OVERHEAT
INNOVATIVE STRATEGIES FOR CONTAINERSHIP FIRES PREVENTION AND MANAGEMENT

Deliverable title:	Safety and security Assessment Plan
Deliverable ID:	D 7.3
Document version:	1.0
Partner responsible:	ISaSS
Due date:	31.10.2025
Status:	final

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement Project No: 101076633. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Document Control Sheet

Deliverable number	**D 7.3**
Deliverable name	**Safety and security Assessment Plan**
Dissemination Level	**PU - Public**
Call	**HORIZON-CL5-2022-D6-01**
Topic	**HORIZON-CL5-2022-D6-01-08-Safer navigation and tackling containership fires**
Consortium Coordinator	**IMAT**
Partner responsible for the deliverable	**ISaSS**
Edition	**1.0**

Authors of the document

Authors of the document - Representatives of beneficiaries involved in the project		
Name/Beneficiary	Position/Title within the project	Date
Dominic Kudlacek	Leader of deliverable / Head of the institute	25.11.2025
Lennard John	Researcher at ISaSS	25.11.2025
Jasmin Scholz	Researcher at ISaSS	25.11.2025

Reviewers of the document

Appointed reviewers of the document - Representatives of beneficiaries involved in the project		
Name/Beneficiary	Position/Title within the project	Date
Dominic Kudlacek	Leader of deliverable / Head of the institute	25.11.2025
Lennard John	Researcher at ISaSS	25.11.2025
Jasmin Scholz	Researcher at ISaSS	25.11.2025
Francesco Russo / TopView S.r.l.	TopView PoC	29.10.2025
Vittorio Sangermano / ISSNOVA	ISSNOVA PoC	25.11.2025
Marco Pasciuto / IMAT	IMAT Project Manager	27/11/2025
Valentina Lasco / IMAT	IMAT Researcher	27/11/2025
Modestino Manfredi / IMAT	IMAT Master	27/11/2025

Responsible for the document approval

List of people approving the document - Representatives of beneficiaries involved in the project		
Name/Beneficiary	Position/Title within the project	Date
Dominic Kudlacek / ISaSS	ISaSS PoC	25.11.2025
Marco Pasciuto / IMAT	OVERHEAT Project Manager	25.11.2025
Vittorio Sangermano / ISSNOVA	ISSNOVA PoC	25.11.2025
Bartosz Dziugiel / ILOT	ILOT PoC	25.11.2025
Holger Kramer / ISL	ISL PoC	25.11.2025
Fabienne Vallee / Port of Brest	Port of Brest PoC	25.11.2025
Rafael Company / VPF	VPF PoC	25.11.2025
Stefano Ricci / DITS srl	DITS PoC	25.11.2025

Théo Delferriere / CIRCOE	CIRCOE PoC and Leader of WP 7	25.11.2025
Pedro Merino-Laso / ENSM	ENSM PoC	25.11.2025
List of people approving the document - Representatives of beneficiaries involved in the project		
Name/Beneficiary	Position/Title within the project	Date
Nicola Pacini / GTS	GTS PoC	25.11.2025
Gunnar Tietze / SeaTopic	SeaTopic PoC	25.11.2025
Massimo Capozza / PeopleTrust	PeopleTrust PoC	25.11.2025
Francesco Russo / TopView	TopView PoC	25.11.2025
José Miguel Basset Blesa / VFF	VFF PoC	25.11.2025
Simone Panfiglio / Caronte	Caronte PoC	25.11.2025

ABSTRACT

Deliverable 7.3, *Safety and security Assessment Plan*, defines the methodological framework for identifying, analysing and mitigating risks associated with the demonstration and simulation activities of the OVERHEAT project.

The assessment approach follows the principles of ISO 31000:2018 Risk Management, the ALARP concept (As Low as Reasonably Practicable) and the methodologies defined in Work Package 3 *Knowledge base Navigation safety occurrence design and classification*, providing a structured and replicable procedure for evaluating both technical and operational risks.

The framework distinguishes between system-specific and cross-cutting hazards and applies a 5 × 5 qualitative risk matrix to ensure consistency and comparability across technologies and partners.

To demonstrate its application, the methodology is implemented for two representative systems developed within OVERHEAT: the Bosch BME688 sensor system, used for gas and temperature monitoring and the OVERHEAT Autonomous Drone system, enabling autonomous aerial surveillance of containership decks. For each system, risks are identified, assessed and treated through preventive design measures, operational controls and procedural safeguards.

As the demonstration and simulation campaigns have not yet been carried out, the assessments presented in this deliverable are preliminary and based primarily on technical documentation, laboratory testing and design analysis.

By combining a robust methodological framework with practical implementation, D 7.3 establishes a transparent and adaptable foundation for ensuring safe, reliable and secure deployment of innovative technologies within maritime fire prevention and response.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

AI	Artificial Intelligence
ALARP	As Low as Reasonably Practicable
BSEC	Bosch Software Environmental Cluster
ESD	Electrostatic Discharge
GDPR	General Data Protection Regulation
GNSS	Global Navigational Satellite System
GPS	Global Positioning System
IMU	Inertial Measurement Unit
IoT	Internet of Things
MFA	Multi-Factor Authentication
NOTAM	NOTice to Air Man
PIC	Pilot In Command
RTH	Return-to-Home
RTK	Real-Time Kinematic
SOLAS	Safety Of Life At Sea
UAV	Unmanned Aerial Vehicle
UPS	Uninterruptible Power System
VOC	Volatile Organic Compound
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WP	Work Package

1. INTRODUCTION

Maritime transport plays a vital role in global trade, with containerships forming the backbone of international logistics. However, cargo fires remain one of the most severe and persistent safety challenges in this sector. Despite technological advances in ship design and operation, the risk of fire incidents on containerships, particularly above the weather deck, continues to pose a significant threat to human life, vessel integrity, cargo and the marine environment.
Current international regulations, such as the International Convention for the Safety of Life at Sea (SOLAS Chapter II-2, Regulation 7), require fixed fire detection and alarm systems in machinery spaces and accommodation areas. As a result, there are still no mandatory requirements for fixed fire detection above the weather deck of containerships. In practice, this means that fire detection in cargo areas relies primarily on visual observation by the crew, a method limited by restricted visibility from the bridge, adverse weather conditions, container stacking arrangements and operational factors such as fatigue or routine work patterns. Consequently, situational awareness is reduced and the early identification of hazardous events becomes highly dependent on human observation and judgment.

In response to these limitations, OVERHEAT integrates emerging technologies to enhance safety and resilience at sea. Among the most promising innovations are autonomous drones for aerial surveillance and intelligent IoT-based sensors capable of detecting smoke, heat and volatile compounds. Together, these systems form a multi-layered detection and monitoring network that supports predictive risk analysis and enables a faster, data-driven response to potential fire events.

Work Package 7 *Simulation and demonstration activities*, led by CIRCOE, focuses on validating the technical and operational feasibility of the developed solutions in simulated and real-world environments. Within this framework, Deliverable 7.3 *Safety and security Assessment Plan* establishes the Safety and Security Assessment Plan used to evaluate all related risks. It defines a unified methodological framework based on ISO 31000:2018, the ALARP principle and the methodologies defined in Work Package 3 *Knowledge base Navigation safety occurrence design and classification*, ensuring consistent identification, analysis and mitigation of technical, operational and cyber-related hazards across the project.

By applying this methodological framework to the Bosch BME688 sensor system and the OVERHEAT Autonomous Drone system, the deliverable provides a preliminary yet comprehensive assessment of system-specific hazards, supported by risk matrices, mitigation measures and preventive checklists. These results contribute directly to the project's overarching objective of strengthening preventive measures, improving situational awareness and fostering a robust safety culture across the maritime sector.

2. METHODOLOGICAL FRAMEWORK FOR SAFETY AND SECURITY ASSESSMENT

The Safety and Security Assessment Plan developed under WP 7 establishes the methodological foundation for analysing and managing risks within the OVERHEAT project. It defines a unified approach for identifying, evaluating and mitigating hazards associated with the technical systems and demonstration activities carried out in the project. This framework ensures that all partners apply consistent criteria for assessing safety and security aspects, regardless of their technological or operational context.

2.1 Methodology

The safety and security assessment in OVERHEAT follows a structured process aligned with the principles of ISO 31000:2018 Risk Management.

According to this standard, effective risk management involves four key steps (ISO 31000:2018):

1. Risk identification

Detection of potential hazards or unsafe conditions that could affect system performance or operational safety

2. Risk analysis

Examination of the identified risks to determine their causes, possible consequences and influencing factors

3. Risk evaluation

Qualitative assessment of each risk with regard to its likelihood of occurrence and its potential impact on safety, reliability or data integrity

4. Risk treatment (mitigation)

Implementation of preventive and corrective measures to reduce the risks to an acceptable level.

This process is applied throughout the project to ensure that all safety and security aspects are analysed consistently. The risk treatment phase is implemented through the preventive checklists and mitigation measures developed for each technological system, which serve as practical tools for maintaining safe operation during the OVERHEAT demonstrations.

The framework distinguishes between two analytical dimensions:

- Technical risks, relating to the integrity, configuration and performance of system components
- Operational risks, arising from environmental influences, human factors or procedural deviations

2.1.1 Likelihood and consequence scales

Each risk category within the framework is assessed using the same 5 × 5 qualitative matrix, ensuring comparability across systems and consistency in evaluation. A qualitative risk matrix is a standard mechanism in safety and security management for visualising risk levels and supporting acceptance decisions. Each cell in the matrix represents a specific combination of likelihood and consequence. (Olsen 2024)

The 5×5 risk matrix used in this deliverable follows the scales defined in WP 3. These scales ensure a consistent evaluation of all risks identified during the demonstrations. Each risk is assessed based on its likelihood of occurrence and the severity of its potential consequences. (C. S. Carlson 2014; M. Glossop et al. 2000)

Likelihood scale (1-5)

The likelihood scale describes the estimated frequency of the hazard. It is based on qualitative categories used in WP 3 and adapted to the operational context of the OVERHEAT demonstrations.

Table 1: Likelihood scale

Level	Descriptor	Definition
1 – Extremely improbable	Very unlikely event	Occurs only under exceptional or unforeseen conditions
2 – Improbable	Unlikely event	Could occur, but not expected during normal operation
3 – Remote	Possible event	Might occur under specific conditions or during prolonged operation
4 – Occasional	Regularly possible event	Could occur several times during the demonstration campaign
5 – Frequent	Likely event	Expected to occur repeatedly and under normal conditions

Consequence scale (A-E)

The consequence scale assesses the severity of harm to system integrity, operational performance or safety. The definitions follow the WP3 classification model derived from maritime risk analysis.

Table 2: Consequence scale

Level	Descriptor	Definition
A - Catastrophic	Critical impact	Complete system loss, fire escalation or risk of fatality
B - Hazardous	High impact	Severe system failure, major damage or risk of serious injury
C - Major	Significant impact	System malfunction, operational disruption or risk of minor injury
D – Minor	Low impact	Temporary degradation of performance, no safety effect
E - Negligible	No significant impact	Minor deviation, no harm, system recovers immediately

Each combination of likelihood and consequence results in a risk level. Each level determines the type and urgency of the recommended action.

Intolerable risks require immediate measures. Activities must be stopped or modified until the risk is reduced. Priority mitigation is necessary to ensure that additional or enhanced preventive controls are implemented to lower the risk to a tolerable level.

Tolerable risks may remain in place under controlled conditions. They can be accepted temporarily, but safety measures must be applied. Additional mitigation may be required based on management decisions and operational judgement.

Acceptable risks are considered sufficiently low. No further mitigation is required, and the activity can proceed without additional controls.

This classification follows the ALARP principle described in Chapter 2.

Two primary risk categories form the structural backbone of the framework. Technical risks include failures in hardware, software, communication, or data acquisition, whereas operational risks arise from incorrect procedures, environmental exceedance, or insufficient training.

These categories are inherently interdependent: a technical malfunction can trigger operational issues (for example, a loss of positioning leading to manual intervention), while weak data integrity can compromise coordination across systems. Recognising and managing these interdependencies is essential to prevent cascading effects and to ensure that mitigation strategies address the complete chain of potential consequences. The framework therefore adopts a system-of-systems approach, treating all technologies within OVERHEAT as interlinked elements of a shared operational environment.

Monitoring is an integral component, ensuring that risk management remains adaptive throughout the project lifecycle. During all demonstration and simulation activities, technical and operational data are collected, analysed and used to refine the risk profiles. Each partner is responsible for recording anomalies, incidents and near-miss events in a standardised format, ensuring traceability and comparability of risk information.
In line with the recommendations of Olsen (2024), the structure of the safety and security assessment plan follows an iterative and team-based approach to risk analysis. This process includes the identification of hazards, qualitative evaluation of likelihood and consequence and the documentation of mitigation measures through a structured review involving technical experts and operational stakeholders. Such an approach ensures that the risk assessment remains evidence-based, collaborative and continuously updated throughout the project execution.

2.2 Structure of the risk assessment plan

The structure of the Safety and Security Assessment Plan follows a systematic and collaborative process that ensures both methodological rigour and practical applicability in maritime and autonomous system contexts.

A robust risk assessment plan consists of several essential elements (Olsen 2024):

- Definition of objectives and scope

Clearly specify the systems, operations and environments to which the assessment applies, including assumptions and boundaries

- Identification of hazards

Gather input from technical documentation, operational experience and expert knowledge to identify potential failure modes or unsafe conditions

- Qualitative evaluation

Assess each hazard in terms of its likelihood and consequence using the agreed-upon 5 × 5 matrix and corresponding ALARP criteria

- Documentation of results

Record all risks, their ratings and proposed mitigation measures in a centralised and traceable format, such as a risk register

- Review and validation

Conduct structured team reviews involving a Risk Leader, Subject Matter Experts and a Recorder to ensure accuracy, consensus and completeness

- Mitigation and follow-up

Translate the evaluation results into actionable measures and monitoring plans, assigning responsibilities for implementation and verification
The process should be updated whenever new information becomes available, or system conditions change and proportional to the complexity of the system under assessment. By following this structured approach, the Safety and Security Assessment Plan ensures transparency, traceability and continuous improvement in the management of risks associated with demonstration and simulation activities. (Olsen 2024)

2.3 Application within OVERHEAT demonstrations

The methodological framework provides a common reference for all partners participating in the simulation and demonstration activities of the OVERHEAT project.
Before each test campaign, a pre-operational risk review is carried out to identify potential hazards, define control measures and assign responsibilities. During operation, real-time risk monitoring supports informed decision-making and enables immediate corrective actions when deviations from the expected conditions occur. After each demonstration, a post-operational evaluation is conducted to assess performance, verify the effectiveness of mitigation measures and update the associated risk documentation.
Through this process, the framework establishes a continuous safety management cycle that connects planning, execution and evaluation in a single, iterative structure. It ensures that risks are not only identified and assessed at the beginning of the project but are also actively managed, reviewed and refined throughout its implementation.
In this deliverable, the framework is applied to two representative technologies used within OVERHEAT: the Bosch BME688 sensor system and the OVERHEAT Autonomous Drone system.
For both systems, the same methodological sequence is applied to assess their safety, reliability and operational integrity. This ensures a consistent and comparable evaluation across technologies while maintaining the flexibility required to address their specific operational contexts.
However, both assessments are preliminary in nature as the simulation and demonstration activities have not yet been conducted. The analysis presented here is based primarily on technical documentation, design specifications and laboratory testing. Consequently, practical experience and empirical validation from real-world operation are not yet available.

2.4 Methodology for identifying and managing emerging risks

Emerging risks are hazards that were not identified during the initial assessment or that change significantly due to new operational, technical or environmental conditions. Demonstration activities involve dynamic environments, therefore a structured process for identifying and managing these risks is necessary. This section defines the standard procedure for detecting, analysing and controlling emerging risks. The procedure follows methodological foundations developed in WP3 (C. S. Carlson 2014; M. Glossop et al. 2000).

The procedure ensures that new hazards arising during the demonstrations are identified in a timely manner and evaluated with consistent criteria. It supports adaptive risk management and complements the initial risk assessment conducted for each system. All partners apply the same method to ensure traceability, comparability and reproducibility of results.

2.4.1 Trigger conditions for emerging risk identification

An emerging risk assessment is initiated when one or more of the following conditions occur:

- deviations from expected operational behaviour of the IoT sensors or the UAS,
- anomalies in communication links, positioning data, battery performance or sensor output,
- unexpected interactions between systems, crew activities or environmental factors,
- unsafe situations, near misses or interruptions reported during demonstrations,
- changes in weather, visibility, electromagnetic interference or deck layout,
- introduction of new operational tasks or modification of demonstration procedures.

These triggers reflect the hazard identification principles defined in WP 3, including technical failures, human factors and external influences.

2.4.2 Standardised identification process

1. Step: Observation and reporting

   Operators, crew members and researchers document deviations or unsafe conditions in a hazard log. Each entry includes a short description, time, system involved and immediate observable consequences.

2. Step: Preliminary classification

   The reported event is screened against the hazard taxonomy developed in WP3. This taxonomy covers technical malfunctions, dangerous goods behaviour, human error, mechanical failures and external factors. If the hazard does not fit into an existing category, a new category is created.

3. Step: Methodological assessment

The event is analysed using one or more of the hazard identification and risk analysis methods defined in WP 3 and in accordance with the Formal Safety Assessment (FSA) Guidelines as over-arching reference for maritime risk evaluation:

- Failure Mode and Effects Analysis (FMEA) for technical component issues
- Fault Tree Analysis (FTA) for causal chain examination
- Event Tree Analysis (ETA) for scenario development
- HAZOP or What-If Analysis for operational deviations

The selection of the method depends on the nature of the hazard.

4. Step: Documentation and integration

All analysis results are documented in the hazard log. The responsible partner adds the hazard to the main risk register if it is confirmed to be relevant. The entry includes an initial risk rating, proposed mitigation actions and responsibilities.

Each emerging risk is evaluated using the 5×5 matrix introduced in Chapter 2. The likelihood and consequence levels follow the definitions developed under WP 3 (C. S. Carlson 2014; M. Glossop et al. 2000). These definitions include five qualitative likelihood levels and five consequence categories that range from negligible to catastrophic impact. Using these scales ensures comparability between initial and emerging risks.
Confirmed emerging risks are treated with preventive or corrective measures. Actions may include configuration updates, procedural changes, environmental adjustments or enhanced supervision. Each action is evaluated for effectiveness during subsequent demonstrations. The risk register is updated accordingly.
At the end of each demonstration, all emerging risks and their mitigation measures are reviewed. Lessons learned are integrated into the next operational cycle. This process ensures that the risk assessment remains dynamic and reflects real-world performance of the technologies.

3 SAFETY AND SECURITY ASSESSMENT OF THE BOSCH BME688 SENSOR SYSTEM

This chapter presents the safety and security assessment of the Bosch BME688 sensor system by following the methodological framework defined in Chapter 2 and applies it to a specific technological case study. It evaluates the system's technical characteristics, built-in safety mechanisms, data protection features and operational handling requirements under conditions relevant to maritime environments.
Section 3.1 provides a technical description and functional overview of the BME688 sensor. Section 3.2 examines the system safety aspects, describing the hardware- and software-based design features. Section 3.3 discusses the operational safety requirements. Together, these sections provide a comprehensive assessment of the Bosch BME688 sensor system and establish a structured basis for its safe integration into the project's technical and operational environment.

3.1 Technical description and functional overview of the Bosch BME688 Sensor System

The Bosch BME688 sensor represents the technological foundation of the gas detection component developed within the OVERHEAT project. The BME688 is a compact environmental sensor that combines the measurement of gas concentration, temperature, humidity and barometric pressure in a single device. The integration of these four parameters allows a multidimensional evaluation of ambient conditions and supports the detection of volatile compounds that may indicate overheating, smoke formation or cargo emissions.
The sensor detects gases by measuring changes in electrical resistance on a micro-heated metal-oxide layer. This element operates in cyclical heating phases, referred to as heater profiles, which activate different chemical reactions on the surface depending on temperature. The BME688 thus produces unique electrical signatures for specific gas mixtures and volatile compounds. The duty cycle controls the alternation between measurement and resting periods, balancing sensitivity, response time and energy consumption.
By integrating multiple sensing elements with artificial intelligence, the BME688 enables advanced assessment of the atmospheric state within cargo areas. It can identify characteristic chemical signatures associated with the early stages of fire development or hazardous gas release. Its ability to detect volatile organic compounds (VOCs), sulphur compounds, hydrogen and carbon monoxide in the parts-per-billion range adds a critical layer of preventive monitoring to maritime safety applications.
Sensor control and data management are handled through the Bosch Software Environmental Cluster (BSEC) and the Bosch AI-Studio platform. The BSEC software manages data acquisition, drift compensation and humidity correction, while AI-Studio provides tools for data labelling, algorithm training and export of validated detection models.
Each measurement session generates structured datasets containing timestamps, sensor identifiers, heater settings and calibration metadata. This format ensures full traceability and

reproducibility of all recorded data. Error codes are automatically generated if communication faults or invalid configurations occur, enabling prompt fault detection.
The availability of multiple operational modes and adaptive software control allows the BME688 to be deployed across a wide range of use cases. Its low energy consumption, small size and environmental resilience make it particularly suitable for applications that require mobility and long-term reliability.
The Bosch BME688 Development Kit complements the sensor by providing an experimental environment for configuration, calibration and validation. This configuration enables the simultaneous testing of multiple sensor settings, which improves statistical accuracy and reduces development time. The development kit operates under the same AI-Studio software used for algorithm training, ensuring methodological consistency between laboratory testing and field deployment. It supports redundancy checks, error analysis and performance verification under controlled conditions, forming the basis for calibration procedures and reliability assessments. (Bosch Sensortec GmbH 2022a, 2021, 2024)

3.2 System safety of the Bosch BME688 Sensor System

The system safety of the Bosch BME688 sensor is determined by its design characteristics, operational limits and built-in protective mechanisms. As an electronic micro-sensor operating at elevated temperatures and within variable environmental conditions, its safety performance depends on thermal control, material stability, power management and the reliability of both hardware and software components.
The BME688 incorporates several design elements that ensure operational safety under normal and extended conditions. The sensing element is mounted on a micro-hotplate that operates at controlled temperatures defined by user-selected heater profiles. Bosch defines strict limits for heater temperature and duration to prevent thermal stress and material degradation. If these parameters are followed, the component remains stable over its lifetime without exceeding safe thermal thresholds. Excessive or continuous high-temperature operation, however, can lead to local overheating, reduced sensitivity and accelerated sensor aging. Proper duty-cycle configuration and periodic validation of the heating profile are therefore essential safety measures.
The sensor’s electronics operate at a low supply voltage. This low-voltage design minimizes the risk of electrical overload and supports safe integration into larger electronic systems. Internal current regulation and signal conditioning protect against short-term voltage fluctuations, while external circuit design must include appropriate filtering and grounding to avoid electromagnetic interference.
Newly installed sensors require an initial stabilisation period of approximately 24 hours before valid measurements can be obtained to reduce the likelihood of false readings. During regular operation, recalibration should be performed at defined intervals to compensate for long-term drift and to maintain accuracy.

The sensor's firmware and configuration software include diagnostic and fault-detection routines that contribute to operational safety. Error codes are automatically generated when communication interruptions, invalid configurations or sensor malfunctions occur. These codes support early identification of potential failures and allow corrective action before data integrity or system stability is compromised. Regular monitoring of diagnostic outputs is therefore part of the preventive safety concept. (Bosch Sensortec GmbH 2024, 2022a)

3.2.1 Security and data protection of the Bosch BME688 Sensor System

The Bosch BME688 sensor system requires measures that ensure the security and integrity of its digital processes. Since the sensor's functionality depends on software-controlled data acquisition, configuration files and algorithmic processing, the protection of these elements is an essential part of system safety.

The BME688 relies on the Bosch Software Environmental Cluster and the AI-Studio software for configuration, calibration and data management. These applications define how raw sensor data are processed, compensated and translated into usable outputs. To maintain integrity, access to configuration interfaces and algorithmic models must be restricted to authorised personnel. Changes to configuration files or firmware must be documented and validated before deployment to avoid operational errors or performance degradation.

All communication between the sensor, development kit and connected devices should be conducted through secure channels. To protect stored data, all measurement files and configuration datasets should be kept in controlled environments with restricted access. Backups must be maintained to prevent data loss in case of hardware or communication failures.

Ensuring cybersecurity for the BME688 system directly contributes to its operational safety. Compromised configuration files, corrupted firmware or unauthorised access to sensor data could result in incorrect readings or false alarms. For this reason, digital protection mechanisms, regular verification of firmware integrity and secure access control form an integral part of the system's overall safety design. (Bosch Sensortec GmbH 2021, 2022b)

3.3 Operational Safety of the Bosch BME688 Sensor System

The operational safety of the Bosch BME688 sensor system depends on correct handling, appropriate environmental management and the consistent application of maintenance and calibration procedures. While the sensor is designed for reliable use under a broad range of operating conditions, safe and accurate performance requires adherence to defined procedures for installation, operation and data management.

The environmental control is a critical factor for operational safety. The BME688 is designed to function between − 40 °C and + 85 °C, at relative humidity levels from 0 to 100 % and within a pressure range of 300 to 1100 hPa. These parameters cover most maritime and industrial conditions; however, exposure to condensation, dust or corrosive gases can impair performance. Protective enclosures or sensor housings should therefore be used in humid or salt-laden environments.

Furthermore, operators must ensure that the chosen operational mode complies with manufacturer recommendations and that power supply parameters remain within the safe range. To

mitigate these risks, staff responsible for configuration and operation should receive dedicated training in sensor control and parameter management.
Electrostatic discharge (ESD) protection is another aspect of safe handling. Personnel should work within ESD-protected areas and use grounded tools when handling components, particularly in metallic or conductive environments.
During field operations, the monitoring of diagnostic information provided by the sensor firmware is essential. The BME688 automatically generates error codes in cases of communication failures, invalid configurations or signal loss.
In maritime applications, operational safety further relies on the integration of the sensor into broader system-level safeguards. The BME688 functions as an auxiliary detection device and should be deployed as part of a redundant monitoring network that includes visual and thermal inspection tools. This layered approach ensures that potential failures or false readings from individual sensors do not compromise the overall safety of the system. (Bosch Sensortec GmbH 2024, 2022a)

4 RISK ASSESSMENT FOR THE BOSCH BME688 SENSOR SYSTEM

The aim of the risk assessment is to systematically identify, evaluate and classify potential hazards that could affect the safety, reliability or data integrity of the system during its use within the OVERHEAT project.
Risks are following the 5×5 matrix methodology described in Chapter 2. The method focuses on risks that may arise during the integration of the BME688 sensor in maritime environments, particularly when mounted on containers or deployed as part of drone-based monitoring systems. The analysis considers environmental, technical and cyber-related hazards, along with human and operational factors that influence safe performance.

4.1 Risk identification and evaluation for the Bosch BME688 Sensor System

The identification and evaluation of risks were based on information provided in the Bosch Sensortec documentation, testing results from the development kit and technical analyses conducted within the OVERHEAT project.
Potential hazards were identified through a comprehensive review of the sensor's technical specifications, operational procedures and expected environmental conditions during deployment.
The most important risks identified were then qualitatively assessed using two parameters: the probability of occurrence and the potential impact on system functionality, data reliability, or operational safety
The identified risks for the Bosch BME688 sensor system are summarised in Table 3. They represent the main technical and operational hazards that may occur during installation, use and maintenance of the sensor in maritime and experimental environments. Each risk was assessed qualitatively with respect to its likelihood of occurrence and potential effect on system functionality, data reliability and operational safety.
The evaluation Table 4 shows that most risks of the Bosch BME688 sensor system fall within the tolerable range. These risks include sensor overheating (R1), material degradation (R2), environmental vibration or corrosion (R3), measurement errors caused by condensation or salt exposure (R4), electrical instability (R5) and unauthorised modification of configuration or firmware (R6). Although these hazards may influence sensor performance or operational stability, their likelihood and consequences remain limited and they can be controlled with appropriate preventive measures.
The only risk classified as intolerable is the occurrence of false alarms resulting from software behaviour or signal misinterpretation (R7). This hazard is critical because it can lead to systematic alarm fatigue, reduce trust in sensor output and compromise the early detection of fire-related events. For this reason, R7 requires specific attention and targeted mitigation to ensure data reliability and safe operation.

Table 3: Summary of identified risks of the Bosch BME688 Sensor System

Risk ID	Risk description	Potential consequences	Likelihood (1–5)	Consequence (A-E)	Risk level
R1	Sensor overheating	Fire of sensor	2	B	Tolerable
R2	Material degradation/ Material fatigue	False alarms	3	D	Tolerable
R3	Environmental vibration or corrosion	Loss of sensor	4	E	Tolerable
R4	Measurement errors due to condensation, dust or salt exposure	False alarms	4	E	Tolerable
R5	Electrical instability or power failure	False alarms	3	D	Tolerable
R6	Unauthorised modification	No alarms	2	A	Tolerable
R7	False alarms	Ignoring the alarms	3	A	Intolerable

4.1.1 Risks of the Bosch BME688 Sensor System

The likelihood and consequence values assigned to the risks of the Bosch BME688 sensor system are based on technical specifications and the operational context of the OVERHEAT demonstrations. Direct expert input from Bosch personnel or operational experienced personnel was not available during the assessment; therefore, the evaluation reflects a conservative and documentation-based analysis.

R1 Sensor overheating

The likelihood is rated as 2 because the heater profiles and duty cycles are strictly defined by Bosch and remain stable under normal operation. Deviations occur rarely and usually only when operating conditions fall outside recommended ranges. The consequence is B because overheating may damage the sensing element or reduce sensor lifetime, but such failures do not result in hazardous system-level effects.

R2 Material degradation or material fatigue

The likelihood is moderate (3) due to long-term exposure to humidity, salt and mechanical stress in maritime environments. Small changes in sensor response may develop over time. The consequence is D because degradation can lead to reduced sensitivity or increased drift, but it does not compromise overall system safety.

R3 Environmental vibration or corrosion

Likelihood is 4 because vibration, salt deposits and exposure to exhaust gases are common on containership decks and can affect small electronic components. The consequence is E because severe corrosion can cause sensor failure or loss of function, resulting in unreliable measurements.

R4 Measurement errors due to condensation, dust or salt exposure

The likelihood is 4 due to the sensor's sensitivity to moisture and airborne particulates. These conditions are typical in maritime environments and may temporarily affect readings. The consequence is E because such errors can create false alarms or mask relevant gas signatures, reducing detection reliability.

R5 Electrical instability or power failure

The likelihood is 3 because power fluctuations, grounding issues or cable corrosion can occur in field deployments. The consequence is D because temporary power loss results in missing data or sporadic false alarms but does not damage the device.

R6 Unauthorised modification

The likelihood is low (2) because system access is restricted and configuration files are stored locally under controlled conditions. However, the risk cannot be completely excluded in multi-partner environments. The consequence is A because incorrect configuration or unauthorised firmware changes can disable the detection function entirely and compromise system integrity.

R7 False alarms caused by software behaviour or signal misinterpretation

The likelihood is moderate (3) because algorithmic sensitivities, environmental interference and incomplete calibration profiles can lead to misclassification of gas signatures. The consequence is A because repeated false alarms may lead operators to disregard critical warnings, undermining the sensor's role in fire detection.

4.2 Risk assessment matrix for the Bosch BME688 Sensor System

To visualise the overall risk distribution, the identified and evaluated hazards were transferred into a 5×5 qualitative matrix, Table 4, that combines likelihood and consequences scores.
This matrix provides a transparent overview of how each risk contributes to the overall safety profile of the Bosch BME688 sensor system and supports the prioritisation of mitigation actions.
Each identified hazard is classified into one of three categories: Intolerable, tolerable and acceptable. These categories reflect the level of risk acceptance and the required mitigation actions.

Intolerable:

Risks in this category are considered unacceptable as they represent a high probability of major consequences, such as complete system failure, severe data loss, or critical safety impacts.
Immediate management attention and corrective action are required to reduce the risk to tolerable levels. These risks must be addressed through design modifications, access control, or redundant safety mechanisms to ensure safe operation.

Tolerable:
Risks in this category are tolerable under controlled conditions but can still lead to degraded performance, intermittent data loss, or reduced operational reliability. They require regular monitoring, preventive maintenance and adherence to operational limits. Management actions may be scheduled rather than immediate, but these risks must be tracked to avoid escalation over time.

Acceptable:
These risks are minimal and acceptable, with limited or negligible impact on system integrity, performance, or data accuracy. These risks are unlikely to occur under normal operating conditions and typically require no special management actions beyond standard good practices and periodic verification.

Table 4: Risk Assessment Matrix for the Bosch BME688 Sensor System

Likelihood	Risk Assessment Matrix					
	5 Frequent	Intolerable	Intolerable	Intolerable	Tolerable	Tolerable
	4 Occasional	Intolerable	Intolerable	Tolerable	Tolerable	Tolerable **R3, R4**
	3 Remote	Intolerable **R7**	Tolerable	Tolerable	Tolerable **R2, R5**	Acceptable
	2 Improbable	Tolerable **R6**	Tolerable **R1**	Tolerable	Acceptable	Acceptable
	1 Extremely improbable	Tolerable	Acceptable	Acceptable	Acceptable	Acceptable
		A Cata-strophic	**B** Hazardous	**C** Hazardous	**D** Minor	**E** Negligible
		Consequence				

5 RISK MITIGATION AND PREVENTIVE CHECKLIST FOR THE BOSCH BME688 SENSOR SYSTEM

The risk mitigation strategy for the Bosch BME688 sensor system is designed to ensure that all identified hazards are either eliminated or reduced to an acceptable level in line with the ALARP principle (As Low as Reasonably Practicable).
According to this principle, a risk is considered tolerable when it has been reduced to the lowest level that can reasonably be achieved, meaning that no further mitigation is required unless additional measures would provide a clear safety benefit in proportion to their cost or effort. The ALARP concept recognises that absolute safety cannot be achieved. Instead, resources for risk reduction must be applied where they deliver a meaningful improvement in safety outcomes. It provides a structured balance between the effort, cost and benefit of implementing further controls, provided that safety is not compromised. (Olsen 2024)

In practice, the model, Figure 1, distinguishes between three levels of residual risk (Olsen 2024):

- Intolerable risks, which are unacceptable under any circumstances and must be mitigated before operation can proceed
- ALARP-region risks, which are tolerable only when further reduction is impracticable or disproportionate to the improvement gained
- Broadly acceptable risks, which are so low that no additional measures are required, although improvements may still be implemented when feasible

Within the OVERHEAT project, this principle serves as the foundation for assessing and managing the risks associated with the Bosch BME688 sensor and the OVERHEAT Autonomous Drone system. The goal is to achieve a controlled and verifiable safety level by systematically applying preventive design measures, operational controls and procedural safeguards.
Since the BME688 is a low-voltage, non-critical component, risk mitigation primarily focuses on ensuring technical robustness, environmental protection and data reliability rather than on life-critical safety interventions. The identified risks are therefore addressed through targeted measures related to thermal stability, electrical integrity, environmental resistance and software configuration management.

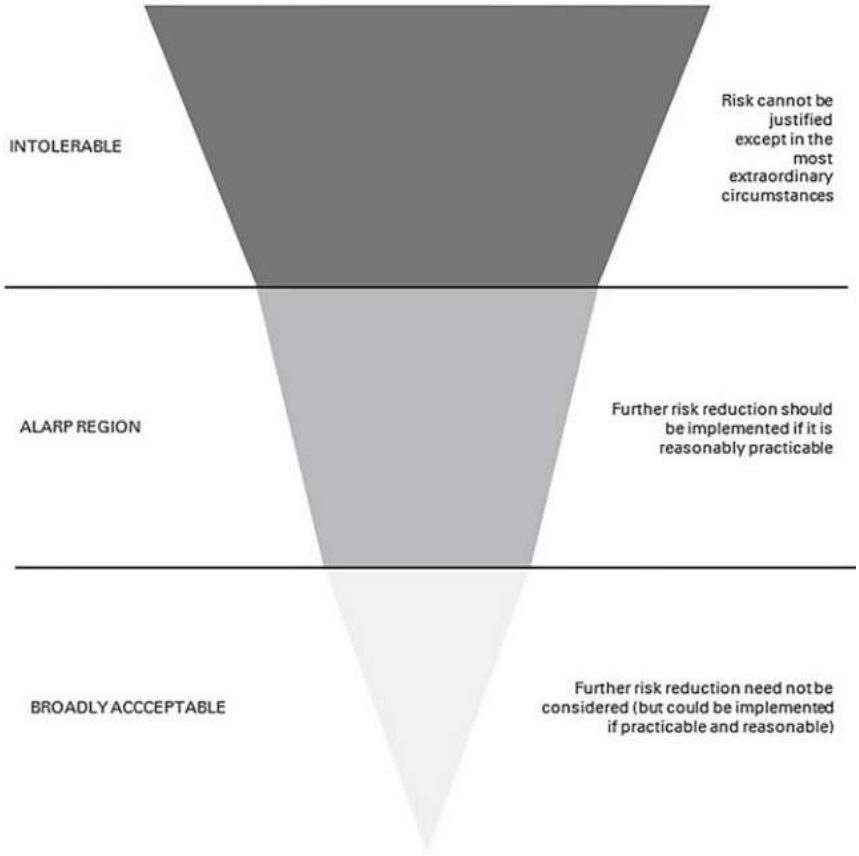

Figure 1: ALARP diagram (Olsen 2024 Fig. 28.5 p. 446)

5.1 Mitigation measures for the Bosch BME688 Sensor System

The Table 5 summarises the mitigation measures defined for the Bosch BME688 sensor system. These measures address the specific risks identified in Table 3 and ensure that all hazards are reduced to an acceptable level in line with the ALARP principle.

Table 5: Mitigation measures for the Bosch BME688 Sensor System

Risk ID	Risk description	Mitigation measure
R1	Sensor overheating	Ensure all heater profiles and duty cycles comply with Bosch specifications. Continuously monitor temperature and current during operation. Maintain stable voltage supply and galvanically isolated power lines to prevent short circuits or fluctuations.
R2	Material degradation / material fatigue	Inspect sensors regularly for corrosion or physical damage. Use corrosion-resistant mounting materials and vibration-damping elements. Recalibrate or replace degraded sensors to maintain performance.
R3	Environmental vibration or corrosion	Mount sensors in weatherproof housings to prevent exposure to salt spray, exhaust gases, or mechanical shock. Verify proper air circulation and check for condensation or corrosion.
R4	Measurement errors due to condensation, dust, or salt exposure	Avoid installation near contamination sources. Use sealed housings with appropriate IP protection. Clean sensor surfaces and recalibrate when drift or false readings occur.
R5	Electrical instability or power failure	Maintain a stable, grounded power supply with surge protection. Implement galvanic isolation and proper filtering in external circuits. Verify grounding for sensors on conductive surfaces.
R6	Unauthorised modification	Restrict configuration access to authorised personnel only. Use version-controlled repositories for all firmware and AI-Studio models. Validate updates through checksum and digital signature verification.
R7	False alarms	Ensure configuration models are validated and consistent with sensor calibration data. Maintain backup of configuration and measurement files. Regularly verify firmware integrity and retrain models as needed.

5.2 Example of a checklist for preventing risks during field use of the Bosch BME688 Sensor System

The following example of a checklist, Table 6, summarises essential control points for the safe and reliable use of the BME688 in maritime and experimental environments.

Table 6: Example Checklist for the Bosch BME688 Sensor System

Control Area	Verification Method	Frequency	Done	Remarks
Heater configuration	Laboratory validation prior to installation			
Power supply	Continuous monitoring; inspection			
Environmental protection	Visual inspection			
Maintenance	Replace damaged units			
Software updates	Documented version control and digital signature check			
ESD protection	At every installation or maintenance activity			
User	Training and familiarization			

6 SAFETY AND SECURITY ASSESSMENT OF THE OVERHEAT AUTONOMOUS DRONE SYSTEM

Within the OVERHEAT project, the OVERHEAT Autonomous Drone is deployed to assess the potential of autonomous aerial surveillance for the early detection of fire-related incidents and temperature anomalies on containership decks. The system enables continuous situational awareness by performing fully autonomous take-off, flight, landing and recharging operations, thereby extending the monitoring capabilities of the vessel's crew.

In the context of WP 7, the OVERHEAT Autonomous Drone supports the validation of innovative digital tools for safety monitoring and operational risk management. Its evaluation within this deliverable follows the same methodological procedure applied to the Bosch BME688 sensor system, in accordance with the principles of ISO 31000 Risk Management and the ALARP concept.

The assessment therefore includes the systematic identification, analysis, evaluation and mitigation of risks using the qualitative 5 × 5 matrix introduced in Chapter 2. This ensures methodological consistency across technologies and allows direct comparison of risk levels, mitigation strategies and operational controls.

The following sections describe the OVERHEAT Autonomous Drone's design features, operational constraints, safety mechanisms and cybersecurity framework, focusing on technical safety, system reliability, environmental robustness and data protection under maritime demonstration conditions

Figure 2: OVERHEAT Autonomous Drone System

6.1 Technical description and functional overview of the OVERHEAT Autonomous Drone System

The OVERHEAT Autonomous Drone is an aerial system that integrates high-end industrial solutions with customized designs tailored specifically for maritime operations. The system is designed to ensure efficient and effective fire detection and firefighting support, both in port environments and on board of the vessels.

The core of the system is the DJI Dock 2: a high-performance, automated hangar that features a lightweight and compact design. This advanced docking station is engineered for rapid deployment, allowing two operators to carry and install it with ease. Its integrated body structure simplifies setup, reducing installation time and ensuring an efficient deployment.

The drone itself, the DJI MATRICE™ 3TD, is a state of the art in autonomous aerial technology. This sophisticated aircraft boasts a six-directional vision system, providing comprehensive obstacle detection for enhanced flight safety. Additionally, its infrared sensing capabilities enable precise environmental awareness, making it well-suited for complex missions. The RTK (Real-Time Kinematics) system ensures highly accurate positioning, crucial for precision-based operations. With an IP54 protection level, the drone is resilient against dust and water, enabling reliable performance in various conditions.

The OVERHEAT mission planning software is a customized version of DJI FlightHub 2, offering users an advanced, cloud-based environment purpose-built for the dynamic needs of maritime drone operations. This web platform is engineered to streamline every aspect of autonomous aerial task management, providing powerful tools for planning, coordination and oversight.

Adding to its versatility, the vessel version of the system includes satellite-based internet connectivity via Starlink for Maritime. This ensures uninterrupted communication and seamless data transmission, allowing users to operate the drone remotely from virtually anywhere. With Starlink's reliable, high-speed internet, operators can conduct real-time flight task planning, remote aircraft controls, live site monitoring and debugging, enabling efficient mission execution even in remote oceanic regions. (F. Russo 2025; F. Russo et al. 2025)

6.2 System safety of the OVERHEAT Autonomous Drone system

The system safety of the OVERHEAT Autonomous Drone system is based on its mechanical robustness, environmental control, redundant navigation and electrical protection. These design features ensure stable and predictable operation during autonomous missions. The system's safety architecture is primarily embedded in the physical design of the dock, the flight control logic of the drone and the integration of multiple redundant sensors.

The OVERHEAT Autonomous Drone provides a controlled environment for the drone during charging and standby. Its enclosure maintains internal temperature within the operational range of −25 °C to +50 °C and prevents the accumulation of condensation or dust. A climate regulation system ensures thermal stability during long idle periods, while ventilation and drainage components protect sensitive electronics from humidity.

The dock's overvoltage and grounding protection prevent damage from power fluctuations and an uninterruptible power supply (UPS) allows safe landing or controlled shutdown in case of external power failure. The charging process is managed automatically. Integrated sensors monitor the

drone's battery voltage and temperature, ensuring that power transfer occurs only within defined thresholds. If any irregularities are detected, charging stops immediately and an alert is transmitted to the operator. This automated control process prevents thermal overload or energy imbalance during repeated charging cycles.
Mechanical safety is achieved through precise landing guidance and a secure locking mechanism. Before charging begins, internal position sensors confirm that the drone is correctly aligned on the docking platform. This verification prevents mechanical strain or contact failure between charging interfaces.
The dock's housing and structural frame are built from corrosion-resistant materials suitable for long-term exposure to maritime environments. Mechanical seals, shock-absorbing mounts and protective coatings minimise the effects of vibration, moisture and salt intrusion.
The Matrice 3TD drone incorporates multiple redundant subsystems to maintain flight stability and navigational reliability. They use dual GNSS and RTK modules for precise positioning, inertial measurement units (IMUs) for flight attitude control and multi-directional obstacle detection sensors for collision avoidance. These systems continuously verify each other's readings to detect inconsistencies. If one component fails, the control logic automatically prioritises alternative data sources to maintain stable flight.
Autonomous safety mechanisms are embedded in the flight control software. Before each mission, the dock initiates automated diagnostics to assess weather conditions, propeller integrity, battery status and navigation accuracy. If any parameter lies outside acceptable limits, the launch is automatically aborted. During flight, safety thresholds, such as wind speed, altitude and battery level, are continuously monitored. If critical values are exceeded, the Return-to-Home (RTH) protocol is activated, guiding the drone to the dock or a predefined safe area for landing. This combination of redundancy, diagnostics and automated fail-safes ensures a high degree of technical reliability throughout operation. (F. Russo 2025; F. Russo et al. 2025)

6.2.1 Security and data protection of the OVERHEAT Autonomous Drone system

The OVERHEAT Autonomous Drone system integrates multiple layers of cybersecurity and data protection to ensure the confidentiality, integrity and availability of all operational and mission-related data. These measures safeguard communication between system components, protect firmware integrity and maintain compliance with data management requirements.
All communication between the dock, the Matrice 3TD drone and the FlightHub 2 management platform is encrypted. This encryption protects against unauthorised interception or manipulation of telemetry and control data. Each connection is authenticated through secure certificates and user access to the FlightHub 2 platform is protected via password and multi-factor authentication (MFA). The platform supports role-based access control, allowing administrators to assign distinct permissions for operation, maintenance and data management. Firmware integrity is maintained through digitally signed updates that are verified before installation. This ensures that only authentic and manufacturer-approved software versions are executed on the dock and drone.

Automatic updates can be disabled for closed-network or research operations, enabling compliance with organisational cybersecurity policies. Regular verification of digital signatures and checksum validation is recommended to prevent unauthorised code injection or corruption.
The system's data management features allow operators to choose between cloud-based synchronisation and Private Mode, in which all flight data remain stored locally on the dock and drone. In Private Mode, communication with external DJI servers is disabled.
Flight data, images and telemetry logs are synchronised automatically after each mission. These datasets include metadata such as mission time, location and drone identifiers to ensure full traceability. All files must be handled according to data retention and confidentiality requirements. Regular backups and access logging are required to guarantee data integrity and to support later verification of results.
Cybersecurity risks such as signal interference, GPS spoofing or unauthorised network access are mitigated through encrypted transmission, frequency monitoring and network isolation. When FlightHub 2 is accessed remotely, the connection should be secured using a Virtual Private Network (VPN) or a dedicated firewall.
Physical access to the dock's communication ports and network interfaces must be restricted to authorised personnel only. Any maintenance activities involving software or data transfer should be documented to maintain accountability. Together, these measures ensure that the OVERHEAT Autonomous Drone system maintains both operational and information security throughout its lifecycle. (F. Russo 2025; F. Russo et al. 2025)

6.3 Operational safety of the OVERHEAT Autonomous Drone system

Operational safety for the OVERHEAT Autonomous Drone system encompasses all procedural, environmental and organisational measures that ensure the safe operation of the drone and its supporting infrastructure during real-world use. While the system itself integrates a range of automated safety mechanisms, effective risk prevention in practice depends on correct operational procedures, adherence to environmental limits and the competence of trained personnel.
The following section outlines the key requirements for safe deployment, operation and maintenance of the OVERHEAT Autonomous Drone system within the OVERHEAT project.

Pre-Flight Procedures

Before each mission, operators must conduct a comprehensive pre-flight inspection to confirm the system's readiness.
This inspection verifies that both the dock and drone are fully functional and that environmental conditions are within safe operating limits. (F. Russo 2025; F. Russo et al. 2025)

Essential steps include (F. Russo 2025; F. Russo et al. 2025):

- System readiness: Confirm that the dock is connected to a stable power supply and that the uninterruptible power system (UPS) is active. Check that the drone's battery level is above 95 % and that the system shows nominal status in FlightHub 2
- Physical inspection: Visually inspect the drone, propellers, sensors and camera for damage, wear or contamination. Ensure that the dock's doors move freely and the landing platform is clear of debris
- Communication and navigation check: Verify stable communication between dock, drone and FlightHub 2 and confirm GNSS/RTK signal quality. Avoid sites with electromagnetic interference
- Mission validation: Review Return-To-Home coordinates
- Weather verification: Check local conditions and onboard weather data. The system may only be operated with wind speeds below 12 m/s
- Airspace restriction verification according to National Civil Aviation authority.

In-Flight Operations

During flight, at least one trained operator must supervise the mission remotely through FlightHub 2. Operators must continuously monitor telemetry data, including position, altitude, wind speed and battery level. If abnormal readings occur the operator must initiate a controlled landing or trigger the RTH procedure. Manual override commands must remain accessible at all times. The communication link between the drone, dock and control interface must remain stable throughout the mission.

When operated aboard vessels, additional precautions apply: the dock must be placed on a level, vibration-free surface with minimal magnetic interference and the drone's flight path must remain clear of rigging, cranes and other structures. (F. Russo 2025; F. Russo et al. 2025)

The pilot in command (PIC) shall check the presence of concurrent aerial traffic which may interfere or influence the operation.

Post-Flight Procedures

After each mission, a structured post-flight inspection ensures the system's continued readiness and the validity of collected data.

Operators must (F. Russo 2025; F. Russo et al. 2025):

- Inspect propellers, landing gear, gimbal and sensors for mechanical wear or residue
- Clean camera lenses and sensor surfaces with dry, non-abrasive materials
- Verify that the drone has landed correctly and that charging has started
- Review flight logs for anomalies such as signal loss, low battery or environmental warnings
- Confirm that data transfer to FlightHub 2 has completed successfully

Emergency Procedures

In the event of malfunction, communication loss or sudden weather deterioration, operators must follow the defined emergency protocol. If the drone loses signal or battery power reaches the critical threshold, the Return-to-Home function activates automatically. Before each mission, operators must ensure that the RTH coordinates correspond to the current dock position or an alternative safe landing area. In case of dock malfunction (e.g. door or power failure), the drone must divert to a predefined secondary landing site. Manual override via FlightHub 2 must remain available to force landing or abort missions.

Following any emergency event, a complete system inspection must be performed before further use and the incident documented in the operational log. (F. Russo 2025; F. Russo et al. 2025)

Personnel and Training

Operation of the OVERHEAT Autonomous Drone system must be conducted only by trained and authorised personnel.

Training must cover (F. Russo 2025; F. Russo et al. 2025):

- execution of pre-flight, in-flight and post-flight procedures
- use of FlightHub 2 for mission planning and supervision
- identification and response to error alerts
- compliance with safety distances and privacy regulations

7 RISK ASSESSMENT FOR THE OVERHEAT AUTONOMOUS DRONE SYSTEM

The purpose of this assessment is to systematically identify and describe all risks that could affect the safe, reliable and efficient operation of the system within the OVERHEAT project.
This section applies the same methodological approach used for the Bosch BME688 sensor system, ensuring consistency in risk identification, evaluation and mitigation according to the principles defined in Chapter 2. The analysis focuses on the specific conditions associated with the operation of the OVERHEAT Autonomous Drone system in maritime environments and considers a wide range of influencing factors, including technical performance, environmental exposure, power stability and human interaction.

7.1 Risk identification and evaluation for the OVERHEAT Autonomous Drone system

The evaluation in Table 7 and Table 8 show that all identified risks for the OVERHEAT Autonomous Drone system fall within the acceptable or tolerable range. Acceptable risks include ground-related hazards such as proximity to vehicular traffic (GR1), powerline infrastructure (GR2), buildings (GR3), gathering points (GR4), trees (GR5) and the possibility of a drone fly-away (GR9). These risks also include several aerial hazards such as glider or ultralight activity (AR3), NOTAM-related mission rescheduling (AR4) and aerial fly-away events (AR6). Their likelihood and consequences are low and no additional mitigation beyond existing procedures is required.
Tolerable risks include potential electromagnetic interference (GR6), the presence of unauthorised or unaware persons in the operational area (GR7), interference from wild animals (GR8) and aerial risks such as conflicting air traffic (AR1), emergency helicopter operations (AR2) and other UAS activity (AR5). These hazards may influence flight stability, communication performance or situational awareness, but their risk levels remain manageable. They require adherence to established operational controls, continuous monitoring and the preventive measures specified in the mitigation tables.
None of the identified risks are classified as intolerable. This indicates that the drone system can be operated safely when appropriate procedures and mitigation measures are applied.

The ground risks identified are listed in the following Table 7 for each typology of mission.

Table 7: Ground-related risks

Risk ID	Risk description	Potential consequence	Likelihood (1–5)	Consequence (A-E)	Risk level
GR1	Presence of streets with high vehicular traffic	Crash with vehicles caused by drone fall	1	D	Acceptable
GR2	Presence of electric powerline infrastructure	Interferences or crash with powerlines	1	C	Acceptable
GR3	Presence of buildings	Collision with building	1	D	Acceptable
GR4	Aggregation points with possibility of gathering of people	Injuries to people caused by drone fall	1	B	Acceptable
GR5	Presence of trees	Collision with Trees	1	D	Acceptable
GR6	Presence of sources of electromagnetic interference (Cellular radio base stations)	Interferences may cause loss of C2 Link	3	C	Tolerable
GR7	Unauthorized or unaware persons in the area of flight operations	Not authorized persons that may disturb or interfere with the PIC during flight operations	2	C	Tolerable
GR8	Wild animals	may disturb or interfere with the pilot during flight operations;	2	C	Tolerable
GR9	UAS fly away	UAS falls and crashes on the ground	2	D	Acceptable

7.1.1 Ground-related risks

GR1 - GR5 (traffic, powerlines, buildings, gathering points, trees)
These risks were assigned low likelihood values (1) because the drone operates with precise RTK positioning, automated obstacle detection and predefined flight corridors. The Matrice 3TD maintains stable altitude and lateral control, making unintended drift unlikely. Consequence levels remain low (C or D) because any collision would occur at low altitude and reduced ground speed during take-off or landing, limiting potential damage.

GR6 Electromagnetic interference
The likelihood is moderate (3) because cellular base stations and port-side radio installations can introduce interference on GNSS/RTK corrections. Such conditions are occasionally observed during industrial drone operations. The consequence is rated as C because temporary signal degradation may require a forced landing or trigger the Return-to-Home procedure but does not typically result in loss of the aircraft.

GR7 Unauthorised or unaware persons
The likelihood is rated 2 because access to the drone operation area is controlled during demonstrations, but human presence cannot be fully excluded in harbour environments. The consequence is C because unexpected human intrusion may require immediate mission interruption or landing to ensure operational safety.

GR8 Wild animals
The likelihood is moderate (2) due to occasional presence of birds near port structures. The consequence is C because bird interference may affect flight stability or sensor visibility but rarely leads to severe damage. Such interactions are known from routine industrial drone missions.

GR9 UAS fly-away
The likelihood is very low (1) because the dock system performs comprehensive pre-flight diagnostics, including battery health, sensor status and GNSS calibration. Consequence is D because in the unlikely event of a fly-away, the aircraft would eventually land or crash, but with minimal probability of severe harm due to controlled environment and geofencing.

The aerial risks identified are listed in the following Table 8 for each typology of mission.

Table 8: Aerial-related risks

Risk ID	Risk description	Potential consequence	Likelihood (1–5)	Consequence (A-E)	Risk level
AR1	Interfering traffic (CTR / ATZ operations)	Temporary request of landing	2	C	Tolerable
AR2	Presence of emergency helicopters	Immediate stop of flight operations	2	B	Tolerable
AR3	Gliders, paragliding activity Ultra-light flight	In-flight crash	1	B	Acceptable
AR4	NOTAM	Mission re-schedule	1	B	Acceptable
AR5	Other UAS interfering activities	Temporary landing or in-flight crash	2	B	Tolerable
AR6	UAS fly away	UAS falls and crashes on the ground	1	D	Acceptable

7.1.2 Aerial-related risks

AR1 Interfering air traffic
Likelihood is moderate (2) because harbour areas occasionally lie near controlled airspace boundaries. Consequence is C because the drone may need to interrupt the mission or descend quickly, but collision risk remains low due to defined altitude limits and airspace monitoring through NOTAMs.

AR2 Emergency helicopter operations
Likelihood is low (1) because helicopter movements are infrequent and typically pre-announced. Consequence is B because an unexpected helicopter entering the flying zone requires an immediate stop of operations to maintain safe separation.

AR3 Gliders or ultralight aircraft
Likelihood is very low (1) in the maritime test environment. Consequence is B because a conflict could result in a high-severity airborne incident, even though the probability is minimal.

AR4 NOTAM-related restrictions
Likelihood is very low (1) because NOTAM changes are infrequent and can be monitored before each mission. Consequence is B because such restrictions require mission rescheduling but do not pose a direct operational hazard.

AR5 Other UAS activity

Likelihood is moderate (2) because parallel UAS operations may occur, especially in port demonstration scenarios. Consequence is B because airspace congestion or interference can require an immediate landing or automatic RTH activation.

AR6 UAS fly-away

Likelihood is very low (1) due to the same diagnostic and redundancy systems as GR9. Consequence is D because loss of the aircraft in mid-air could result in uncontrolled descent, but maritime test areas maintain safety buffers to minimise harm.

7.2 Risk assessment matrix for the OVERHEAT Autonomous Drone System

As with the Bosch BME688 sensor assessment, the evaluation of risks for the OVERHEAT Autonomous Drone system follows the same methodological approach. All identified hazards were plotted into a 5 × 5 qualitative risk matrix, Table 9, which combines likelihood and consequence scores to visualise the overall risk distribution.

Table 9: Risk Assessment Matrix for the OVERHEAT Autonomous Drone System

Likelihood	Risk Assessment Matrix					
	5 Frequent	Intolerable	Intolerable	Intolerable	Tolerable	Tolerable
	4 Occasional	Intolerable	Intolerable	Tolerable	Tolerable	Tolerable
	3 Remote	Intolerable	Tolerable	Tolerable **GR6**	Tolerable	Acceptable
	2 Improbable	Tolerable	Tolerable **AR2, AR5**	Tolerable **GR7, GR8 AR1**	Acceptable **GR9**	Acceptable
	1 Extremely improbable	Tolerable	Acceptable **GR4 AR3, AR4**	Acceptable **GR2**	Acceptable **GR1, GR3, GR5 AR6**	Acceptable
		A Cata-strophic	**B** Hazardous	**C** Major	**D** Minor	**E** Negligible
		Consequence				

8 RISK MITIGATION & PREVENTIVE CHECKLIST FOR THE OVERHEAT AUTONOMOUS DRONE SYSTEM

The risk mitigation strategy for the OVERHEAT Autonomous Drone system aims to ensure that all identified hazards are controlled through preventive engineering measures, operational discipline and procedural safeguards.
The OVERHEAT Autonomous Drone is a complex, autonomous system operating in dynamic maritime conditions; therefore, risk reduction focuses on the areas of flight integrity, environmental protection, power and communication reliability and data security.

8.1 Mitigation measures for the OVERHEAT Autonomous Drone System

The following tables present the mitigation measures developed for the OVERHEAT Autonomous Drone system, addressing both ground-related and aerial risks identified in the previous section. Table 10 outlines mitigation measures for ground-related risks, which focus on ensuring the safety of personnel, infrastructure and equipment during take-off, landing and low-altitude operations. These measures combine technical precautions, such as obstacle mapping, exclusion zones and interference monitoring with procedural controls for managing human and environmental factors. Table 11 summarises the actions designed to manage aerial risks, concentrating on flight integrity, airspace coordination and the prevention of in-flight conflicts or system malfunctions.

Table 10: Mitigation measures for ground-related risks

Risk ID	Risk description	Mitigation measure
GR1	Presence of streets with high vehicular traffic	Define exclusion zones; establish safety perimeter; operator supervision during take-off and landing
GR2	Presence of electric powerline infrastructure	Avoid flight routes near powerlines; verify GNSS/RTK accuracy; use electromagnetic interference detection tools
GR3	Presence of buildings	Pre-flight route planning and obstacle mapping; ensure accurate altitude control via telemetry
GR4	Aggregation points with possibility of gathering of people	Maintain safety distances; plan emergency landing areas; avoid populated zones in mission planning
GR5	Presence of trees	Define obstacle-free flight corridors; maintain sufficient altitude buffer
GR6	Presence sources of electromagnetic interference (Cellular radio base stations)	Avoid areas with strong radio signals; verify C2 link quality pre-flight; monitor telemetry data for signal loss
GR7	Un-authorized or unaware persons in the area of flight operations	Establish controlled operation zone; inform nearby personnel; abort mission in case of human intrusion
GR8	Wild animals	Conduct pre-flight area inspection; abort mission if animal interference detected
GR9	UAS fly away	Verify communication link stability; confirm RTH setup; maintain manual override readiness

Table 11: Mitigation measures for aerial-related risks

Risk ID	Risk description	Mitigation measure
AR1	Interfering traffic (CTR / ATZ operations)	Pre-flight airspace validation; NOTAM check; continuous telemetry monitoring; emergency return protocol
AR2	Presence of emergency helicopters	Real-time monitoring through FlightHub 2; communication with airspace authorities; immediate landing procedure if conflict detected
AR3	Gliders, paragliding activity	Airspace scan and NOTAM verification before mission; define safe altitude corridors; abort protocol in case of unknown traffic
AR4	NOTAM	Check for new NOTAMs before each mission; adjust mission plan; maintain communication with local ATC
AR5	Other UAS interfering activities	Detect nearby UAS through telemetry; avoid congested airspace; activate Return-to-Home (RTH) if signal interference detected
AR6	UAS fly away	Confirm GNSS/RTK stability before launch; verify Return-to-Home coordinates; use redundant communication links

8.2 Example of a checklist for preventing risks during field use of the OVERHEAT Autonomous Drone system

The following checklist in Table 12 summarises essential control points for the safe and reliable use of the OVERHEAT Autonomous Drone system in maritime and experimental environments.

Table 12: Example Checklist for the OVERHEAT Autonomous Drone System

Control Area	Verification Method	Frequency	Done	Remarks
Maintenance and cleaning	Inspect air inlets, ventilation filters and landing platform; replace damaged or corroded components			
Power supply and battery health	Monitor power input and battery condition during flight; perform UPS and charging system inspection			
GNSS/RTK positioning	Conduct pre-flight RTK/GNSS signal check; verify redundancy and satellite link stability			
Weather and environmental conditions	Verify temperature, humidity and wind parameters before each launch; suspend flights above 12 m/s wind speed			
Data security and access control	Restrict user access, operate in Private Mode			
Training	Ensure personnel are briefed on safety procedures			
Temporary Ground obstacles	Obstacle does not present in previous site inspection			
Alternative Landing site identification	Check possible alternative landing sites to be used in case of contingencies			
Check of Airspace Restriction (e.g. NOTAM)	Check presence of unexpected airspace restrictions			
Unexpected gathering of people	Verify presence of unexpected gathering of people			

9 CONCLUSIONS

Deliverable 7.3 establishes a unified methodological approach for managing safety and security risks within the OVERHEAT project. By applying a consistent framework based on ISO 31000:2018, the ALARP principle and the methodologies developed in WP 3, the deliverable ensures that all technological systems evaluated under WP 7 are assessed using comparable criteria for risk identification, evaluation and mitigation. The approach promotes transparency, traceability and continuous improvement across the project's simulation and demonstration activities.

The framework was applied to two representative systems: the Bosch BME688 sensor and the OVERHEAT Autonomous Drone. This application demonstrates how the same structured method can be adapted to different technological and operational contexts. For the BME688, the analysis centred on environmental robustness, electrical safety and data integrity, while for the drone system it focused on flight safety, power stability and cybersecurity. In both cases, mitigation measures and preventive checklists were developed to ensure that operational risks remain within tolerable limits.
In addition, the deliverable introduces a structured process for identifying and managing emerging risks. This mechanism ensures that the assessment framework remains adaptive during the upcoming demonstration phase and can be refined as new information becomes available. As the demonstration and simulation campaigns have not yet been completed, the results presented here are preliminary.

Overall, D 7.3 contributes both a methodological and practical foundation for risk management in maritime innovation. It supports the broader objectives of OVERHEAT by enhancing preventive capabilities, strengthening situational awareness and promoting a robust safety culture across shipboard and port operations.

REFERENCES

Bosch Sensortec GmbH (Hg.) (2021): BME AI-Studio Manual.

Bosch Sensortec GmbH (Hg.) (2022a): BME688 4-in1 environmental sensor unit with AI.

Bosch Sensortec GmbH (Hg.) (2022b): BME688 Development kit.

Bosch Sensortec GmbH (Hg.) (2024): BME688 Digital low power gas, pressure, temperature & humidity sensor with AI.

C. S. Carlson (2014): Understanding and applying the fundamentals of FMEAs.

F. Russo (2025): User Manual of the UAS Recharging Station. TOPVIEW.

F. Russo; L. Porricelli; M. Iadaresta; G. Gagliarde; G. Luisi; A. Mennella (2025): User Manual of the UAS Recharging Station Software. TOPVIEW.

M. Glossop; A. Loannides; J. Gould (2000): Review of hazard identification techniques.

Olsen, Alexander (Hg.) (2024): Safety Culture and Leading Indicators for Safety in the Maritime and Offshore Environment. Cham: Springer Nature Switzerland (Springer Series on Naval Architecture, Marine Engineering, Shipbuilding and Shipping, 20).

ISO 31000:2018, 2018: Risk management - Guidelines.

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement Project No: 101076633. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.