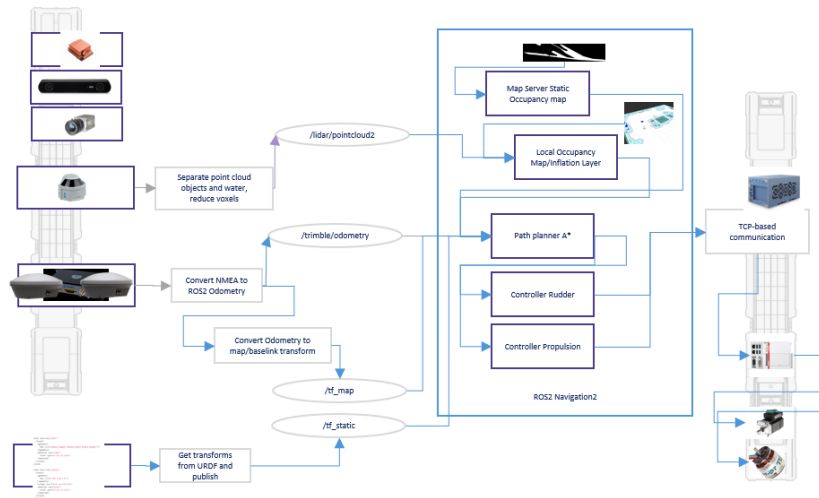


Figure 8: Software Level of ELLA.

Table 13: Sensors of ELLA.

Sensor	Manufacturer	Data type (ROS2)	Frequency
Lidar	Sick	sensor_msgs/Pointcloud2	2 Hz
Radar	Navtech CIR	radar_msgs/RadarScan *	4 Hz
AIS	ICOM MA510-TR	nmea_msgs/Sentence *	
GNSS	Trimble	sensor_msgs/msg/NavSatFix	
Weather	Airmar WX120	Still needs to be defined	

Table 14: Sensor data of ELLA.

Type	Manufacturer	Model	No.	Interface	Field of view	Resolution
Lidar	SICK	MRS6000	3	Ethernet	120° × 15°	0.13° × 0.625°
Lidar	Field of view	Cube1	1	Ethernet	70° × 30°	0.4° × 5°
Mono camera	Basler	Ace2	3	Ethernet	45° × 29°	3.2 MP
Radar	NavTech	CIR	1	Ethernet	360	0.044 m
Stereo camera	StereoLabs	Zed2i	2	USB	120° × 70°	2.74 MP
Thermal imaging camera	FLIR	M300C	1	Ethernet	24° × 24°	Night: 0.33 MP / Day: 2.07 MP
Ultrasound	Pepperl-Fuchs	UC2000-L2	12	CAN	15° × 15°	0.4 mm
IMU	XSense	MTi-30	1	USB	-	-
GNSS	Trimble	BX992	1	Ethernet	-	-
Weather station	Airmar	WX120	1	NMEA2000	-	-

VeLABi – Simulator and Control Center (DST)

- High-performance simulation and control infrastructure for inland navigation automation functions; remote operations, HIL coupling, training/test scenarios.

VERA – Digital Twin/Simulation (DST)

- UE5-based photorealistic environments (>100 km of waterways); 3D terrain from DTM/OSM, photogrammetry; dynamic weather/current.
- Virtual sensors (camera/LiDAR/radar) via GPU ray tracing; error/noise models; streaming (RTSP/FFmpeg); ROS2/FastDDS communication; scenario manager (determinism, playback DB).
- HIL/SiL support; distributed setups via VPN.

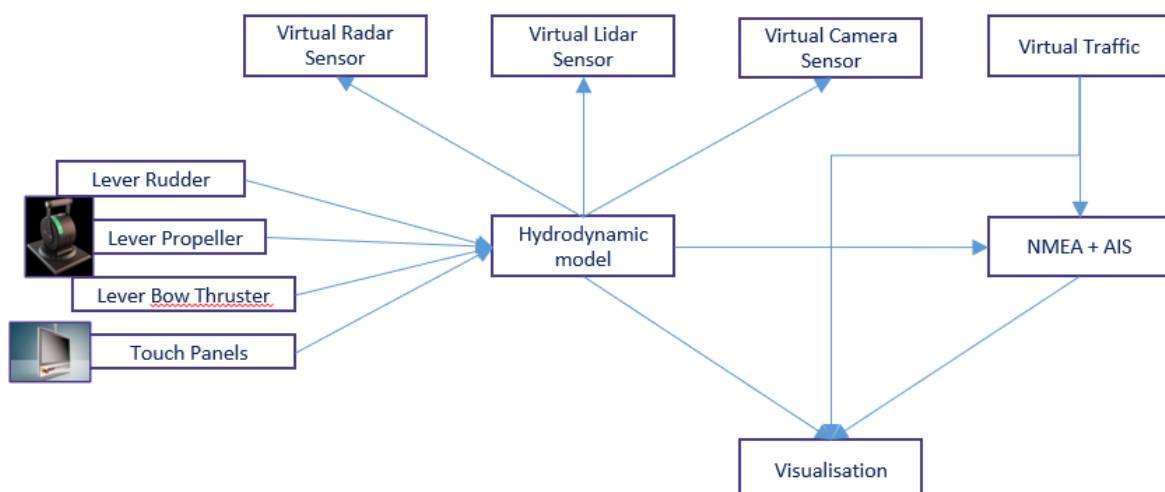


Figure 9: Structure of VERA.

Table 15: Sensor data of VERA.

Sensor	Data type (ROS2)	Frequency
GPS	vera/custom_messages/Position *	100 Hz
Lidar	vera/sensors/LidarPackage *	
Radar	vera/sensors/RadarPackage2 * ASTERIX CAT-240	
AIS	nmea_msgs/Sentence *	
Camera	RTSP stream	
Weather	vera/custom_messages/WeatherMessage *	

Communication/IT Resources (DST)

- Multi-WAN/Peplink routers; 4G/5G SIMs (unlimited, test duration); NAS storage; outdoor laptops; workstations for sensor fusion/ML; software licenses (e.g., Unreal).

5.4.2 Activities and roles

DST, as the lead partner for LL3, is responsible for the overall coordination of activities, including the execution of experiments on the NOVA and ELLA platforms. Its tasks comprise the development and implementation of the safety concept, data collection and annotation, Hardware-in-the-Loop (HIL) campaigns, and sim-to-real comparisons. DST will also monitor Key Performance Indicators (KPIs) and conduct virtual testing in VeLABi using the digital twin VERA.

SINTEF Ocean contributes by developing the methodology for the WDS/SRODS framework, focusing on usability studies based on System-Theoretic Process Analysis (STPA). The team supports usability improvements, including semi-automated Unsafe Control Action (UCA) derivation and the development of the scenario generator.

DNV leads the assurance and approval aspects in LL3, covering threat models, safety and security assurance cases, and design assurance levels. It co-leads the development of the HAZOP/STPA framework for AI-enabled IT/OT systems, providing guidance and checklists, and ensuring consistency with IACS UR E26/E27. Furthermore, DNV contributes to KPI definition, the structuring of evidence chains (claims–evidence–arguments), and performs pre-audits of LL3 results to support verification and validation processes.

NTUA implements the extended HAZOP developed in WP1, using the WDS model defined in Use Case 1 to build hazard libraries and “what-if” scenarios for typical inland waterway manoeuvres, including bridges, locks, and narrow passages. The team also integrates the usability improvements developed in WP2 into the extended HAZOP framework and benchmarks these against the baseline implementation to assess their effectiveness.

TU Delft develops the methodology and design of the Intelligent Dependability Supervisor, which encompasses distributed adaptive and predictive control, virtual sensors and actuators, and active diagnosis capabilities. It further establishes coupling between the Supervisor, the Knowledge Graph, and the Digital Twin to enable planning and re-planning under uncertainty. TU Delft also co-designs mechanisms for Quality of Service (QoS) management and degradation modes in communication and control systems.

KONNECTA focuses on implementing the WARRANT Knowledge Platform and its associated tools, including the WDS metamodel, Knowledge Graph, and WDS Cognitive Registry. The partner develops dataspace connectors (ROS2/FastDDS, IoT/API/Cloud) and DLT-based identity and trust management mechanisms. In addition, KONNECTA integrates federated learning techniques for anomaly detection and integrity verification into the LL3 data flows, enhancing data reliability and security.

INLECOM is responsible for LL3 data space coordination, management, and continuous assurance across both control and data planes, using DCAT/ORDL cataloguing. The partner performs sim-to-real comparisons, metric aggregation, and ensures reproducibility of LL3 campaigns through a dedicated playback database. Finally, INLECOM contributes to the planning of diffusion and scale-up activities and serves as the interface to WP4, ensuring the seamless integration of LL3 results into the wider project framework.

5.4.3 Timeline of planned activities

Process/Flow (textual representation)

- **Phase A:** Requirements elicitation and hazard analysis (DST, NTUA, DNV, SINTEF OCEAN) → Reference WDS model LL3, KPI baseline.
- **Phase B:** Tooling & platform (KONNECTA, INLECOM) → KG/Dataspace/Identity; VERA/VeLABi coupling.
- **Phase C:** Supervisor design & simulation (TU DELFT, SINTEF OCEAN, DST) → SiL in VERA; test cases/failure scenarios; preliminary KPI assessment.
- **Phase D:** HIL tests with ELLA (DST lead) → Validation of path following/manoeuvres under disturbances; communication fail-over; cyber tests.
- **Phase E:** NOVA on-water campaigns (DST lead) → Resilience proofs, data collection; assurance review (DNV).
- **Phase F:** Consolidation, training, blueprints (all) → Documentation, dissemination, adoption paths.

Timeline (Project start 01.04.2025 = M1; expected end 31.03.2028 = M36)

- **M1–M9:** Setup LL3, safety and approval planning, KPI detailing, data management/DPIA (DST, INLECOM, DNV).
- **M3–M9:** hazard/risk baseline, reference WDS model, VERA scenario setup (SINTEF OCEAN, NTUA, DST); first STPA/HAZOP runs; dataspace cataloguing (INLECOM).
- **M6–M12:** Platform bring-up (KONNECTA/INLECOM): KG, Identity/DLT; first SiL runs of the Supervisor - test of virtual sensor (TU DELFT/SINTEF OCEAN) in VERA.
- **M10–M18:** HIL campaigns with ELLA (DST): trajectory following, berthing/unberthing, bridges/locks; communication fail-over; security scenarios; interim KPI review (DNV).
- **M16–M26:** NOVA on-water campaigns (DST): resilience supervisor in real missions; data collection for federated learning; assurance cases (DNV).
- **M24–M30:** Consolidation methodology/tools; blueprint “Resilient Automation for Green Inland Vessels”; training/material (WP4.3).
- **M30–M36:** Finalisation, standardisation input, exploitation/adoption paths (VLTN/INLECOM/SINTEF OCEAN), lessons learned and sustainability plan LL3.

Interaction with WPs

- **WP1 (Methodology, M1–M30):** LL3 delivers requirements/data; validates HAZOP/STPA and Supervisor concept; feedback loops in M9/M18/M26.
- **WP2 (Knowledge Platform, M1–M33):** LL3 uses KG/Dataspace/Security tools; provides operational data/models; tests federated learning modules.

- **WP3 (LLs, M1–M26):** Coordination of campaigns; joint milestones MS4 (M14) and MS6 (M24).
- **WP4 (Dissemination/Scale-up, M1–M35):** Demos/data stories from LL3; training (cybersecurity/assurance); contributions to standardisation (ISO/IEC/IMO/IACS).
- **WP5 (PM, M1–M36):** QA/risk management; DMP/GDPR/ethics; milestone reviews M18, M30.

5.5 Stakeholder Engagement

Stakeholder categories

- Authorities/regulators: Waterways and Shipping Administration, CCNR, EMSA; local approval bodies.
- Classification societies/insurers: DNV (in consortium), other classes, insurers/risk assessors.
- Port operators/infrastructure: Port of Antwerp-Bruges (in consortium), Duisport, lock/bridge operators.
- Operators/fleets: shipping companies, shipmasters/associations, remote operation centres (SEAFAR).
- Industry/technology: sensor/radar/LiDAR manufacturers, communication providers, PLC/automation OEMs, cybersecurity vendors.
- Research/academia: universities/research institutes; standardisation bodies (ISO TC8/IEC TC80/IACS).
- Public/environment: local communities, environmental NGOs.

Engagement methods and frequency

- Quarterly workshops (hybrid) with live demos/simulator sessions (VeLABi/VERA), focus on requirements, risks, KPIs.
- Semi-annual on-water demonstrations (ELLA/NOVA) with structured feedback collection (surveys/interviews).
- Co-creation sprints (2–3 per year) on HMI/workflows, emergency procedures, and degradation modes (with shipmasters/ROC operators).
- Regular communication: quarterly newsletters, issue briefs (assurance/standardisation), open artefacts (e.g. scenarios/KPIs) where possible.
- Feedback integration: change management with traceability (issue tracker), review cycles at M9, M18, M26.

5.6 Implementation Risks

Table 16: Identified risks related to the implementation of LL3 and mitigation measures.

#	Risk Category	Risk Description	Mitigation Measure(s)
R1.1	Technical risks	Insufficient sim-to-real transferability	modelled sensor errors/atmosphere, deterministic replays, parameter tuning, HIL before field test
R1.2		Communication outages/interference	multi-link design (4G/5G/sat/VHF), L3/L7 fail-over < 1s, store-and-forward, bandwidth adaptation; dead-zone mapping (NOVA)
R1.3		Sensor/actuator failures	virtual sensors/actuators, plausibility checks, redundant paths; FDIR strategies (fault detection, isolation, recovery)
R1.4		AI/ML misbehaviour	data integrity checks, explainability/uncertainty estimation, domain validation; AML robustness tests; fallback to classical rule-based functions
R2.1	Safety/operations risks	Navigation hazards (current/wind/traffic, narrow passages)	staged release (sandbox → pilot → free navigation), geofencing, chase boat/observers, E-stop/takeover
R2.2		Low/High water/environmental variability	adaptive mission planning, reserve profiles, test window planning; emergency plans and abort criteria
R2.3		Human factors	HMI usability tests, SOPs, crew training; workload measurement; clear human-automation handover protocols
R3.1	Cybersecurity/privacy	Exploits/poisoning/evasion	SBOM maintenance, patch management, pen-tests/red-team drills, AML tooling (TECNALIA), zero-trust principles, DLT-based identity
R3.2		Data/privacy/GDPR	DPIA, pseudonymisation/anonymisation, access control/RBAC, EU hosting, defined retention; release only of aggregated data
R4.1	Approvals/stakeholder acceptance	Delayed approvals/test windows	early involvement of authorities/ports, phased test scenarios, alternative test areas
R4.2		Acceptance risks	transparent communication, ride-alongs/simulator experiences, evidence through KPIs and assurance cases
R5.1	Delivery/resource risks	Hardware supply chains/staff shortages	safety stock of critical components (Peplink/sensors), cross-skilling in team, modular test plans with simulator substitution
R6.1	Quality/data risks	Data gaps/inconsistencies	DMP processes (WP5), validation rules, mandatory metadata, data quality KPIs; use of synthetic data with labelling

Cross-cutting mitigation

- Safety Management Plan (SMP) and Test Hazard Log; pre-test HAZID/toolbox talks; lessons-learned cycles per campaign.
- Milestone gates (M14/M24/M30) with go/no-go criteria; independent reviews (DNV).

6 LL4 “Enhanced Dependability of Remote Operation Systems”

6.1 Scope and Specific Objectives

LL4 goal is to enhance the dependability of Seafar Remote Operation Systems (ROS), specifically targeting applications in remote ship operations on the Rhine and in the Port of Antwerp, through the implementation of the WARRANT Methodology and Knowledge Platform.

The main goal is structured around four specific objective areas:

- **Connectivity (C):** Establish fast and reliable connections through optimized multiple communication channels, with robust encryption and error correction to ensure data integrity and protection against cyberattacks.
- **Situational Awareness (SA):** Implement systems for detecting and analysing environmental and operational conditions, using machine learning for identifying vulnerabilities.
- **Vehicle Control System (VCS):** Ensure robust hardware interfaces, redundancy, and fail-safe strategies to maintain control during failures, with thorough verification of AI algorithms.
- **Human Factors (HF) & HMI:** Enhance usability and resilience, ensuring effective manual control and fail-safe mechanisms in unexpected conditions.

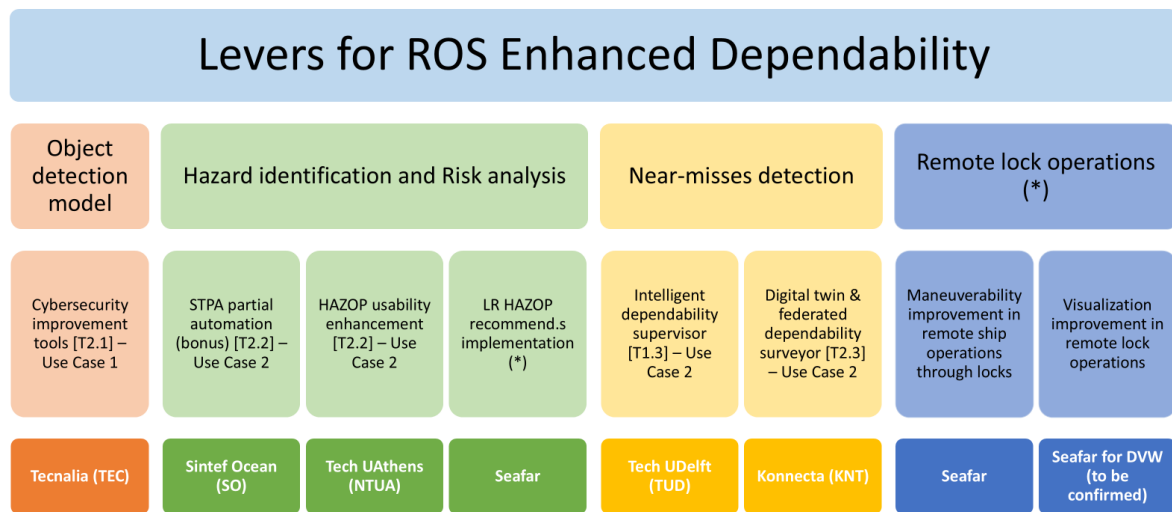
To translate these objectives into concrete actions, LL4 focuses on four main study objects through which dependability improvements will be pursued:

- **Object Detection Model (ODM):** Refinement of SEAFAR AI-based object detection system, designed to recognize and classify elements such as vessels or obstacles, with the goal of significantly improving precision and accuracy to enhance situational awareness.
- **Hazard Identification and Risk Analysis (HIRA):** Application of systematic methodologies (e.g., HAZOP, STPA) to proactively assess risks associated with remote manoeuvres and define appropriate mitigation strategies.
- **Near-Miss Detection (NMD):** Development of automated systems to detect “near-miss” events, critical situations that do not cause damage but provide valuable learning opportunities for continuous safety improvement.
- **Remote Lock Operations (RLO):** Addressing the complex manoeuvres required for passing through locks. Given the high precision demanded, this represents an ideal testbed for integrated dependability across the system. Moreover, discussions are ongoing with the Flemish Waterway Authority (De Vlaamse Waterweg) regarding the potential application of Seafar’s object detection system and sensor fusion algorithms to their remote station for a lock in Flemish territory.

Table 17 shows the mapping between these study objects and their target dependability aspects. A visualization is also available in Figure.

Table 17: LL4 Dependability Aspects.

Levers for ROS Enhanced Dependability	Target Dependability Aspect
Object Detection Model (ODM)	Cybersecurity
Hazard Identification and Risk Analysis (HIRA)	Safety
Near Misses Detection (NMD)	Cybersecurity and Safety
Remote Lock Operations (RLO)	Safety



(*) Activities performed only by Seafar (no use cases)

Figure 10: LL4 Dependability Levers.

A system of KPIs has been defined to **measure progress towards these objectives**. As shown in Table 18, each KPI is linked to one or more objectives and dependability levers. Some KPIs already have quantified target values, while others will be refined during the initial phases of the Living Lab to establish measurable thresholds for achievement by the end of the project.

Table 18: LL4 KPIs.

KPI	Target Value	Objective Area	Dependability Lever
K1.1	Connection failure duration ≤ 400 ms	C	HIRA, NMD
K2.1	Detection accuracy $> 80\%$	SA	ODM
K2.2	AI-system response time ≤ 100 ms	SA	ODM
K2.3	Operator workload reduction	HF & HMI	HIRA, NMD
K2.4	AI-system interruptions ≤ 300 ms	SA	ODM
K2.5	Increased user satisfaction	HF & HMI, SA	HIRA
K3.1	Reduced response time to operational issues	SA, C, VCS	RLO
K3.2	Increased customer satisfaction	HF & HMI	RLO
K3.3	Clearer and more timely communication	C, HF & HMI	RLO

The relationship between KPIs and dependability levers is not always direct but reflects the **complex interdependencies** of the system. For example, indicator K1.1 is associated with connectivity but is also crucial for HIRA, as risk analysis must assume a maximum disconnection threshold for safety assessment. It is equally relevant for NMD, since a near-miss detection system would be ineffective if unable to transmit real-time alerts. Similarly, K2.3 falls under HF & HMI but also reflects HIRA and NMD: robust risk analysis contributes to intuitive interfaces, while

automated near-miss detection reduces the need for constant vigilance, thereby lowering the operator's cognitive workload.

6.2 Living Lab Challenges

LL4 focuses on enhancing the dependability of **Remote Operation Systems (ROS)** used for inland and near-port operations, particularly in the Rhine and Antwerp regions. With SEAFAR already operating remote-controlled barges, this Living Lab applies the WARRANT methodology to ensure that **remote operations are safe, cybersecure, and resilient under real-world conditions**. The emphasis is on validating **AI applications, connectivity assurance, and human-machine collaboration**, supported by a **Remote Operations Digital Twin** that integrates regulatory compliance and resilience testing.

Current challenges in remote operations include:

- **Connectivity fragility:** ROS depend heavily on multiple communication channels (satellite, 5G, VHF, optical). Disruptions or degraded quality can cause loss of control or delays in hazard response, with potentially severe safety implications.
- **AI assurance gaps:** Machine learning (ML) components are increasingly used for anomaly detection, situational awareness, and decision support. Yet most ML models lack structured assurance processes, leaving operators and regulators uncertain about their reliability in critical scenarios.
- **Human-automation interface risks:** Remote operators must be able to seamlessly hand over, override, or complement AI-driven decision-making. Failures in this collaboration can lead to delayed or unsafe responses, especially in congested waterways or port areas.
- **Regulatory uncertainty:** Remote operation falls under evolving standards that combine inland navigation law, flag state requirements, and class society certification. Current assurance cases often lag behind operational innovation, creating a compliance gap.

LL4 contributions to overcoming these challenges:

- **Digital Twin-enabled ROS assurance:** Calibrate a Digital Twin of SEAFAR's ROC environment, modelling vessel states, communication links, and port interactions. This provides a controlled testbed for dependability and resilience analysis, feeding back into hazard libraries and assurance cases.
- **Connectivity resilience:** Validate multi-channel comms strategies, including redundancy and automatic switching, to ensure that data transmission success rates and system availability remain within regulatory and safety thresholds.
- **AI assurance and adversarial testing:** Catalogue current and future AI applications within ROS (decision support, anomaly detection, predictive maintenance) and test them using **adversarial ML techniques**. This reveals vulnerabilities to manipulated or corrupted data inputs and establishes verification protocols.
- **Resilience controllers for remote operations:** Deploy Intelligent Dependability Supervisors (IDS) to manage hazards dynamically, automatically reconfiguring system

behaviour in degraded states and ensuring that vessels maintain COLREG-compliant manoeuvrability under remote control.

- **Secure identity management:** Test blockchain/DLT-based identity and access management to ensure only verified vessels, devices, and operators interact with the ROC system, enhancing cybersecurity assurance.
- **Training & procedures:** training for remote operators on safe human–AI handovers and override procedures, with updated ROC SOPs codified and integrated into national assurance frameworks.
- **Compliance integration:** Translate the outcomes of LL4 testing into assurance cases aligned with evolving inland and ROS-specific standards, supporting both national authorities and class society certification processes.

Expected outcomes:

- **Blueprint for Dependable Remote Operation Systems**, providing validated resilience measures, assurance processes, and regulatory compliance pathways.
- Demonstrated improvements in **system availability, redundancy effectiveness, and time-to-detect/mitigate threats**, measured via KPIs.
- Evidence-based guidance for scaling remote operations safely across inland and coastal fleets, with direct input into regulatory frameworks and industry best practices.

LL4 thus ensures that remote ship operation systems evolve beyond experimental pilots into a **dependable, regulation-ready mode of operation**, enabling Europe to safely expand the role of ROS in smart, sustainable, and autonomous shipping corridors.

6.3 Use cases

LL4 addresses two use cases, covering three dependability levers (ODM, HIRA and NMD):

Verification and dependability management of AI applications in ROS

- **ODM:** TECNALIA will analyse Seafar’s object detection model from a cybersecurity perspective. The partner will conduct in-depth threat research, implement representative attack techniques, and provide tailored recommendations for improving the cybersecurity of Seafar’s object detection system. *Linked with T2.1.*

ROS digital twin-enabled dependability management and intelligent supervision for hazard mitigation

- **HIRA:** NTUA will apply the HAZOP methodology with usability improvements to a process/system within Seafar’s ROS and ensure that safety officers can perform the analysis with comprehensive knowledge support. In parallel, SINTEF OCEAN will apply the STPA methodology to the same process/system (to be defined) to evaluate which AI tools can automate its third and fourth steps. *Linked with T2.2.*

- **NMD:** TU DELFT will develop an intelligent dependability supervisor, a digital representation of sensors and actuators designed to maintain operations even when the physical components experience failures. KONNECTA will implement a digital twin for simulation and scenario planning and further develop a federated dependability surveyor. Seafar expects these tools to support the detection of near misses. *Linked with T1.3 and 2.3.*

6.4 Living Lab Structure

Based on the previously defined objectives, dependability levers, and KPIs, the planning phase consists of defining a **structured yet flexible work plan**. This plan is organized across multiple levels: a high-level Work Breakdown Structure (WBS) and a RASCI matrix have been developed to provide an overview of the entire LL4 lifecycle, defining **major activities and responsibilities**. In parallel, a risk analysis has been conducted to identify and mitigate potential issues that could arise during execution. From these high-level elements, a **detailed schedule for the first operational cycle** (October 2025 – March 2026) has been derived.

6.4.1 Available Resources

Seafar's primary role is to provide partners with access to **operational data** (including, but not limited to, latitude, longitude, heading, engine power, speed and AIS), which can be extracted from **any vessel equipped with Seafar's system**. The only restriction is that these vessels must operate within the Port of Antwerp-Bruges and the Rhine river areas.

In addition, Seafar's team (including the QSHE Manager, Technical Project Analyst, Regulatory Affairs Specialist, Product Manager, R&D Manager, and AI Developer) is available for discussions and **knowledge exchange** with the partners.

6.4.2 Activities and roles

The high-level Work Breakdown Structure (WBS) for activity T3.5 (LL4) organizes tasks into functional packages reflecting Seafar's central coordinating role. The subsequent sections describe each package in detail. Table 19 presents the WBS.

T3.5.A Lock ROS: The experimental core of LL4 revolves around lock operations, adopting a twofold approach. The first, already confirmed, focuses on the remote ship operator perspective, aiming to improve safety and manoeuvrability. The second, to be confirmed with the Flemish Waterway Authority (De Vlaamse Waterweg, DVW), will explore the remote lock operator perspective, leveraging the Object Detection Model (ODM). Visual information from the ODM will be integrated with sensor fusion techniques, combining camera data with other systems such as AIS and radar to provide more accurate and robust distance and trajectory estimates, overcoming individual sensor limitations.

T3.5.B HAZOP: Risk analysis activities are practical and action-oriented, building upon recommendations from a previous HAZOP analysis conducted with Lloyd's Register. On the vessel *Brunello*, specific systems will be implemented, co-financing their installation, including Bridge Navigational Watch Alarm System (BNWAS), a general E-stop for the ROC, an external microphone, and automated controls.

T3.5.C LL4 Management: Coordinating the project’s operational processes across two main use cases; contributing to the WDS alliance, organizing a workshop for the alliance, and preparing progress reports (deliverables D3.1 and D3.5).

T3.5.D Data & Validation: The success of the LL is tightly linked to this package, organized according to an agile logic. A first dataset will be shared to initiate partner development, followed by a phase where partners apply their tools to Seafar’s systems, and a second dataset sharing for final evaluation, with the possibility of additional refinement cycles.

T3.5.E KPI Definition: This package formalizes the performance measurement process. It starts with defining an initial baseline for each indicator and proceeds to **quantify targets with measurable thresholds**, ensuring that LL progress can be continuously tracked against the agreed objectives.

Table 19: LL4 High-Level Work Breakdown Structure.

Code	Activity
T3.5.A	Lock ROS
T3.5.A.1	Requirements extraction
T3.5.A.2	Use case definition
T3.5.A.3	Detailed implementation planning
T3.5.A.4	Implementation
T3.5.A.5	Testing and data collection
T3.5.A.6	Finalization and validation
T3.5.B	HAZOP
T3.5.B.1	BNWAS implementation
T3.5.B.2	ROC general E-stop implementation
T3.5.B.3	External microphone implementation
T3.5.B.4	Automated controls implementation
T3.5.B.5	Internet connection reliability review
T3.5.B.6	Knowledge sharing and experience
T3.5.C	LL4 Management
T3.5.C.1	Contribution to WDS alliance
T3.5.C.2	Use Case 1 management (ODM lever)
T3.5.C.3	Use Case 2 management
T3.5.C.3.1	HAZOP & STPA (HIRA lever)
T3.5.C.3.2	Intelligent supervisor & Digital Twin (NMD lever)
T3.5.C.4	Reporting D3.1
T3.5.C.5	Reporting D3.5
T3.5.C.6	LL4 Workshop organization
T3.5.D	Data & Validation
T3.5.D.1	Cycle 1: data sharing
T3.5.D.2	Cycle 1: feedback
T3.5.D.3	Cycle 2: data sharing
T3.5.D.4	Cycle 2: feedback
T3.5.D.5	Additional iterations (if necessary)

Code	Activity
T3.5.D.6	Final algorithm validation
T3.5.E	KPI Definition
T3.5.E.1	Initial baseline definition
T3.5.E.2	Quantification of measurable targets

The RASCI matrix is presented in Table 20. This tool not only assigns tasks but also clarifies the **collaboration and leadership dynamics** within LL4.

Table 20: LL4 Responsibilities.

Activity (WBS)	SEA	TEC	TUD	KNT	SO	NTUA	POAB	INLE	DVW
T3.5.A	A/R				I	I	C	I	C
T3.5.B	A/R				I	I	I	I	I
T3.5.C	A/R	S	S	S	S	S	C	S	
T3.5.C.1	R	S	S	S	A	S	C	S	
T3.5.C.2	A/R	S				I		I	
T3.5.C.3	A/R		S	S	S	S		I	
T3.5.C.4/5	A/R	C	C	C	C	C	C	C	
T3.5.C.6	A/R	C	C	C	S	S	S	C	C
T3.5.D	A/R	C	C	C	C	C		I	
T3.5.E	A/R					I		I	
Abbreviations:									
A/R = Accountable/Responsible, R = Responsible, C = Consulted, I = Informed, S = Support									

For packages **T3.5.A** and **T3.5.B**, Seafar is **fully Responsible**, as these are experimental and implementation activities conducted on its own resources (vessels and the ROC). PORT ANTWERP-BROUGE and DVW are appropriately included as **Consulted or Informed**, being the owners of the operational context in which the tests take place.

A more complex dynamic emerges in the management package **T3.5.C**. Seafar retains overall responsibility (Accountable), but operates in a **highly collaborative framework**, with most academic partners in a Support role. Notably, task T3.5.C.1 (Contribution to the WDS alliance) is an exception, with final responsibility assigned to SINTEF OCEAN. This choice is strategic, as the alliance falls under WP4 (Dissemination and Standardization), led by SINTEF OCEAN, while Seafar actively contributes. Use case management reflects the collaborative nature of the work: in the first use case (T3.5.C.2), Seafar leads while TECNALIA provides support through its cybersecurity recommendations for Seafar algorithms. In the second, more complex use case (T3.5.C.3), Seafar is Responsible for integration but relies on the specialized support of TU DELFT, KONNECTA, SINTEF OCEAN, and NTUA for the various technological and methodological components.

The agile logic of the LL is particularly evident in the penultimate work package. In **T3.5.D**, Seafar acts as the provider of operational data (Accountable/Responsible), while the academic partners are the “clients” who use it to develop and test their solutions. Accordingly, they are **continuously Consulted** to ensure the datasets provided are relevant and sufficient for their objectives.

Finally, in package **T3.5.E**, Seafar is **Responsible** for the laboratory’s performance measurement. In this context, the roles of NTUA and INLECOM as **Informed** are significant: as leaders of WP3

and CL, respectively, they need to be constantly updated on results to support supervision and overall project reporting.

6.4.3 Timeline of planned activities

The planning of Living Lab 4 has been structured into successive cycles:

- **Cycle 1 (April 2025 – September 2025):** Initiation and strategic planning phase. This period is dedicated to kick-off meetings, bilateral discussions with partners, and internal alignment at Seafar to define a shared plan and mitigate initial risks. The output of this cycle is deliverable D3.1, which formalizes the detailed LL4 plan.
- **Cycle 2 (October 2025 – March 2026):** First operational cycle of the LL. Activities focus on initial data collection, development of early prototypes, and preliminary analyses. The KPIs baseline will be established through the quantification of performance indicators.
- **Cycle 3 (April 2026 – September 2026):** Second development iteration, focusing on processing collected feedback and testing the first integrations between partner solutions.
- **Cycle 4 (October 2026 – March 2027):** Finalization and operational validation of technological solutions. This phase concludes with the final performance evaluation, measuring results against the targets defined in Cycle 2.
- **Reporting Phase (April 2027 – May 2027):** Final two-month phase entirely dedicated to drafting and finalizing the LL4 technical report, deliverable D3.5. Subsequent activities, such as dissemination, will continue according to the overall project plan but are no longer part of LL4 operational work.

The following detailed plan focuses on **Cycle 2 (October 2025 – March 2026)**, the first fully operational cycle of the project. Below is a narrative description of the activities for each process, corresponding to the dependability levers, including their specific objectives and the interactions among partners.

Process 1: ODM (T3.5.C.2)

This development line, led by Seafar in close collaboration with TECNALIA, aims to enhance the Object Detection Model (ODM) and validate its resilience to cyberattacks (Use Case 1). The process starts with **Data Sharing** (ongoing), where Seafar provides specific datasets. These data feed into TECNALIA's **Threat Analysis and Research**, aimed at identifying model vulnerabilities. Based on the results, **Attack Simulation** will be conducted to test system behaviour under adverse conditions. The cycle concludes with **Validation Tests** to quantitatively measure the improvement in model robustness.

Process 2: HIRA (T3.5.C.3)

This workflow, involving Seafar, NTUA, and SINTEF OCEAN, aims to lay the foundations for partial automation of risk analyses. The first phase consists of **Selecting the System/Process** to analyse (ongoing). Candidates include, for example, the full remote navigation process or operator shift optimization for sequential management of multiple vessels. Once the scope is defined, a **Reference Analysis (HAZOP/STPA)** is performed using traditional methodologies. This benchmark is critical as it provides a reference for comparing the results of new semi-automated tools in subsequent cycles.

Process 3: NMD (T3.5.C.3)

In collaboration with TU DELFT and KONNECTA, this line focuses on designing the intelligent dependability supervisor architecture. Initial **Data Sharing** by Seafar is the starting point, followed by **Initial Data Analysis** to understand signal patterns and features. The main outcome of this cycle is the **Design of the Cyber-Physical Framework**, defining the system architecture, including interactions between AI models, sensors, and actuators, in preparation for full development in subsequent cycles.

Process 4: RLO (T3.5.A)

This process, coordinated by Seafar with potential involvement of DVW, is exploratory in this first operational cycle. Parallel activities of **Requirements Extraction** and **Operator Criticality Analysis** (through interviews or workshops) aim to collect all necessary information (ongoing). The goal is to converge by December on a **Definition of Future Developments**, i.e., a clear action plan to guide software development for RLO starting January 2026.

The description of these four operational processes forms the executive core of Cycle 2. The Gantt chart below translates the narrative plan into an **operational timeline** (Table 21).

Table 21: LL4 Cycle 2 Gantt Chart.

Task / Process	Sep 25	Oct 25	Nov 25	Dec 25	Jan 26	Feb 26	Mar 26	Apr 26
T3.5.C.2 ODM & Cybersecurity								
Data Sharing								
Data Analysis & Threat Research								
Attack Simulation								
Validation Tests								
T3.5.C.3 HIRA								
System/Process Selection								
Reference Analysis (HAZOP/STPA)								
T3.5.C.3 Intelligent supervisors								
Data Sharing								
Initial Data Analysis								
Cyber-Physical Framework Design								
T3.5.A Remote Lock Operations								
Requirements Extraction								
Operator Criticalities Analysis								
Definition of Future Developments								
Management & Milestones								
D3.1 Submission								
End of Cycle 1 (milestone)								
Initial KPI Quantification								
Monthly WP3 Meetings								
End of Cycle 2 (milestone)								

6.5 Stakeholder Engagement

Table 22 summarizes stakeholder categories, examples, and planned engagement activities. This framework ensures regular collaboration with core stakeholders and broad dissemination of project results. A key milestone will be the **conclusive project workshop in summer 2027**, aligning with the grant agreement: *“R13 Blueprint Digital Twin for continuous hazard mitigation stakeholder workshop with 20+ participants from ship and barge operators, ports, and authorities to align with industry best strategies”*.

Table 22: LL4 Stakeholders.

Stakeholder Category	Examples	Suggested Engagement Activities
Authorities	Port of Antwerp-Bruges (in the consortium), Flemish Waterway Authority, CCNR and its delegations	Regular meetings, consultations on regulatory compliance, and progress reporting.
Vessel Owners	Clients from Seafar’s portfolio, independent barge operators	Surveys, workshops, and periodic feedback sessions to align on operational needs.
Captains	Freelance captains, crew from partner shipping companies	Direct consultations, hands-on testing sessions, and structured interviews.
Training Centers	Antwerp Maritime Academy, Maritime Academy in Harlingen	Collaboration on skill development, curriculum workshops, and feedback on training content.
Technology Developers	Tresco, Shipping Technology	Technical meetings, prototype testing, and iterative feedback loops on development.
Research Centers	SINTEF (in the consortium), MARIN	Knowledge exchange forums and joint studies.
Chartering Companies	HGK Shipping, Cargill, Kühne + Nagel, DSV	Periodic consultations and feedback on operational and market requirements.
Classification Companies	DNV (in the consortium), Lloyd’s Register	Compliance reviews, technical assessments, and formal reporting.
Funders	European Commission	Progress reports, milestone reviews, and formal financial and activity reporting.
Legal Advisors	Specialized maritime law firms	Consultations on legal frameworks, regulatory advice, and compliance verification.
Remote Operations / Inland Navigation Facilitators	Pro Danube, Nautilus International, European Barge Union, European Skippers’ Organization	Dissemination of results.

6.6 Implementation Risks

The planning phase concluded with the identification and assessment of risks that could affect the LL4. Using a Risk Breakdown Structure (RBS), the risks were classified by type (technical, organizational, financial, etc.), evaluated through a probability-impact matrix, and linked to specific response strategies. The RBS is available in Table 23.

Table 23: LL4 Risk Breakdown Structure and Mitigation Measures.

#	High-Level Source	Detail Source	Description	Related Task	Response	Mitigation Measure
R1	Technical	Technological immaturity	Overestimation of TRL	T3.5.A	Reduce	Set clear expectations with potential users.
R2	Technical	Technological immaturity	Lack of scalability or robustness	T3.5.A	Reduce	Be aware and avoid insisting on non-scalable solutions.
R3	Technical	Integration issues	Incompatibility with existing systems	T3.5.A	Accept	Document the causes of malfunction.
R4	Technical	Integration issues	Lack of standardized interfaces	T3.5.A	Accept	Document the causes of malfunction.
R5	Technical	Data quality	Sensor or data collection failures	T3.5.D	Reduce	Provide rapid and adequate IT support.
R6	Technical	Data quality	Isolated data or limited access (IP/privacy)	T3.5.D	Reduce	Clarify willingness to share historical data and federation needs.
R7	Technical	Data quality	Incomplete or distorted datasets	T3.5.D	Reduce	Provide rapid and adequate IT support.
R8	Ethical & Legal	Civil liability	Accidents or damages during tests	T3.5.A, T3.5.B	Avoid / Transfer	Avoid, but transfer risk via insurance.
R9	Ethical & Legal	Civil liability	Lack of insurance	T3.5.A, T3.5.B	Avoid	Take out appropriate insurance coverage.
R10	Ethical & Legal	Civil liability	Misuse of data/technology	T3.5.C, T3.5.D	Reduce	Clearly explain to partners how data and technology will be used.
R11	Stakeholder	Misaligned expectations	Expectation of a finished product (not prototype)	T3.5.A	Reduce	Manage expectations as in R1.
R12	Stakeholder	Resistance to change	Lack of trust in technology/partners	T3.5	Reduce	Respond to doubts with evidence and concrete data.

7 Conclusions

The WARRANT Living Labs (LL1–LL4) constitute the project’s primary means of validating the methodology and tools developed in WP1 and WP2. Together, they demonstrate how the proposed framework for dependable Waterborne Digital Systems (WDS) can be applied in diverse operational contexts, ranging from ocean-going containerships and smart container systems to autonomous inland vessels and remote operation centres. Their comparative insights (see Table 24) feed directly into the WARRANT Knowledge Platform (encompassing the Digital Twin, Dataspace, and Knowledge Graph), updating hazard libraries, resilience controllers, cybersecurity toolchains, training and procedures, framed as procedural assurance components, together with regulatory solutions. This ensures that the WARRANT methodology remains adaptive, scalable, and regulation-ready across all major maritime domains.

Each Living Lab is designed to capture distinct dependability challenges and defines a set of use cases that serve as concrete testbeds for the project’s objectives - testing, feedback, and refinement of the WARRANT methodology, a role beyond a simple pilot. These use cases must therefore be understood as planned experimental activities, coordinated to ensure consistency across partners and alignment with the objectives of the task:

1. Gathering stakeholder requirements and translating them into technical validation scenarios.
2. Testing and refining the dependability methods and tools developed in WP1 and WP2.
3. Quantifying impact through harmonised KPIs for safety, resilience, cybersecurity, and reliability.
4. Establishing sustainability and exploitation pathways for post-project continuation.

From a coordination perspective, the four LLs collectively ensure coverage of the main WDS categories and provide complementary viewpoints:

- **LL1 (Danaos)** focuses on the coordination of cybersecurity and resilience activities on large containerships, detailing the planned phases, involved partners, and dependencies with WP1–WP2 risk analysis tools.
- **LL2 (AELER)** plans the integration and testing of smart container communication within ship and port infrastructures, with clear milestones and contingency options for pilot execution.
- **LL3 (DST)** schedules iterative validation cycles for autonomous inland vessels, explicitly linking activities and KPIs to the development of resilience controllers and HIL/SiL testing.
- **LL4 (Seafar)** coordinates dependability improvement actions for remote operation systems through structured work breakdowns, RASCI matrices, and defined experimental cycles.

This deliverable therefore provides a detailed coordination framework, specifying how objectives are operationalised through activities, roles, schedules, and evaluation metrics. The planning ensures that the LLs collectively validate the full dependability loop envisioned in WARRANT:

from model development → to operational validation → to feedback and continuous improvement.

The outputs of these activities — in the form of validated methodologies, KPIs, and Digital Twin-based Blueprints — will feed the WDS Knowledge Platform and form the foundation for Deliverables D3.2–D3.5, demonstrating measurable and transferable improvements in WDS dependability, resilience, and security.

Table 24: Comparative overview of the WARRANT LLs.

Aspect	LL1 (Danaos)	LL2 (AELER)	LL3 (DST)	LL4 (SEAFAR)
Vessel / System Type	Large ocean-going container ships (deep-sea routes).	Smart container systems.	Autonomous inland vessels & port-linked operations.	Remote Operation Systems (ROS) for barges (Rhine & Antwerp).
Operational Focus	Cybersecure navigation, assurance Digital Twins, Port operations (berthing, mooring)	Dependable container monitoring with ship-LAN integration; hazard alerts.	Resilience controllers, modular sensing, redundancy, HIL testing.	Dependability of ROS: connectivity, human-AI collaboration, AI assurance.
Regulatory Context	IMO & IACS cyber-resilience standards (MSC.428, E26/E27).	Gaps in container-ship integration not yet covered by maritime regulations; evolving ISO/UNECE standards.	National/regional inland waterway rules (CESNI), different from IMO ocean regimes; strong port authority role.	Mixed regulatory setting: flag state rules for ROS, inland navigation law, class society certification for remote ops.
Key Hazards	GNSS spoofing/jamming, ECDIS data corruption, multi-vector cyberattacks.	Lack of LAN integration → delayed fire/overboard alerts; insecure wireless relays (GSM/BLE).	Restricted waterways, lock/bridge constraints, port interaction failures, local comms disruptions.	Connectivity loss, AI misclassification, cyberattacks on ROC, sensor faults.
Testing Approach	Mapping WP1 WDS models to actual LL ships; validation via assurance DTs and cyber-vulnerability testing.	Digital testing of container hazards, integration into ship LAN + DT; validation of alert latency and reliability.	HIL testing with DST simulators & inland testbeds; validation of resilience controllers and redundancy strategies.	ROC Digital Twin calibration; adversarial ML testing of AI apps; evaluation of human-AI collaboration under degraded states.
Resilience Enablers	Intelligent Dependability	Encrypted, authenticated	IDS adapted for inland operations;	IDS for ROS hazard mitigation; multi-

Aspect	LL1 (Danaos)	LL2 (AELER)	LL3 (DST)	LL4 (SEAFAR)
	Supervisor (IDS), DT-enabled assurance, automated compliance reporting.	container-ship comms; DT validation of hazard scenarios.	modular physical + Virtual sensors; federated redundancy.	channel secure comms; Distributed Ledger-based identity management.
Expected Outcomes	Blueprint for Dependable Containership WDS (cybersecure, regulation-compliant, proactive assurance).	Blueprint for Dependable Smart Container Systems with validated ship-LAN connectivity and hazard alerts.	Blueprint for Resilient Autonomous Inland Vessel Operations , adapted to regulatory and inland waterway contexts.	Blueprint for Dependable Remote Operations , demonstrating safe human-AI collaboration and continuous hazard mitigation.

References

- Hollnagel, E. (2009). The Four Cornerstones of Resilience Engineering. In *Resilience Engineering Perspectives, Volume 2*. CRC Press.
- Laprie, J. C. (1992). Dependability: Basic Concepts and Terminology. In J. C. Laprie (Ed.), *Dependability: Basic Concepts and Terminology: In English, French, German, Italian and Japanese* (pp. 3–245). Springer. https://doi.org/10.1007/978-3-7091-9170-5_1
- Malmberg, K., Vaittinen, I., Evans, P., Schuurman, D., Ståhlbröst, A., & Vervoort, K. (2017). *Living Lab Methodology Handbook*. <https://doi.org/10.5281/ZENODO.1146321>