

D5.1 QUALITY ASSURANCE AND RISK MANAGEMENT



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	D5.1: Quality Assurance and Risk Management
Deliverable Due Date	30.09.2025
Deliverable Submission date	30.09.2025
Work Package	WP5
Lead Partner	NTUA
Leading Author	Alexandros Koimtzoglou Konstantinos Louzis Sofia Koufou
Dissemination Level	Confidential

Document History

Version	Date	Author	Description of change
0.1	23.06.2025	NTUA	First version (TOC, Quality Review process, Configuration Management, Risk Management, Appendix A, B, C)
0.2	01.09.2025	NTUA	Draft version (80% ready)
0.3	16.09.2025	INLECOM	Version ready for review
0.4	17.09.2025	INLECOM	Review
0.5	25.09.2025	NTUA	Revision of review comments
1.0	30.09.2025	NTUA	Final version

Table of Contents

1 EXECUTIVE SUMMARY	7
2 INTRODUCTION	8
3 QUALITY REVIEW WITHIN WARRANT	11
4 DOCUMENT CONFIGURATION MANAGEMENT	21
5 QUALITY ATTRIBUTES AND KEY PERFORMANCE INDICATORS	23
6 CONCLUSIONS	29
APPENDIX A: REVIEWERS LIST AND REVIEW DEADLINES	30
APPENDIX B: REVIEW FORM	31
APPENDIX C: DELIVERABLES LIST	33
APPENDIX D: MAJOR RISKS AND RISK REGISTRY	35

List of Figures

FIGURE 1 THE WARRANT REVIEW PROCESS.....	16
--	----

List of Tables

TABLE 1 DOCUMENT DELIVERABLE QUALITY CRITERIA.....	12
TABLE 2 WARRANT REVIEWERS LIST.....	19
TABLE 3 DELIVERABLE NAMING SCHEME.....	21
TABLE 4 DELIVERABLE REVIEW NAMING SCHEME.....	22
TABLE 5 NAMING CONVENTION THE MEETING MINUTES DOCUMENT.....	22
TABLE 6 THE SCALE OF SEVERITY RATING (S).....	25
TABLE 7 THE SCALE OF THE PROBABILITY RANKING (P)	26
TABLE 8 THE SCALE OF THE DETECTION RATING (D).....	26
TABLE 9 RISK MATRIX.....	26
TABLE 10 INITIAL KEY PERFORMANCE INDICATORS (KPIS).....	27

Acronyms

AB	Advisory Board
DL	Deliverable Leader
DoA	Description of Action
EC	European Commission
FMEA	Failure Mode and Effects Analysis
GA	Grant Agreement
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
LL	Living Lab
PC	Project Coordinator
PMR	Periodic Management Report
PO	Project Officer
PR	Project Reviewer
PSB	Project Steering Board
QA	Quality Assurance
TL	Task Leader
ToC	Table of Contents
WP	Work Package
WPL	Work Package Leader
QA	Quality Assurance
QRM	Quality and Risk Manager
TL	Task Leader

1 Executive Summary

This document provides an overview of the quality management procedures applied throughout the WARRANT project, including design, implementation and living labs stages. It presents planned and systematic processes and steps to ensure that the project achieves its quality objectives and delivers high-quality results.

The document defines Key Performance Indicators (KPIs) for monitoring project progress and quality, identifies major risks related to project operations and proposes mitigation strategies. Compliance with the Quality and Risk Management Plan is a joint responsibility of all project partners until all obligations under the European Commission (EC) Grant Contract are fulfilled. The plan also supports the monitoring of corrective actions to ensure that agreed procedures are effectively implemented.

The document is structured as follows:

- **Section 1** is a preamble of the project's quality management procedures along with the summary of subject document structure.
- **Section 2** is an introductory section that outlines the objectives and results of the document as well as the links to the overall project and other deliverables.
- **Section 3** presents the quality reviewing activities that have been designed for the quality assurance of the project deliverables.
- **Section 4** describes the configuration management activities that will take place within WARRANT for each deliverable.
- **Section 5** highlights the Quality Attributes and the KPIs that were set for the WARRANT project, in order to assess the quality of the project results. At the same time, it introduces an early, but detailed description of the major risks envisaged for the project operation, together with the proposed mitigation strategies.

2 Introduction

This deliverable is part of WP5 “Project management”, task T5.2 “Quality assurance and risk management” and more specifically of sub-task T5.2.1 “Quality plan and assurance”. Its purpose is to define the quality management framework and the respective procedures that the Consortium will follow to ensure high-quality work and effective risk management throughout the WARRANT project. This document sets the foundation for assuring the conformity and quality of all project deliverables with the respective requirements.

The consortium is committed to follow specific processes to provide high quality deliverables and provide reliable results within the defined scope, schedule, and budget. Quality will be ensured by implementing quality management procedures and appointing a Risk and Quality Manager (NTUA), who will be responsible for monitoring and advising partners on quality procedures and ensuring conformity to standards.

In more detail, the objectives of the Quality Management Plan can be listed in five categories:

- Structure: defining the quality management structure and processes adopted;
- Input: clearly defining the strategic goals, milestones, ensuring realistic schedules and sufficient resources;
- Output: implementing an effective internal and external information and communication system, decision making process, documenting intermediate and final results (e.g., software, solutions, tools);
- Feedback: monitoring of the quality of processes and results, keeping the project on schedule and budget;
- Implementation: appointing the responsible body with the authority to take and implement decisions on the necessary corrective measures (QRM, PC and WPL) and ensuring the commitment of partners.

Practices defined in this plan are intended to ensure that quality is integrated into WARRANT working processes. Therefore, the plan consists of dedicated and systematic activities to determine and ensure achievement of the WARRANT quality objectives.

The Quality Management Plan ensures the quality of all project deliverables and the proper risk management, assuring coordination activities among partners during the tasks’ execution, throughout the whole project’s duration. The Quality Management Plan defines procedures and quality KPIs that the Quality and Risk Manager (QRM) will monitor throughout the project. Each Deliverable Leader (DL) will be responsible for the quality of results for the deliverable; the latter will be subject to a review by the QRM and two reviewers from the partners not authoring the specific deliverable.

The Quality Management Plan provides a framework that ensures consistency across all project work packages. Furthermore, quality reviewing procedures, configuration management and risk mitigation strategies defined in this deliverable are applied to all project deliverables.

2.1 Mapping WARRANT outputs

The table below provides the WARRANT Grant Agreement commitments, as defined in the Deliverable and Task descriptions, in relation to the current document.

WARRANT GA Component Title	WARRANT GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D5.1 Quality Assurance and Risk Management	<i>This deliverable establishes robust frameworks for quality assurance and risk management, ensuring project objectives are met efficiently and effectively. Success is verified through compliance with quality standards and proactive risk mitigation during project evaluations, under Task 5.2.</i>	3-5	<i>This deliverable establishes frameworks for quality assurance and risk management by defining procedures, roles, KPIs and risk monitoring process, to ensure that all project objectives are met efficiently. Success is verified through structured peer reviews, continuous monitoring and proactive corrective actions as outlined in the Quality Management Plan.</i>
TASK			
T5.2 Quality assurance and risk management (ST5.2.1 Quality Plan and Assurance & ST5.2.2 Risk Management)	<i>ST5.2.1 Quality Plan and Assurance: Develop a quality plan detailing standards and procedures for reports, deliverables, peer reviews, and monitoring activities. This task ensures that all project deliverables meet the required quality standards and align with the overall project objectives. The Quality Management Plan will serve as the guide for maintaining the quality and conformity of all project outputs, facilitating internal assessments. ST5.2.2 Risk Management: Implement a Risk Management</i>	3-5	<i>The Quality Management Plan validates this framework by defining procedures, peer reviews, KPIs, and monitoring activities that ensure all deliverables will meet quality standards and align with project objectives (ST5.2.1). Risks are proactively managed through continuous assessment and</i>

	<i>Plan to continuously monitor and update the list of project risks, minimizing their likelihood and impact. The task involves proactive management of potential risks throughout the project's duration, ensuring timely awareness and mitigation strategies. The Coordination Team, with support from the Technical Manager, will assess technological changes and advise on necessary actions. Risk management updates will be included in the Periodic Progress Reports.</i>		<i>mitigation strategies, with updates documented in progress reports to maintain project reliability (ST5.2.2).</i>
--	--	--	---

2.2 Intended Readership

The plan set out in this document will govern the actions of all project partners throughout the project duration. It is therefore important that all partners have access to it and a possibility to consult it at all times.

3 Quality Review within WARRANT

The QRM (NTUA) serves as the contact point for the Project Coordinator (INLE) who is leading Project Management and ethics activities and all project partners on all WARRANT quality matters.

Within the WARRANT project, the review of the deliverables will be conducted as described in the following sub-sections.

3.1 Reviews for Documentation - Deliverables

Each project deliverable is assigned to one leading responsible partner (Deliverable Leader, DL), as defined in the WARRANT Description of Action (DoA), who also serves as the Task Leader (TL) of the task to which the deliverable belongs. A detailed list of Work Package Leaders (WPL) and Task Leaders (TL) is presented in Grant Agreement (GA). The DL must guarantee that the deliverable will be submitted on time, along with its high quality. The DL must also assure that the content of the deliverable conforms to the deliverable description of the GA and that the objectives related to the goals of the work package and the project are met. Any issues related to the deliverables, such as endangering the success of the work package or the project, must be reported by the WPL immediately to the PC and be further discussed within the Project Steering Board (PSB), led by the PC, if needed.

Project documentation will be reviewed against the following criteria:

- Format of the document according to the WARRANT template.
- Consistency with GA, to ensure that the deliverable reflects what is stated there.
- Consistency with previous relevant documentation (for example, technical specifications combined with the requirements definition).
- The methodology of the work, development, trial, test, experiment, or study conducted is in a manner appropriate to the task.
- The results are realistic, useful, and reliable and the deliverable is useful to downstream tasks.
- Technical aspects of the documentation will be reviewed from the PC, to ensure that the document meets the technical goals of the project. The conclusion of the deliverable must be comprehensive and coherent and contribute to the overall project objectives.
- Identification of plagiarism, inappropriate authorship credit, data falsification, image manipulation.
- Consistency with ethics issues and gender-inclusive language.
- Citation of appropriate sources must be declared.

Other criteria:



- Identification and correction of typing mistakes, spelling or grammar mistakes that may cause misunderstanding.
- The structure of the document is rational and easy to follow.
- Figures and tables are legible and referred to with cross references in the text.
- The length of the deliverable's main body is consistent.
- The references of the papers and other sources used are correct.
- Terms and abbreviations are all defined.
- Any mathematical or other symbols used in the document are sufficiently defined.
- The existence of a conclusions section, which is mandatory for all the deliverables.

The overall procedure and timeline for the review project documentation is described in the following paragraphs.

The deliverables will be assessed by two (2) reviewers, and assessments are based upon the Review Form specifically designed for WARRANT for document deliverables. All deliverables will have passed review successfully and have been internally approved before they are uploaded to the EU monitoring system. The Review Form (shown in Appendix B), will be used during evaluation to assess and evaluate each deliverable's performance with questions pertaining to the criteria presented in Table 1 below.

3.1.1 Document Deliverables

The guidelines for written document deliverables are highlighted. These are especially important for public deliverables, but the partners are generally encouraged to adhere to these to maintain a good level of quality, and for the deliverables to be accessible to all consortium partners.

All deliverables will use the deliverable template provided and will adhere to the formatting guidelines explained in that template. Deliverable language should be British English (UK *not* US). Authors are encouraged to use plain English so that the deliverable is more accessible, except in cases where there is technical language that should be used.

Table 1 Document deliverable quality criteria.

Category	Criterion
Content Quality	Objective(s) of deliverable are clearly addressed.
	Methodology applied is complete and justified.
	Results contribute to project plan and follow the GA.
	Use of references to avoid plagiarism.
	Conclusions are justified from content.
Structure	WP Tasks are identified clearly in the content per the GA.
	Key contributions are easy to track.
	Complete glossary & definitions of terms.
	Mathematical symbols are defined adequately.
	Template has been applied properly.
	Correct & consistent citing of other work & resources.

Readability	Key vision, ideas, contributions & State-of-the-art improvements are discussed explicitly and are easy to understand.
	Fonts, figures, tables, screenshots etc. are clearly legible.
	The English language is used appropriately & the deliverable is easy to understand.

It is important that terminology and technical terms are consistent within the deliverable, and across deliverables to the extent possible. Although there is a glossary for terms and acronyms at the start of the document, authors should spell out in full the acronym on its first use for ease of reading. Authors should cite work external to the project appropriately, using APA citation standard.

All deliverables should include an executive summary of the deliverable no more than one page long. This should explain in brief the contribution of the deliverable towards WARRANT's goals and should summarise the purpose and vision of the work presented along with key techniques, state-of-the-art contributions, and findings. Ideally, and especially for technical deliverables, the reader should be able to understand all these aspects without being a technical expert. So, authors are encouraged to summarise chapters in plain language at each chapter's start as well.

Last, deliverables should not exceed 100 pages. In the case where there are too many figures and tables that must be provided, exceptions can be made.

3.1.2 Review process

The review process of deliverables is a formal procedure which is mandatory, and partners are requested to pay particular attention to this process and adhere to the format and procedures explained in this section. It is essential to initiate the review process as early as possible to give the authors enough time to make proper amendments to the document. A summary of the review process can be seen in Figure 1. In particular, the process consists of three steps

- The initial step where, the ToC of the deliverable will be reviewed, in order to ensure that the structure of the deliverable is efficiently approached and presented therein.
- The intermediate step where the deliverable (with 50% level of completion) will be reviewed, 4 months prior the submission date, to ensure the content and the progress is made at this stage.
- The final step where the deliverable will be reviewed by two (2) reviewers.

Initial Step (Review of Table of Contents)

This step includes an initial review of the earliest stage of the deliverable development. The DL will prepare the ToC reflecting the proposed structure and content of the deliverable. The ToC must be provided to the QRM and PC by the end of the first month of the task that the deliverable is associated. The purpose of this step is to ensure that the deliverable's early development aligns with its objectives as well as the DoA to prevent any major changes that could invalidate work already completed.

Intermediate Step (Review 50% Draft Deliverable)

This step serves as an internal project milestone to ensure the content and the progress achieved for the deliverable as well as ensure a high quality of results and issues or risk that have been resolved close to the submission dates of the deliverables. The process for the intermediate step is as follows:

- DL will provide a draft deliverable which is at least 50% ready to MS Teams, by the designated date (4 months prior the submission date).
- DL will notify the QRM to review the document. The QRM will provide clear suggestions to the authors via email, and if further clarifications are required the involved partners will meet via a teleconference to discuss and resolve them.
- DL along with the deliverable partners will amend the document as suggested, if necessary.
- The QRM and the PC will review the revised draft and will approve the 50% Draft version via email to the DL.

Final Step (Formal Review)

If the previous review process steps deadlines have been followed, the DL should have uploaded to MS Teams the 100% Draft deliverable at most one month prior to the deliverable submission due date. From that point on and until the official submission of the deliverable by the PC, the deliverable authors must be available through email as well as teleconference.

Upon completion and upload of the 100% Draft, the DL must submit the deliverable for formal Review. This should be done one month prior to the deliverable submission due date to avoid any delays in the process. Submission requires the DL author to upload on the MS Teams the 100% Draft deliverable and also send it to the assigned reviewers via email including the QRM as well as the PC. In the email, the DL and the authors should highlight any internal quality check processes undertaken within their organisation that apply to the deliverable. Furthermore, it must be clear whether the document has been submitted to plagiarism detection software (available in all universities, or free e.g. Dupli Checker, etc.), detailing the results and the actions taken.

There are a few additional things that are very important to keep in mind for the submission:

- Make sure that the document sent for review is complete (final 100% draft).
- The deadlines should be met to allow enough time for the review and revision.
- Acknowledge all the contributors in the document.

After the DL submits the file to the reviewers, the formal review process starts. *Reviewers are required to finish the review 15 days after receiving the submitted deliverable.* If this is not a working day, reviewers can submit their review the first working day after the 15-day deadline if they wish to. Reviewers can contact the author(s) at any point for clarifications and can request a teleconference with the authors prior or during the review, should they wish to, for the authors to explain the purpose, structure, and context of the deliverable, or any other clarifications related to the deliverable under review.

Reviewers should use the Review Form (provided in Appendix B) and evaluate the deliverable according to the criteria in the form (also explained in Section 3.1.1) in a systematic way, filling in the corresponding boxes for each criterion. Reviewers should evaluate the deliverable also against

other relevant project documents such as the GA, other relevant deliverables, and related external resources such as scientific literature and common practices.

The reviewers will indicate in the Review Form whether, in their opinion, the deliverable needs minor or major corrections. In both cases, and especially in the case of major rework, the reviewer should make suggestions to the authors to help revise/rework the document using the comments box in the form. In the case where the reviewer indicates major amendments are required, it is *mandatory* that the authors re-submit the document to the reviewers for a second round of formal review.

The Reviewers for each deliverable were selected by applying the following criteria:

- They should not be in the author's list or contribute to deliverable that will be reviewed.
- The dependencies among WPs, Tasks and Deliverables. For instance, if a partner is DL for an upcoming deliverable that depends on a previous one, then it was selected as a reviewer.
- The overall budget of each partner in the project. Efforts were made to ensure that partners with lower budget were assigned fewer reviews compared to those with higher budget.

A detailed list of Reviewers for each deliverable can be found in Appendix A. The Reviewers List was provided to all partners to provide any comments or objections. Therefore, *the selected reviewers will not be able to decline the invitation to review the deliverable except in special and adequately justified circumstances*. In case Partners (reviewers) have justified reasons to decline, they are to notify the QRM and the PC at the earliest convenience for them to be replaced. Additionally, early in the project, partners will be asked to provide the persons who are going to carry out their reviews by filling their name and email in the Reviewers List in the MS Teams project repository.

Regardless of the Review Form, reviewers are strongly encouraged to use the "Track Changes" function in Word and make direct corrections on the deliverable regarding e.g. grammatical/punctuation errors or short rephrases if the content is not clear enough. Reviewers should also add comments in the document to indicate necessary clarifications in certain parts or to express their concerns in more detail.

Submission of the Formal Review Form

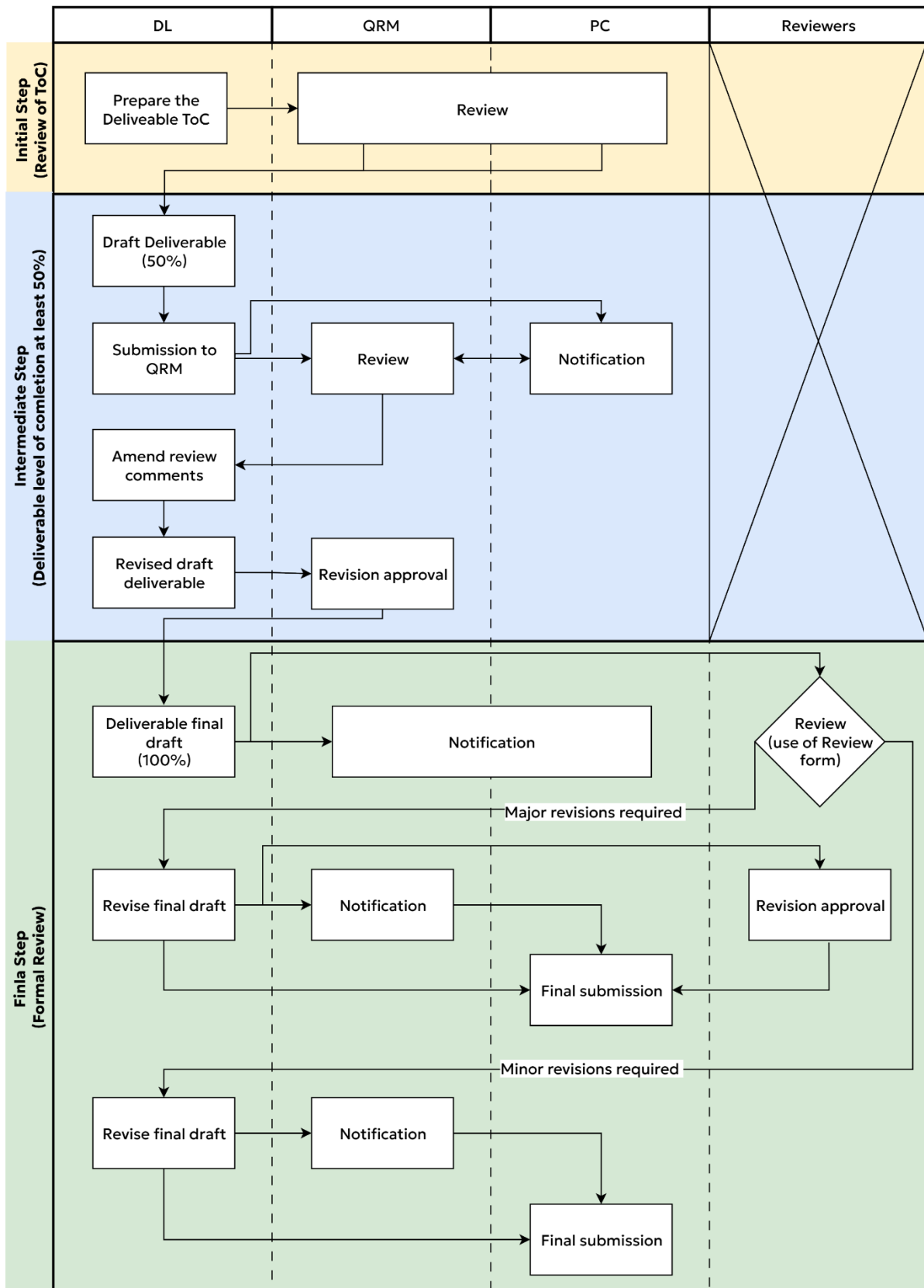
Upon completion of the Review Form, the reviewers must send it via email to the deliverable author(s) and add the QRM and the PC in cc. The reviewers should also upload the completed review forms in MS Teams. The email should also include the reviewed version of the deliverable which should include relevant comments and corrections by the reviewers. Authors should begin addressing the reviewers' comments and concerns immediately. Authors are required to indicate in the review forms they received how and where in the document they addressed reviewers' comments. Authors will email the corrected version of the deliverable together with the completed review forms back to the reviewers, adding the QRM in cc. The reviewers need to reply that indeed their concerns have been addressed. The document should be ready and approved by the reviewers at most one week prior to the official submission due date.

Sometimes it may be the case that (i) there are contradicting views by the reviewers, (ii) major changes are necessary, and/or (iii) the authors are unsure about what exactly is being suggested



by the reviewers. Should any of these occur, the authors may contact via email the reviewers adding the QRM and PC in cc, then the authors and reviewers should set up a teleconference meeting quickly (within a few days at most so that authors have time to address issues) to discuss the concerns. Especially in the case where the views of the reviewers may be contradictory, the reviewers must discuss with each other and come to an agreement on (i) whether there is indeed a contradiction in their reviews, and (ii) what the suggested action by the authors is, if the previous is true.

Figure 1 The WARRANT review process



3.2 Review for Hardware, Software and Living Labs Monitoring

Software document deliverables will follow the same QA procedure as for regular document deliverables, as explained in Section 3.1.

There will be no explicit formal review for software components. Instead, quality assurance for the software components will be pipelined through the QA monitoring and reporting processes of the LLs as presented in this Section. Nevertheless, partners should apply proper and suitable practices in the development of the software they are responsible for.

It will be the partners' responsibility to review and select the most appropriate practices according to their needs and the requirements of their respective tasks. Therefore, for efficient software implementations of high quality, and for tracking the work done effectively, partners are strongly encouraged to:

- Use source & version control, and bug tracking. Git is suggested as a version control system. These can all be accommodated via using e.g. GitLab which is a strong DevOps platform for source code management.
- Test software appropriately.
- Consider the licensing implications early on. Partners are free to use any libraries, tools, and programming environments they wish, but these will have certain implications according to the license they are distributed with.
- Prototypes should be readily available, and partners should seek out feedback as early as possible.

Living Labs monitoring procedure is described in the following steps:

1. LL Specification. Decide what applications are involved in use-cases, aligned with the overall strategy.
2. Application of the proposed technologies. Meetings will be organised across LLs to share intermediate findings.
3. Validation of the results. The QRM and the PC, with the input of relevant partners, will specify the level of achieving the various KPIs.

3.3 Reviews for Dissemination Material

Dissemination material, such as leaflets, newsletters, conference presentations, and scientific publications will undergo a quality check by the PC, the Dissemination and Communication (D&C)



Manager and the QRM before their actual publication. This review process aims for quality, fairness, transparency and maximization of impact. The PSB will review the submissions and verify that:

- The quality is at the desired and expected level.
- The contents have proper references to the work conducted by the partners and no information which may require clearance from the partners.
- That proper acknowledgement to the EC is made, including Grant Agreement number.
- In case there are issues of any kind, the board should be able to properly justify its decisions.

3.4 Deliverable Assignments for the Review Process

The relevant two (2) reviewers for each deliverable have been assigned by the QRM and the PC are shown in Table 2 below. The reviewers should be notified at least one (1) month prior to the submission of the deliverable.

Table 2 WARRANT Reviewers List.

Del. No.	Deliverable Name	Lead Partner	1 st Reviewer	2 nd Reviewer
D1.1	WDS and SRODS Models and Methodology for robust system integration and HAZOP analysis	SO	VLTN	NTUA
D1.2	WDS Dependability assessment and enhancement management	INLE	KNT	DNV
D1.3	Intelligent Dependability Supervisor with Modular Sensing and Actuation	TUD	DST	DAN
D1.4	Consolidated Methodology enabling effective HAZOP and STPA analysis of AI- enabled ship IT/OT systems	DNV	SO	TEC
D2.1	Innovative WDS Cybersecurity Improvement Tools	TEC	INLE	KNT
D2.2	Support Tools for Methodology Adoption by Industry	SO	NTUA	KNT
D2.3	Reference Digital Twin Dependability Management for WDS	KNT	SD	POAB
D2.4	WARRaNT Dataspace	INLE	DNV	TUD
D3.1	Detailed planning and coordination of LLs	NTUA	SO	KNT
D3.2	LL1 Dependable Containership Digital Systems	DAN	TUD	INLE
D3.3	LL2 Application of the WARRaNT Methodology to Smart Container Systems	AEL	NTUA	INLE
D3.4	LL3 Increasing the resilience of automation systems in autonomous green vessels	DST	SO	TUD

Del. No.	Deliverable Name	Lead Partner	1 st Reviewer	2 nd Reviewer
D3.5	LL4 Enhanced Dependability of Remote Operation Systems	SEA	POAB	TEC
D4.1	Dissemination and Communication Plan v1	KNT	AEL	SEA
D4.2	Dissemination and Communication Plan v2	KNT	DST	SEA
D4.3	Dissemination and Communication Plan final version	KNT	DNV	TEC
D4.4	Innovation Management and Exploitation Strategy	INLE	SEA	VLTN
D4.5	Cybersecurity training	SD	NTUA	DNV
D4.6	Adoption pathways simulation and optimization	VLTN	DAN	SO
D4.7	Capacity building – Standardization and policy recommendations	SO	DAN	NTUA
D5.1	Quality assurance and risk management	NTUA	INLE	AEL
D5.2	Data Management, GDPR and Ethics v1	INLE	SD	AEL
D5.3	Data Management, GDPR and Ethics final version	INLE	TUD	SD

The list of deliverables with additional information is presented in Appendix C.

4 Document Configuration Management

Document Configuration Management deals with the overall project consistency, identification and tracking of changes related to all project results, including the deliverables, documents, testing procedures and any other related activity. The QRM will be responsible for the overall monitoring of all configuration management activities described in this section.

The Document Management process will be ensured through version tracking and history of changes of the various project documents, including the following:

- Deliverables (as stated in the deliverables list in the WARRANT GA).
- Meeting minutes.
- Reviewed documents.

Document history will be tracked in each deliverable in a separate table, describing the different versions of the document and the reasons of the changes/updates on it. The main author of each deliverable is responsible for keeping the changes performed on the document up to date.

Document versioning will be tracked through the monitoring of the Configuration Matrix, in which all versions of each document will be tracked. Also, this table will be updated by each document author.

In the following subsections, the document naming conventions to be followed in WARRANT are analysed.

4.1 Deliverables Naming

Table 3 presents the convention followed for naming the project's deliverable documents.

Table 3 Deliverable naming scheme.

Coding:	GA number_WARRANT_Deliverable Code and Title_vA.B
A:	S/N for major release of the deliverable (Submission to Commission)
B:	S/N for updates during the preparation phase
Example	101136257_WARRANT D1.1_Project Management Plan_v1.0 (for submission to the Commission) 101136257_WARRANT D1.1_Project Management Plan_v0.9 (for internal updates and submission for internal review) Version number to be increased when the review comments have been taken into account the proper modifications have been made

4.2 Deliverables Review Naming

In Table 4 the format regarding the naming convention of the deliverables considering the review process is shown. This format will be used for the reviewed deliverable document (comments and track changes on the existing document) or the Review Form.

Table 4 Deliverable review naming scheme.

Coding:	GA number_WARRANT_Deliverable Code and Title_vA.B_Partner's abbreviation review
A:	S/N for major release of the deliverable (Submission to Commission)
B:	S/N for updates during the preparation phase
Example	101136257_WARRANT_D1.1 Project Management Plan_v0.3_NTUA review

4.3 Meeting Minutes

In Table 5 the format of the naming convention regarding the meeting minutes is presented. This format must be followed for every document of such kind.

Table 5 Naming convention the meeting minutes document.

Coding:	Date_WARRANT_Type of Meeting_Minutes_Place vA.B
A:	S/N for major release of the document
B:	S/N for updates during the preparation phase
Date:	Date(s) the meeting was held. Format: YYYYMMDD
Place:	Place where meeting was held
Example	20240116_WARRANT_Kick-Off Meeting Minutes_Athens/Virtual v1.0

4.4 E-mailing Conventions

Electronic mail will be an important mean of exchanging information in the WARRANT project. All e-mail subject headings must start with the text "WARRANT" and be followed by the relevant WP. Additional tags can be added to specify relevant tasks and deliverables, where appropriate and if deemed useful.

Some indicative examples of email subject headings are:

- WARRANT - WP6 - Title
- WARRANT - WP1 - Task1.2 - D1.2 Title
- WARRANT - WP4 - Task4.1 Title

5 Quality Attributes and Key Performance Indicators

To assess the quality of the project results, in general, several qualitative attributes will be used based on the nature of the WARRANT project and the characteristics of its end-users, as well as the “context of use” of project results.

Furthermore, quality is also addressed by ensuring the compliance of all the project activities to the development process. The main attributes that address this need are:

- Planning accuracy.
- Rework occurrence.
- Conformity to methodologies.
- Redundancy.

All these attributes will play an important role in the measurement of the project Key Performance Indicators (KPIs) described in the following section.

5.1 Risk Management

In WARRANT, risks are considered as an integral part of the workplan. The complexity of the problem at hand and the trans-disciplinary nature of the consortium add to the number of risky aspects that may cause issues during the project lifecycle. However, all these issues are tackled a priori by exploiting the accumulated project implementation experience of partners and by applying a well laid-out management scheme.

WARRANT Risk management is a circular/iterative process, in which risks are identified, monitored, analyzed and managed. The WARRANT risk management process is implemented by the QRM and discussed between PC and WPL during PSB meetings. The QRM is responsible for continuously monitoring project risks, by updating the WARRANT risk register, and drafting an appropriate mitigation strategy for unacceptable risks. The elements of the WARRANT risk management process are outlined below:

Risk identification: All partners involved in the project need to be aware of their contribution to the project objectives and the involved risks that might prevent them from delivering it. These risks will be reviewed at regular intervals to restate current priorities, as project priorities may shift over time (deadlines, budget re-forecasts, and performance expectations) and unforeseen difficulties might arise.

Risk analysis: WARRANT will use estimates of likelihood and impact against the key risks. WARRANT will try to quantify risks wherever possible, by using a scoring system to ensure comparison of risks. The quantification of project risks will be performed considering the most likely outcome scenario for all identified risks.

Risk management: Risk responses in WARRANT will fall under one of the types: a) Avoid the risk: This can be done by avoiding the use of technologies that do not have feasible alternatives; b) Mitigate the risk: If a risk cannot be avoided, management will try to reduce the risk, by making it either less likely or reduce its consequences. This will include the development of contingency plans for those risks which cannot be avoided; c) Accept or retain the risk: Inevitably there will be some risks that are intrinsic in the nature of the work being undertaken and which it is not possible to mitigate, control or avoid because the time and cost involved is too high to justify the benefits. The number and impact of these sorts of risks in the WARRANT project are minimal.

Risk monitoring: WARRANT will run a well-maintained risk registry for monitoring risk-management performance. The registry defines mitigating actions for each risk, citing who will do what and by when.

Risk Contingency Plans: To monitor and minimize WARRANT risks, the consortium will prepare a list of risks and propose contingency plans as early as possible. Table D-1 in the Appendix D presents an initial identification of the main risks and the proposed risk mitigation measures, as described in the WARRANT GA.

More specifically a Failure Mode and Effects Analysis (FMEA) process will be applied, and quality risk levels will be assigned to each step in the design and manufacturing of WARRANT technologies. This will allow the consortium to anticipate risks at an early stage and implement countermeasures ahead of time.

FMEA is a systemized approach used for identifying risk events during product development or for quality improvement activities. Risk event modes are the ways in which a process can fail. Effects are the ways that these Risk events can lead to waste, defects, or catastrophic outcomes for the customer. As such, FMEA approach is designed to identify, prioritize, and limit these Risk Event modes. As with many powerful techniques, the strength of FMEA, applied to WARRANT, will be derived from a cross-functional, partner-based approach.

Initially, a spreadsheet will be used to document the completed FMEA for WARRANT project. The spreadsheet will be comprised by unique columns, each of these columns must follow the formatting of an FMEA methodology. More specifically, the columns of the spreadsheet shall follow the naming format defined in the list below:

- **FMEA ID #:** This column assigns an identification number for internal use.
- **Item/Function:** This column identifies the subsystems (components) of WARRANT technologies along with their functions.
- **Potential Risk Event:** A risk event is defined as the way the item could potentially fail to meet the function intent. In other words, what can go wrong?
- **Potential Risk Event Impact:** A Risk Event impact is defined as the result of a Risk Event on the function of the product/process as perceived by the customer (internal and external customers). Indicative examples of Risk Event impacts are: inoperability of the product, degraded performance etc. Note that Risk Event impacts should be identified for each Risk Event.
- **Work Package #:** This column indicates the related project work package.
- **Severity (S):** This column indicates how serious the potential Risk Event is. A numerical value, S, is assigned to the severity of the Risk Event. This value is in the range of 1 to 5, 1 being the lowest impact on product function or process output, and 5 being the highest.

- **Potential Causes for Risk Event:** A cause of Risk Event is defined as a design weakness which may result in a Risk Event. Note that all potential root causes need to be identified for each Risk Event.
- **Probability (P):** This column indicates how likely (or often) it is that the cause of Risk Event will occur. A numerical value, P, is also assigned to the occurrence which ranges from 1 to 5.
- **Current Process Controls:** For each potential cause of Risk Event, this column identifies current tests or mechanisms in place to prevent the cause of the Risk Event from occurring or which detect the Risk Event before reaching the customer.
- **Detection Rating:** It estimates how well the controls in place can detect either the Risk Event cause or its mode. The detection rating is on a scale of 1 to 5 where 1 means the control is certain to detect the problem and 5 means the control is certain not to detect it.
- **Risk Priority Number (RPN):** In this column, the risk priority number is evaluated for each cause of Risk Event, by multiplying the severity by the probability by the detection rating as follows:

$$\text{RPN} = \text{Severity} \cdot \text{Probability} \cdot \text{Detection}$$

The RPN number, along with the risk level provides guidance for ranking potential Risk Events in the order they should be addressed.

- **Risk Level:** Risk is the combination of probability of occurrence and severity. Risk levels can be selected based on a Risk Matrix. It can be observed that the higher the risk level, the more justification and mitigation is needed to provide evidence and lower the risk to an acceptable level.
- **Mitigations/Requirements:** This column indicates the recommended actions taken to mitigate each potential Risk Event cause. Note that these actions may be design or process changes to lower severity or the likelihood of occurrence. This column can also include additional controls to improve Risk Event detection.
- **Responsibility/Target Date:** Responsibility and target completion date need to be assigned in this column. This makes responsibility clear-cut and facilitates tracking.
- **Actions taken:** This column documents the actions taken. After these actions have been taken, severity, S, probability, P, and detection, D, need to be reassessed and consequently, the risk priority number and the risk level re-evaluated. Based on the revised risk priority number and the risk level, the outcome is determined: either close the action or to require further actions.

Table 6 The scale of severity rating (S)

Severity(S)	Meaning
1	Negligible (no relevant effect)
2	Minor (affects very little the project e.g. minor delays)
3	Moderate

4	Critical (significantly affects the progress of the project)
5	Severe (leads to the stop of the project's progress)

Table 7 The scale of the probability ranking (P)

Probability (P)	Meaning
1	Extremely Unlikely
2	Remote (relatively few Risk Events)
3	Occasional (occasional Risk Events)
4	Reasonably Possible (repeated Risk Events)
5	Frequent (Risk Events are almost inevitable)

Table 8 The scale of the detection rating (D)

Detection Rating (D)	Meaning
1	Detection method is highly effective, and it is almost certain that the risk will be detected with adequate time.
2	Detection method has moderately high effectiveness.
3	Detection method has medium effectiveness.
4	Detection method is unproven or unreliable; or effectiveness of detection method is unknown to detect in time.
5	There is no detection method available or known that will provide an alert with enough time to plan for a contingency.

Table 9 Risk Matrix

P/S	1	2	3	4	5
5	Moderate (5)	High (10)	High (15)	Unacceptable (20)	Unacceptable (25)
4	Low (4)	Moderate (8)	High (12)	High (16)	Unacceptable (20)
3	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
2	Low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)
1	Low (1)	Low (2)	Low (3)	Low (4)	Moderate (5)

The next step is for each Work Package Leader to compile the risks associated with their tasks and to assign responsibility for these actions and set target completions dates. Once corrective actions have been completed, WARRANT partners will reassess and record the severity, probability of

occurrence and likelihood of detection for the high priority Risk Events. This is so that the effectiveness of the corrective action taken can be determined. The risks list of the project will be presented and updated by the WPL during the monthly WP meetings and the QRM will regularly present them (briefly on a monthly basis in PSB meetings and in more detail on plenary meetings). An initial risk registry of the risk identified in the GA is presented in Appendix D.

5.1.1 Consortium Risk Management

The WARRANT consortium has considered consortium-related risks that deal with (1) underestimation of some tasks, (2) low productivity and (3) low quality of work. These risks are already minimized during the selection of partners, which most of them have been selected following specific criteria:

- They are leaders in their areas of expertise.
- They are selected after previous successful cooperation, with coordinator or with other trusted members of the consortium.
- They all have evidence of long history of successful completion of research projects.

However, these risks will be minimized and managed by using established methodologies for hardware/software cost estimation, continuous project planning, monitoring, and control. Such methodologies are standard practice in the professional work of the consortium partners. To this end, timely awareness of and reaction to potential problems will be crucial to effective risk management.

5.1.2 Risk Registry

This Risk Registry will be updated monthly by the QRM based on the relevant input received by the WPLs. The QRM will present and discuss the updates on the risk registry in the PSB, which will be conducted bi-monthly. Furthermore, the QRM will present the identified risk bi-annually, in the Interim Reports and in the PMRs in more detail. The risks will be quantified within Task 5.2 “Quality assurance and risk management”. In case of high-risk situations, dedicated meetings will be arranged, if needed, in order to be mitigated.

5.2 Key Performance Indicators

The PC will monitor the progress of the project objectives, while the QRM will oversee quality assurance and risk monitoring through specific KPIs. These KPIs will be monitored bi-annually and they will be presented in the project’s Interim Report and in the Periodic Management Report (PMR). The metrics included in Table 6 will be used as the starting point.

Table 10 Initial Key Performance Indicators (KPIs).



KPI	Goal (Justification and Goal)
Real month of milestone achievement/due month	Keep the project on schedule (KPI=1). Target: KPI≤1, per milestone.
Overall project risk level	Flag any deviations from targets in advance to allow preventive action. Target: Risk level below moderate.
Real month of deliverable submission/Due month	Ensure compliance with task and deliverable performance procedures. Target: KPI≤1, per deliverable.

6 Conclusions

This Deliverable establishes the quality and risk management procedures that will be applied to the WARRANT project. To accurately describe the quality management plan that is implemented in the project, all aspects of the reviewing process were presented and analysed. Standardized document configuration guidelines for the naming conventions, version control, and the structure of meeting minutes have been also defined to ensure procedural coherence, traceability and transparency across the consortium.

The review process that will be applied consists of three stages. In the first step the ToC of the deliverable will be reviewed by the QRM and the PC to ensure that the deliverable structure covers all the required aspects according to the DoA. In the second step the 50% of the deliverable will be reviewed by the QRM and the PC, 4 months prior the submission date, to ensure the content and the progress achieved. Finally, the third step is the official review of the deliverable, which will be conducted by 2 reviewers following a systematic evaluation within clearly defined timelines and under proper guidance, to ensure the high quality of the deliverables. The reviewers for each deliverable (Reviewers List) have been already assigned following specific criteria.

Furthermore, a risk management process based on FMEA was developed to identify, assess and mitigate potential risk during the life of the project. To this end an initial risk registry has been developed, identifying the main challenges that may affect project implementation. For each risk, appropriate mitigation and contingency strategies have been outlined to safeguard the project objectives. This registry will be a living document and will be continuously monitored, updated and refined throughout the project by the QRM. Collectively, these measures will provide a robust quality and risk management framework that ensures accountability and enhances the reliability and impact of the WARRANT project's outcomes.

Finally, initial basic KPIs and their respective targets have been defined to monitor the progress, ensure the quality of deliverables, and support continuous improvement throughout the project.

APPENDIX A: Reviewers List and Review Deadlines

Table A-1 Reviewers List and Review Deadlines.

D. No.	1 st Reviewer	2 nd Reviewer	Review Start Date	Review Submitted Deadline
D1.1	VLTN	NTUA	01-05-27	11-05-27
D1.2	KNT	DNV	01-06-27	11-06-27
D1.3	DST	DAN	01-07-27	11-07-27
D1.4	SO	TEC	01-08-27	11-08-27
D2.1	INLE	KNT	01-06-27	11-06-27
D2.2	NTUA	KNT	01-06-27	11-06-27
D2.3	SD	POAB	01-08-27	11-08-27
D2.4	DNV	TUD	01-11-27	11-11-27
D3.1	SO	KNT	01-08-25	11-08-25
D3.2	TUD	INLE	01-03-27	11-03-27
D3.3	NTUA	INLE	01-03-27	11-03-27
D3.4	SO	TUD	01-04-27	11-04-27
D3.5	POAB	TEC	01-04-27	11-04-27
D4.1	AEL	SEA	01-06-25	11-06-25
D4.2	DST	SEA	01-08-26	11-08-26
D4.3	DNV	TEC	01-01-28	11-01-28
D4.4	SEA	VLTN	01-12-27	11-12-27
D4.5	NTUA	DNV	01-12-27	11-12-27
D4.6	DAN	SO	01-10-27	11-10-27
D4.7	DAN	NTUA	01-12-27	11-12-27
D5.1	INLE	AEL	01-08-25	11-08-25
D5.2	SD	AEL	01-02-26	11-02-26
D5.3	TUD	SD	01-02-28	11-02-28

APPENDIX B: Review Form

WARRANT Review Form	
Deliverable Number	
Deliverable Title	
Reviewer's Name	
Reviewer's Beneficiary	
Review version	
Date	DD/MM/YYYY

General decision		
The Derivable can be submitted:	As it is	
	After minor revisions	
	After major revisions	
	The Deliverable has significant flaws	

General comments and needed improvements:

Item	Yes	No	Comments/Remarks
Is the Deliverable consistent to the Task(s) it refers to?			
Is there any deviation from the original plan?			
If yes, is the deviation well justified?			
Are abbreviations and terminology used consistently?			
Is the Deliverable clearly written?			
Does the Deliverable contain suitable conclusions?			
Does the Deliverable contain appropriate references?			

Are there any additional recommendations or comments? If so, please use the box below:

Format checklist:

Criterion	Item	Yes	No	Comments
Language	Are Grammar and Spelling check, ok?			

	Is the English Language used appropriately? Is the deliverable easy to understand and does it use appropriate terminology where necessary?			
Clarity	Are key vision, ideas, contributions & state of the art improvements discussed explicitly and easy to understand?			
Visuals	Are the fonts, figures, tables, screenshots and other visual elements clearly legible?			
	Are figures, tables referred to in the text?			
Glossary	Is there a complete glossary in the deliverable, detailing all acronyms used and explaining unusual technical terms?			
Nomenclature	Are any mathematical symbols and nomenclature in general clearly explained and easy to follow?			
Template Application	Is the style of the deliverable (headings, body text, Tables and captions) in accordance with the Deliverable template?			
References	Do hyperlinks and references work?			
	Does the deliverable cite other work and resources with an appropriate and consistent citation style?			
Objectives	Does the deliverable successfully address the objectives of the respective tasks it involves?			
GA Compliance	Are the results presented contributing to the project plan? Are they consistent with the Description of the Action in the Grant Agreement?			
Task Identification	Are Work Package Tasks identified clearly in the deliverable's content?			
Methodology	Are the methodology and procedures used explained well, appropriate for the scientific domain, and correct?			
Contributions	Are the deliverable's contributions to the challenges encountered clear?			
Conclusions	Do the conclusions discuss all the important issues in the document, and are they well-supported and justified by the content of the deliverable?			
Overall	Is the deliverable quality good enough so that it can be finished and submitted in time (in approx. 2 weeks)?			

APPENDIX C: Deliverables List

The WARRANT deliverables are listed in Table C-2.

Table C-2 Deliverables.

No.	Deliverable Title	WP No.	Lead Partner	Type	Dissem. Level	Due Month	Due Date Actual
D1.1	WDS and SRODS Models and Methodology for robust system integration and HAZOP analysis	1	SO	R	PU	27	Jun-27
D1.2	WDS Dependability assessment and enhancement management	1	SO	R	PU	28	Jul-27
D1.3	Intelligent Dependability Supervisor with Modular Sensing and Actuation	1	TUD	OTHER	SEN	29	Aug-27
D1.4	Consolidated Methodology enabling effective HAZOP and STPA analysis of AI- enabled ship IT/OT systems	1	DNV	R	PU	30	Sep-27
D2.1	Innovative WDS Cybersecurity Improvement Tools	2	TEC	R	PU	28	Jul-27
D2.2	Support Tools for Methodology Adoption by Industry	2	SO	R	PU	28	Jul-27
D2.3	Reference Digital Twin Dependability Management for WDS	2	KNT	OTHER	SEN	30	Sep-27
D2.4	WARRaNT Dataspace	2	INLE	OTHER	PU	33	Dec-27
D3.1	Detailed planning and coordination of LLs	3	NTUA	R	PU	6	Sep-25
D3.2	LL1 Dependable Containership Digital Systems	3	DAN	R	SEN	25	Apr-27
D3.3	LL2 Application of the WARRaNT Methodology to Smart Container Systems	3	AEL	R	SEN	25	Apr-27
D3.4	LL3 Increasing the resilience of automation systems in autonomous green vessels	3	DST	R	SEN	26	May-27
D3.5	LL4 Enhanced Dependability of Remote Operation Systems	3	SEA	R	SEN	26	May-27
D4.1	Dissemination and Communication Plan v1	4	KNT	R	PU	4	Jul-25
D4.2	Dissemination and Communication Plan v2	4	KNT	R	PU	18	Sep-26
D4.3	Dissemination and Communication Plan final version	4	KNT	R	PU	35	Feb-28
D4.4	Innovation Management and Exploitation Strategy	4	INLE	R	SEN	34	Jan-28
D4.5	Cybersecurity training	4	SD	R	PU	34	Jan-28



No.	Deliverable Title	WP No.	Lead Partner	Type	Dissem. Level	Due Month	Due Date Actual
D4.6	Adoption pathways simulation and optimization	4	VLTN	R	PU	32	Nov-27
D4.7	Capacity building – Standardization and policy recommendations	4	SO	R	PU	34	Jan-28
D5.1	Quality assurance and risk management	5	NTUA	R	SEN	6	Sep-25
D5.2	Data Management, GDPR and Ethics v1	5	INLE	R	SEN	12	Mar-26
D5.3	Data Management, GDPR and Ethics final version	5	INLE	R	SEN	36	Mar-28

APPENDIX D: Major Risks and Risk Registry

The major risks that have been initially identified along with the proposed mitigation strategies that are part of the WARRANT GA are listed in Table D-1, together with an initial risk level calculation.

Table D-1 Major Risks and initial risk registry.

#	Risk Description	WP	Probability (P)	Severity (S)	Risk Level	Mitigation Measure
1	Underperforming partner	All	1	3	Low (3)	All partners are solid and committed to the project, progress and involvement will be continuously monitored.
2	Consortium partner leaving	All	1	3	Low (3)	Management structure and consortium agreement will allow for inclusion of new partners.
3	Dependence on key personnel	All	3	3	Moderate (9)	All partners are involved with several experienced staff members and will ensure a seamless substitution.
4	Suboptimal project schedule	All	1	3	Low (3)	The project work will be monitored against project plan and corrective actions will be agreed with the EC.
5	Delayed project milestones or deliverables	All	3	3	Moderate (9)	Regular monitoring and WP meetings will ensure that these things are

#	Risk Description	WP	Probability (P)	Severity (S)	Risk Level	Mitigation Measure
						uncovered in early stages and corrective actions are implemented.
6	Low deliverable quality	All	1	5	Moderate (5)	The QRM and review process will ensure good quality.
7	Problems with necessary approvals related to physical demonstration	All	3	5	High (15)	Early communication with relevant stakeholders will be ensured through regular touchdowns and meetings.
8	Challenges in validation of KPIs	All	1	3	Low (3)	WARRANT KPIs will be integrated into all evaluation and demonstration activities.
9	Global events obstructing physical demonstration	All	1	5	Moderate (5)	The project will establish backup activities which can be initiated in case the physical demonstration cannot be performed within the project period.
10	Data availability and variety are crucial for integrated WDS datasets. Inadequate or inconsistent data can compromise model reliability in dependability assessments.	1 2	1	5	Moderate (5)	Each LL will provide data for WDS, tested with robust governance practices. If data is missing, simulations will be run with specified assumptions, and results will be given

#	Risk Description	WP	Probability (P)	Severity (S)	Risk Level	Mitigation Measure
						appropriate confidence levels.
11	The high complexity of WDS models, with multiple abstraction levels, may result in diverse generic and tailored outcomes.	1 2 3	1	5	Moderate (5)	Large-scale sensitivity analyses and simulations will refine parameters and optimize model combinations, enhancing the achievement of target outcomes. Both Methodology and WDS Modelling Framework modular.
12	Rapidly advancing technologies could render elements of the methodology obsolete or incompatible, requiring continuous updates.	1 2 3	3	3	Moderate (9)	The methodology will be adaptable to incorporate new technologies. A continuous improvement cycle via the Dataspace will provide regular updates.
13	Ensuring the methodology is scalable across different types and sizes of vessels and operations may be challenging.	1 2 3	2	4	Moderate (8)	The methodology is based on generic WDS model that covers types and automation level LLs with different vessel types ensure methodology can be adapted.
14	The risk of evolving cyber threats targeting SDSs could compromise the integrity of the methodology, particularly if	1 2 3	2	3	Moderate (6)	The methodology employs layered security architectures, regular threat assessments and updates,

#	Risk Description	WP	Probability (P)	Severity (S)	Risk Level	Mitigation Measure
	robust security measures are not continuously updated.					continuous monitoring, and incident response plans to protect against evolving threats – linked to Dataspace.
15	WDS compatibility issues and complexities in applying HAZOPS and developing dependability enhancements for diverse systems, including AI, IoT, and cybersecurity, may challenge interoperability and consistent performance.	1 2 3	1	5	Moderate (5)	Promote standardization and interoperability of WDS monitoring, use modular design for WDS, sensing, and actuation, and apply rigorous digital, HI testing, and continuous assurance for AI components. Enhanced knowledge of limitations will support progress in automation, efficiency, and sustainability optimization.
16	Data space: user adoption and privacy concerns and management challenges.	1 2 3	1	5	Moderate (5)	The Dataspace will leverage scrutiny using the methodology and DTLF, EDICT developments building trust, ensuring interoperability, implementing strong governance.
17	Development may be constrained by limited expertise, time, and resources, potentially	1 2 3 4 5	1	5	Moderate (5)	All partners have a strong track record in collaborative projects and

#	Risk Description	WP	Probability (P)	Severity (S)	Risk Level	Mitigation Measure
	compromising the methodology's comprehensiveness and effectiveness.					expertise in their tasks. Key deliverables and milestones are designed for effective resource management, prioritizing high-impact areas through a phased development approach.
18	Ensuring thorough and accurate validation of the methodology across diverse scenarios is challenging.	3	1	5	Moderate (5)	All LLs will implement a two-stage process, the first being focused [n oner subsystem or domain, and supported by partners with different expertise per use case activity.
19	The need for effective collaboration across multiple disciplines (e.g., engineering, cybersecurity, human factors) can introduce misalignment in the methodology's.	1 2 3	1	3	Low (3)	A Design Team will be set up with key experts ensuring collaboration across disciplines through regular meetings, workshops, and integrated project methodology's development management tools.
20	Difficulty in engaging key stakeholders; Alignment of Stakeholder interests with the project's objectives;	4	1	3	Low (3)	Develop a strong stakeholder engagement strategy, clearly communicate the project's value proposition, and establish

#	Risk Description	WP	Probability (P)	Severity (S)	Risk Level	Mitigation Measure
	Sustainability of the WDS Alliance.					governance mechanisms to ensure WDS Alliance sustainability and aligned interests.