European Maritime Safety Agency

QUANTIFYING THE RISK TO MARITIME SECURITY FROM THE MALICIOUS USE OF UNMANNED AIRCRAFT SYSTEMS

A RISK ASSESSMENT METHODOLOGY FOR PORTS AND SHIPS

Date: 07/2026

EMSA

Recommended citation:

European Maritime Safety Agency (2026), *Quantifying the risk to maritime security from the malicious use of Unmanned Aircraft Systems. A risk assessment methodology for ships and ports*, EMSA, Lisbon

Legal notice:

Neither the European Maritime Safety Agency (EMSA) nor any third party acting on behalf of the Agency is responsible for the use that may be made of the information contained in this report.

Copyright notice[1]:

Cover photo: georgealmanza / Getty Images

Catalogue Number: TN-01-26-005-EN-N
ISBN: 978-92-95229-49-5
DOI: 10.2808/5059307

Publications Office of the European Union
Law | Data | Publications

[1] The copyright of EMSA is compatible with the CC BY 4.0 license

TABLE OF CONTENTS

QUANTIFYING THE RISK TO MARITIME SECURITY FROM THE MALICIOUS USE OF UNMANNED AIRCRAFT SYSTEMS. A RISK ASSESSMENT METHODOLOGY.

This document aims to equip maritime security professionals in both the public and private sectors with a robust tool for evaluating risks associated with Unmanned Aircraft Systems (UAS). It provides a detailed analysis of potential threats, identifies targets in the maritime domain considering Regulation (EC) No. 725/2004 (port facilities and ships), and the actors behind these threats. Furthermore, the document introduces a systematic methodology for assessing such risks and offers practical guidance on security measures to mitigate them, including the allocation of resources based on identified threats, as well as recommendations for implementing the proposed methodology. The implementation framework is the one set out in the International Ship and Port Facility Security (ISPS) Code, SOLAS XI-2 and the Regulation, which emphasises a preventive approach and leaves incident response to law enforcement agencies.

The proposed risk assessment methodology is versatile and applicable beyond threats posed by malicious UAS activities. It can be adapted to evaluate any security threats within the maritime environment, making it a valuable tool for comprehensive security management.

EMSA

1. INTRODUCTION

Regulation (EC) No 725/2004 on enhancing ship and port facility security (from this point referred as the Regulation) requires that Ship Security Assessments (SSA) identify potential threats to the key shipboard operations and assess the likelihood of their occurrence. This process is essential for establishing and prioritising appropriate security measures[1]. Similarly, Port Facility Security Assessments (PFSA)[2] must consider threats to assets and infrastructure, including potential damage to ships as well as port facilities. Moreover, SSAs should consider all possible threats that may include damage to the ship or port facility (PF)[3]. Finally, the Regulation also includes recommendations on how to implement PFSAs for PFs[4].

In this context, among the threats to be considered, those linked to UAS (also known as Remotely Piloted Aircraft Systems (RPAS)) and commonly referred to as "drones" have gained significant attention.

UAS consist of an aircraft capable of autonomous or remote operation, a ground control system and data transfer mechanisms enabling communication between the operator and the aircraft. They can operate individually or in coordinated swarms.

Initially developed for military applications, UAS offer strategic advantages such as a reduced risk to human operators, small size and economic and human lives cost-effectiveness. These features have led to their adoption by State and non-State actors for surveillance and attack purposes, with functions expected to evolve further. Civilian use has also surged due to technological advancements, decreasing costs, and increased accessibility. Their presence in the European skies has increased exponentially in recent years as numerous affordable and reliable solutions have become widely available. The integration of 5G networks and Artificial Intelligence (AI) enhancing connectivity and autonomous decision-making capabilities are also behind the development and widespread use of UAS.

However, the success of recreational UAS has been accompanied by a significant number of safety and security incidents, including thwarted terror plots within the EU. Since UAS are easy to obtain, difficult to detect and counter, and simple to pilot from a remote location, they have become an attractive tool for criminal and terrorist actors. Examples of this use include smuggling illegal goods into prisons and across country borders, spreading propaganda, monitoring law enforcement activities, supporting cyberattacks and disrupting air traffic. Additionally, concerns have been raised regarding the collection of data by UAS, such as imagery of critical infrastructures and the potential access by manufacturers to this information.

Notable instances of malicious UAS use include attacks by Hamas on Israel, Houthi assaults on ships in the Red Sea and the deployment of commercial drones in the Ukraine conflict. These incidents underscore the potential weaponisation of UAS and highlight the need for comprehensive security assessments in maritime contexts.

[1] Regulation 725/2004 annex II Part A 8.4.3.

[2] Regulation 725/2004 annex II Part A 15.5.2.

[3] Regulation 725/2004 annex III Part B 8.9 mandatory as indicated by article 3.5.

[4] Regulation 725/2004 annex III Part B 15.9 to 15.12

This evolving threat landscape creates security concerns that justify the inclusion of UAS-related risks in security risk assessments in the maritime context as defined by the Regulation. Therefore, the present document aims to consider the threat posed by non-military UAS to ships and port facilities. In this regard, the document adapts to the maritime domain the Join Research Centre (JRC) technical report "Protection against Unmanned Aircraft Systems; Handbook on UAS risk assessment and principles for physical hardening of buildings and sites"[5].

[5] Security by Design: Protection of public spaces from terrorist attacks (European Commission, 2022)

Hansen, P. and Pinto Faria, R. (2023), Protection against Unmanned Aircraft Systems: Handbook on the protection of critical infrastructure and public spaces, European Commission, Joint Research Centre, Publications Office of the European Union, Luxembourg, JRC 132714.

Karlos, V. and Larcher, M., Protection against Unmanned Aircraft Systems: Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/758582, JRC132967.

https://dx.doi.org/10.2760/969680

2. DESCRIPTION OF THE THREAT

2.1 POTENTIAL ACTORS

Most of the security related incidents involving UAS in public areas are caused by **clueless** and **careless** individuals. They are either unaware of existing regulations and restrictions or they disregard them. On occasion, system malfunctions might cause incidents. The relevance of these actors my vary depending on the location of the PF or the type/trade of the ship, particularly in areas close to public spaces where their presence can be expected. However, the primary focus of the proposed assessment methodology are **terrorist** and **criminal** users and, in some cases, **activist groups** (e.g. environmental and social). State actors, particularly those using military grade equipment, are outside the scope of the Regulation. However, **State actors** might be involved in terrorist attacks and hybrid warfare. Also, in some cases, terrorist groups (i.e. Houthis, Hamas) use military grade equipment for their attacks. In this context, attacks such as those on ships in the Red Sea are of concern for ship management companies across the world, even if it might be questionable whether they fall under the provisions of the ISPS Code. Nevertheless, since their activities may include tactics similar to those employed by other malicious UAS users, the assessment of the threat and the potential implementation of subsequent protective measures would be comparable and therefore considered in this document.

Defining who a terrorist is, is not straight forward and depends on the subjective judgement of those conducting the assessment. There is also a blurred distinction between criminal and terrorist groups with the main difference being their motivation. Terrorists are driven by ideological, political or religious objectives whereas criminals are typically motivated by financial gain or personal benefit. In terms of tactics, criminals often try to avoid detection and publicity, whereas terrorists seek to draw attention to their acts. However, it is essential to acknowledge that there is a significant overlap between them with some groups exhibit characteristics of both. Many terrorist groups generate funds through criminal activities and/or collaborate with criminal organisations. Furthermore, both criminal organisations and terrorist groups may have access to training and the acquisition of advanced UAS and weapons. In this regard, the distinction between organised crime and petty crime may be more pronounced than the difference between organised crime and terrorist groups.

Environmental and social activists may also pose a threat to certain PFs and ships engaged in specific operations or trade, notably in the energy sector. Their tactics and targets may diverge from those employed by terrorist groups while their objectives differ from those of criminal groups. Nevertheless, they can be highly motivated and may cause significant disruption to operations potentially impacting the safety and security of PFs and ships.

The motivations of the different actors will define the type of PF or ship they target. For example, terrorists are likely to select targets and employ attack tactics that maximise visibility due to the potential for significant casualties or symbolic impact, while activist groups would typically target companies or entities they perceive as hostile to their cause.

In summary, the risk assessment methodology presented in this document focusses on the malicious use of UAS by terrorists, criminals, and activist groups but also considers clueless and careless users. Their motivations, objectives and tactics may differ greatly. However, there might also be a significant overlap between them.

2.2 TYPES OF UAS AND AVAILABILITY

UAS exhibit diverse designs, performance characteristics and operational capabilities. However, when evaluating UAS as a potential threat, the principal factors that serve as effective classification criteria are:

1. Weight/Size: The weight of a UAS is pivotal in determining its overall size and therefore its performance characteristics, including endurance, operational range, speed and payload capacity. It also has an impact in the visibility of the UAS, particularly in daylight.

- **Micro UAS:** These very small UAS weigh less than 2 kg, making them easy to operate and difficult to detect. Due to their compact size, they have limited payload capacity (significantly less than 0.5 kg), endurance and range, rendering them suitable for operations with small payloads and in close proximity to the target. They have very small logistical needs, enabling them to be easily and stealthy transported to the target area and take off from virtually anywhere (no take-off /landing requirements).

- **Small UAS:** Weighing between 2 and 25 kg, these UAS can carry a payload of up to 5 kg, such as explosive devices or surveillance equipment. The maximum payload capacity varies depending on their design, motors, battery life, etc. However, as a general guide the following may be considered:
    - 2-3 kg UAS maximum payload capacity of approximately 0.5 kg.
    - 10-15 kg UAS maximum payload capacity of approximately 2 kg.
    - 25 kg UAS maximum payload capacity of up to 5 kg.

    Note: standard hand grenades, such as the RGD-5 or F1, typically weigh between 300-600 grams, making them a feasible payload for small UAS (as extensively used in Ukraine).

  The endurance, and therefore the range, of small UAS is usually less than 1 hour without payloads, being reduced to approximately 30-40 minutes depending on the specific payload carried.

- **Medium and Large UAS:** Weighing 25 kg or more, these UAS are capable of carrying substantial payloads, including heavier explosives or advanced surveillance gear. They also offer enhanced performance in terms of endurance and range allowing them to be operated from a considerable distance to the target. On the other hand, their larger size and weight make them more challenging to deploy discretely. They are not commercially available (see point 2 below) but their malicious use poses a significant threat.

Category	Weight (kg)	Payload capacity (kg)
Micro	< 2	<<0.5
Small – Low	2-10	<0.5
Small – Medium	10-15	<2
Small – High	15-25	<5
Medium/large	>25	>>5

2. Morphology: Another important parameter to be considered is the rotatory wing (multicopter[6]) vs fixed wing configuration. This has an impact on several factors such as endurance and range, operational logistics and piloting complexity.

- Fixed wing drones are faster and can stay in the air longer, so have a much greater range. However, they may require an airstrip for take-off and landing.

- Multicopter consume more energy to stay in the air, so have a shorter endurance/range. However, they are easier to operate and pilot and have better manoeuvrability.

There are also commercially available hybrid solutions with Vertical Take-off and Landing (VTOL) and Fixed Wing capability.

3. Control: UAS might be remotely piloted within the visual line of sight (VLOS) and beyond (BVLOS). BVLOS with a first-person view (FPV) using goggles, a screen or even be programmed to search for a predefined target, limit the effectiveness of some security measures that seek to prevent direct sight of the target such as privacy fences or planting trees. Lately fibre-optic control drones have gained importance in Ukraine. These UAS are immune to electronic warfare detection and interception, have a cable range of up to 20 km, fly at a low altitude but have reduced manoeuvrability compared to other systems.

4. Accessibility and complexity: This factor classifies UAS according to their accessibility, including required permissions, cost, system complexity and the overall reliability and robustness of each type, thereby indicating how easily an individual can obtain and operate them

- **Commercially available UAS** (Low barrier to acquisition): These systems are readily available for purchase in retail stores or from online platforms. They are primarily intended for recreational purposes. Their cost is relatively low/medium, ranging from a few hundred up to around five thousand euros. The ones in the "open category" can be operated without specialised knowledge or permits and, due to their recreational nature, are designed to be simple and reliable. Drones over 250 gr. require pilot registration and online training[7], with others not in the open category only requiring registration at the shop. They cannot be operated effectively in hostile environments such as GPS denied environments or areas with frequency jamming, since they lack mitigation measures to overcome these deterrence methods.

- **Industrial/Professional UAS** (medium barrier to acquisition): Used in industries like agriculture, real estate and the media, these UAS require a higher level of expertise and a larger budget, limiting their accessibility to the general public. Some models may require specific permissions, licenses or registrations to operate. However, like their commercial counterparts, they do not have any mitigation measures to ensure operation in hostile environments such as GPS denied environments or areas with frequency jamming.

- **Restricted and military UAS** (high barrier to acquisition): Acquiring these advanced systems typically require selected company or authorised governmental involvement. In some cases, their acquisition is limited to military or authorised security agencies. Some models within this category are also referred to as loitering munitions because of their capability to loiter in the area before hitting the target directed by radio signals from the ship. These sophisticated and complex UAS require a high level of training and technical expertise. Moreover, they are equipped with technologies that enable them to be operated in hostile environments. Due to their high cost,

[6] Helicopter configuration is discarded in favour of multicopter also known as multirotor.

[6] EU 2019/945 and EU 2019/947

advanced capabilities and limited availability, these UAS are generally accessible only to State actors or well-organised and well-funded terrorist groups. An example of models commonly used against merchant ships are the Shahed-131 and 136 with ships being targeted up to 600 nautical miles offshore.

- **Improvised UAS (variable complexity):**
    - Modified Commercial UAS: Technically skilled individuals can modify commercial UAS to carry light payloads, potentially posing security risks. This category includes UAS altered for surveillance or simple payload delivery.
    - Homemade UAS: Built from scratch using readily available parts or open-source designs, these systems can be created by hobbyists with basic electronics and aeronautics knowledge. While these UAS are inexpensive and adaptable, they typically lack the reliability and sophistication of commercial or professional drones.

High accessibility increases potential for use, while restricted acquisition limits availability to specialised users with significant resources.

This taxonomy defines the complexity of obtaining and operating the different types of UAS. This complexity will be used to quantify the risk associated with a specific attack. The following table provides an overview considering an increasing scale from 1 to 4 where UAS that are easier to obtain and operate are allocated a higher score. For each type of UAS the most limiting factor should be considered. Therefore, not all the factors are required to be met simultaneously but it is the lower score to be considered. For example, a fixed wing professional UAS would score 2 while a fixed wing military grade would score 1.

Complexity	Weight/Size	Morphology	Control	Acquisition
1			BVLOS/ Programmed	Military
2	Medium/Large	Fixed wing		Improvised
3			VLOS	Professional
4	Micro/Small	Multicopter	FPV	Commercial

2.3. POTENTIAL METHODS TO EXPOSE SECURITY WEAKNESSES (ATTACK TACTICS)

This section provides an overview of the different tactics for the malicious use of UAS that may be employed by the different actors. The tactic used depends on the objective of the actor and its capabilities, and the type of PF or ship and their vulnerabilities.

The key threat tactics related to the use of UAS that have been identified in recent years in a non-military context include the following

- Transfer of hazardous loads for terrorism and sabotage. UAS can easily be used to transfer an improvised explosive device (IED), grenades or chemical, biological, radiological and nuclear (CBRN) materials within a secured perimeter. While most terrorist groups do not have access to CBRN materials, IEDs or grenades are easier to obtain and/or construct. As detailed in the next subsection, UAS are now able to carry substantial loads at great distances with accuracy.

  The load may be placed at a point of interest, which could be at an elevated position (e.g. on the roof of a building), be released through a specially designed mechanism or triggered whilst in mid-air, sacrificing the UAS. The UAS may be deliberately piloted against an exposed facility as a 'kamikaze' or one-way-attack (OWA) using drones that self-destruct on impact. This tactic can be used against infrastructures to cause operational disruption or to target areas with a concentration of passengers. In this regard, FPV UAS are now widely used, improving efficiency and targeting by the aggressor.

  In some cases, UAS may be weaponised by a firearm (or other projectile weaponry) specifically targeting individuals (i.e. VIPs) or to disperse chemical agents. However, at this stage, these tactics are not considered relevant for most PFs and ships.

  The most suitable UAS for this type of attack at close range are small to medium/large multicopters, although fixed wing UAS could also be used for distant targets. The consequences of such attack would largely depend on the payload of explosives and therefore of the size of the drone.

- Smuggling/delivery. A variety of different payloads (e.g. drugs, illicit goods, weapons) can be delivered on board bypassing the PF's security controls.

  In addition, UAS can be used to deliver equipment (e.g. firearms) to an aggressor inside a secured perimeter or at specific locations since they can easily bypass traditional control points and restricted areas while the aggressors themselves enter through normal control procedures.

  Multicopters are the most suitable UAS for this tactic. The payload required would define the size of the drone from small to medium/large.

- Intelligence, surveillance and reconnaissance. UAS may also be used to collect information and observe activities in preparation for an attack.

  This is mainly achieved using cameras that can operate at night or using thermal sensors that can track motion. This enables aggressors to document the vulnerabilities of a potential target remotely and utilise this information to inform their attack strategy or even provide real-time information while the attack unfolds. Other types of sensors used include microphones that facilitate eavesdropping on private/confidential conversations.

A wide range of UAS can be used for this purpose. The location of the area to be surveyed and the time span would define the type of drone, which could go from an inconspicuous micro multicopter to larger fixed wing that can survey large areas far away for longer periods.

- Cyberattacks. UAS can facilitate hybrid attacks that merge physical and cyber tactics. Since technologies such as Wi-Fi, Bluetooth, and radio frequency identification (RFID) have a limited range, restricting access is an efficient measure to prevent hacking. However, UAS equipped with small computers (e.g. Raspberry Pi) and appropriate gear (e.g. a network or radio frequency (RF) scanner) can be deployed on the roof of a building and gain unauthorised access to local wireless networks. It could mimic a Wi-Fi network or hijack Bluetooth devices (e.g. keyboards), disrupt communications, deliver malware, hijack and/or manipulate sensitive data, and even steal passwords from users using keylogging techniques. While UAS can be used as a protective tool for PFs and ships to survey the surrounding area, they can also become the target of cyberattacks, which can attempt to gain control, access their data or disrupt their operations.

  Usually, small multicopters are enough to carry the equipment required for this attack.

- Jamming. This tactic represents another form of hybrid attack that combines electronic warfare with physical elements. By equipping a UAS with appropriate electronic equipment it can be used to interfere with radio signals such as those used by perimeter security systems, ship communications, GPS navigation or mobile phone networks. This tactic can also be exploited to disrupt operations in PFs that rely heavily on automation.

  As in the previous tactic, small multicopters are enough to carry the equipment required for this type of attack.

- Disruption and interference. The presence of a UAS may be sufficient to interfere with the normal operations in PFs and ships due to the potential safety risk it poses. They may also be used to provoke panic reactions in passenger waiting areas, which could lead to injuries/victims or create an opportunity for a secondary attack such as channelling people into specific locations that are more vulnerable to damage.

  Small FPV multicopters might be the most appropriate to implement this tactic.

- Propaganda. UAS may also be used by activist groups as well as terrorist groups to record their actions, spread leaflets or other material in public spaces in an effort to reinforce their propaganda efforts.

  Micro and small multicopters would be sufficient to record an attack while small to medium size might be required to spread leaflets.

These attack tactics will evolve with the development and improvement of UAS capabilities but also with the continuous decline in their price. Furthermore, the pilots' proficiency is bound to improve over time with more and better trained pilots and the use of AI allowing for targeting autonomy. There have already been examples of "drone-swarm" attacks such as the attack on Russian military bases in Syria by a swarm of 13 drones.

3. POTENTIAL TARGETS

3.1. PORT FACILITIES (PFS)

Definition

Commonly known as terminals, according to the Regulation[8], "Port facility is a location [...] where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward, as appropriate".

Typology

The typology of PFs is usually defined by the format of the goods that are handled and the types of ship operating in them. This classification defines the characteristics of the infrastructure (static and dynamic) and the cargo handling equipment used. In this context, the following types of PFs can be considered:

1. **Dry bulk terminals** handle commodities like coal, iron ore and grain that are transported in large quantities. They require specialised equipment (belts and cranes) and open storage space (minerals) or storage facilities (grain). Security is focused on protection of the cargo from theft or sabotage. They are usually specialised in either the export or import of goods which dictates the type of equipment used. They are generally not a likely target for an attack in a peaceful context.

2. **Break-bulk terminals** handle non-containerised cargo that is usually carried in drums, bags, pallets or boxes. They usually require a combination of open storage space and warehouses with cranes and specialised cargo handling gear. The main security concerns for these PFs are theft, tampering or unauthorised access to the cargo.

3. **Container terminals** are designed to handle standardised containers. They are equipped with cranes and heavy-duty equipment (e.g. trucks, reach stackers, forward lifts) to handle containers within the terminal and to/from the ship. Usually, these high intensity operations require a high level of automation which can make cybersecurity a critical concern. In parallel, security measures are focused on preventing theft, smuggling and unauthorised access to the cargo.

4. **Ro-Ro terminals** handle vehicles that are rolled on and off ro-ro ships. They require ramps and parking space and may to a certain extent also accommodate passengers (truck drivers may travel with their vehicles). In the case of regular lines carrying both passengers and Ro-Ro cargo, they are also considered as passenger terminals. Security in these terminals is focused on access control and preventing theft.

[8] Regulation (EC) No 725/2004 Annex I Regulation 1.1.9

5. **Liquid bulk terminals** are designed to handle oil, petroleum products and other liquid commodities including liquified gas and chemicals. They require specialised trans-shipment equipment (piping, manifolds and loading arms) and storage tanks. They may range from sludge reception facilities to high-risk critical infrastructures such as Floating Storage Regasification Units (FSRU) for the reception of Liquified Natural Gas (LNG). The primary threat to these terminals is the transporting of hazardous substances for sabotage and cyberattacks, as well as being potential targets for activist groups. The security of these terminals is important due to the environmental impact, strategic value and subsequent consequences for adjacent areas and/or the economy.

6. **Passenger terminals** operate cruise ships and ferries carrying passengers and vehicles. In these terminals, the primary concern is protecting human lives. Security is focused on access control and the screening of passengers and vehicles. An attack on these PFs may have significant consequences due to the potential loss of life and they may also be targeted due to their symbolic value.

In parallel to this taxonomy based on the types of operation, many other factors should be considered when drafting the attack scenarios. These include the size of the PF and its ownership, the flag and ownership of the ships calling, as well as the ownership of the cargo. For example, a container terminal regularly loading weapons should consider different attack scenarios than one that only loads regular cargo. Similarly, a break-bulk terminal involved in environmentally sensitive operations may need to consider actions by social groups.

Assets to consider.

In order to perform the PF security risk assessments, the main assets to consider should be identified so that the vulnerabilities linked to them can be defined and appropriate measures can be introduced to minimise them. In this context, some of the assets to consider are:

- **Perimeter and access points**: Port facilities may cover a large area with many access points from both land and waterside, which may be challenging to monitor and secure. While fences, barriers and other physical infrastructure provide a primary layer of security, they also become assets that require protection. Using UAS to compromise perimeter integrity creates a 3rd dimension that is frequently overlooked.

- **Cargo handling equipment and storage areas:** The equipment and facilities used for loading and unloading (e.g. loading arms/manifolds, cranes, ramps, belts) and storing cargo (e.g. tanks, warehouse, container yard, freezer warehouse) are the main targets for theft, smuggling and sabotage. In passenger terminals, equivalent areas include gangways, waiting areas and luggage storage and control areas. This makes the implementation of security procedures and infrastructure to control and monitor access to them necessary. UAS can be used to gather intelligence or directly to perpetrate attacks on vulnerable points such as roof ventilation intakes.

- **Ships:** SShips berthed at a port are vulnerable to hijacking, tampering and other threats. Therefore, it is necessary to protect the **ship to PF interface**. This is a critical area that requires coordination and communication. This interface encompasses not only cargo handling but also any exchange of goods and services (e.g. mooring gear, bunkers, ship stores). The use of UAS to gather intelligence or transfer illicit cargo makes the control of this interface more challenging, particularly in passenger terminals.

- **Essential infrastructure and utilities:** This category includes power plants, water supplies, telecommunications systems, security command centres (including closed-circuit television - CCTV), management offices (e.g. loading office/control room) and other vital infrastructure (e.g. canal/dykes locks) that, if damaged or disrupted, could impact port operations and compromise security. UAS can be used to gather intelligence or to transport hazardous substances for terrorism or sabotage these objectives.

- **Information and communication systems** including computer systems and networks deserve special mention due to their vulnerability to cyberattacks and disruption. This threat gains a new dimension with the possibility of hybrid attacks using UAS, particularly if this type of attack is not addressed in the cybersecurity plan.

- **Restricted areas:** Port facilities define restricted areas that require strict access control. However, this control may be challenged using UAS, highlighting the need for enhanced security measures.

- **Adjacent areas:** SSurrounding areas outside the port facility, and even outside the port, including roads, bridges and other infrastructure could be used to gain access or launch attacks. Controlling these areas becomes critical when considering the use of UAS with a short-range and/or visual line-of-sight control.

Some risk assessment methodologies may consider **personnel and passengers** as an asset to protect since the protection of human life is of paramount importance. However, in the proposed methodology, personnel and passengers are not considered a separate asset to protect since the potential human losses are considered in the quantification of the consequences for each attack scenario. Moreover, in passenger terminals, the areas and equipment used by the passengers are already considered assets to protect.

3.2. SHIPS

Definition[9]

The Regulation applies to passenger ships, cargo ships (of 500 gross tonnage and upwards) engaged on international voyages, Class A passenger ships within the meaning of ships[10] operating domestic services and their companies, and mobile offshore drilling units. However, depending on a risk assessment conducted by each Member State, its implementation may be extended to other domestic ships.

Typology

Ships might be classified based on size, purpose, cargo type and method of propulsion. The main distinction is between cargo ships and passenger ships. In addition, there are other types such as warships, fishing vessels, yachts, tugs and barges not considered in this study. For the purpose of the present study, the following types of cargo and passenger ships are relevant:

1. **Container ships,** which transport cargo in standardised containers. They have a high freeboard which provides some shelter for the wheelhouse from the attack of some types of UAS. Container ships range from small feeders to ultra-large transoceanic ships. They are particularly vulnerable to attacks to their manoeuvring systems because of the effect of the wind on the freeboard.

[9] SOLAS-XI-2 Regulation 2 and Regulation 725/2004 Article 3

[10] Article 4 of Council Directive 98/18/EC on safety rules and standards for passenger ships repealed by Directive 2009/45/EC of the European Parliament and of the Council of 6 May 2009 on safety rules and standards for passenger ships (Recast)

2. **Bulk carriers** which transport raw materials like iron ore, grain and coal in bulk. They are usually large in size with an open deck and low strategic value except those carrying grain in vulnerable food security areas or exporting countries dependent on this crop.

3. **General cargo ships** which carry a variety of packaged goods, including reefer ships for the transport of refrigerated cargo. They are usually small to mid-size with an open deck and low strategic value for being targeted but may have importance for the local economy in some places.

4. **Roll-on/roll-off (Ro-Ro) ships** which transport cargo loaded and unloaded using ramps. They are usually small to mid-size with a relatively closed superstructure. They might be critical to the local economy of some communities, particularly islands.

5. **Liquid bulk carriers** which include tankers and gas carriers. They transport liquids such as oil products, chemicals or liquefied gas and range from small to ultra-large tankers and have open decks and low freeboard. Their criticality depends on the product being transported particularly for gas carriers and chemical tankers. Larger tankers may never operate close to the coastline. An attack on these ships may target damage to trade, the environment or the general population depending on the product transported and location.

6. **Passenger ships** which include cruise ships and ferries transporting passengers and vehicles over short distances. Passenger ships, particularly cruise ships due to their symbolic value, could be a target for terrorist attacks using UAS. Ferries have similarities to Ro-Ro ships with closed upper decks while cruise ships may be an easier target to attack using UAS since they are typically designed with open upper decks for the passengers.

7. **Other Ships** which include different types of ship orientated to specific operations such as research vessels, icebreakers and offshore support vessels. Offshore drilling units could also be included in this category. These ships could be targeted by activist groups due to their symbolic value or to disrupt a particular economic activity (e.g. the oil industry, deep sea mining).

This taxonomy affects the likelihood and the consequences of an attack. Since attacks on persons have a high visibility, media repercussions and societal impact, as a rule of thumb passenger ships may be a more likely target for a terrorist attack and have the higher consequences in terms of human lives and injuries. Furthermore, an attack on a specific business such as the cruise industry could have a significant economic impact. Liquid bulk carriers may have a slightly lower likelihood of a terrorist attack since it would require more knowledge to have a significant impact. However, the consequences of a terrorist attack on, for example, a chemical tanker might be catastrophic due to subsequent effects. In addition, these ships may be an attractive target for activist groups. These considerations will be largely affected by other factors such as the location and timing.

Circumstances such as location and timing which affect the consequences of an attack. For example, a container ship losing manoeuvrability in a strategic area for global traffic may cause worldwide economic disruption as already experienced in the Suez Canal. Similarly, a gas carrier experiencing an attack during loading or discharging operations may have subsequent effects for the adjacent tank farm or even nearby facilities. A chemical tanker attacked in proximity to urban areas could also cause significant distress or even catastrophic effects. Ships sailing through the Red Sea where the likelihood of an attack might be higher. Therefore, the trade of the ship and its operational context should be considered when designing the different attack scenarios.

Vulnerable points on a ship susceptible to UAS attacks are relatively common across all types of cargo and passenger vessels. These vulnerabilities include:

- **Communications systems** (i.e. antennas) might be targeted as part of a broader attack to prevent the transmission of alerts. An attack could be focused on physical damage (i.e. using explosives) or hybrid (i.e. using the UAS to place a device to facilitate a cyberattack).

- **Control and manoeuvring systems** may be disrupted through targeting the bridge or the rudder when the ship has the right draft and trim. The consequences of attacks with explosives at the exterior of the bridge would greatly depend on the type of glass fitted since window fragmentation is one of the main dangers for the crew. In this regard, laminated glass particularly to a minimum standard (e.g. EN 1063 BR6) greatly reduces the vulnerability. On the other hand, an explosion at a critical location may disable the rudder. Nevertheless, the feasibility and consequences of such an attack would highly depend on the specific circumstances. .

- **Structural integrity** is less likely to be compromised by an attack using UAS since it would require a significantly larger drone with a substantial payload of explosives. This scenario involving military grade UAS is outside of the scope of the Regulation. However, a Company Security Officer (CSO) would surely consider this hypothesis in the SSA if the ship operated in certain areas (e.g., the Red Sea). Therefore, the methodology described in this document could cover such a scenario even if the protective measure might be limited to avoid the area at certain security levels.

- **Cargo handling** equipment might be vulnerable to attack particularly during operations. In this case, the type of ship is crucial in determining the vulnerability of such equipment. For example, attacks on cargo manifolds in liquid bulk carriers might have significant consequences, particularly considering the potential subsequent effects. Likewise, gangways on cruise ships during embarkation and disembarkation are significantly vulnerable due to the accumulation of passengers.

- **Open decks** for passengers on cruise ships could be easily targeted by terrorists using UAS with explosives, potentially causing significant injuries and casualties. Additionally, a UAS attack with explosives on the pressure-vacuum valves (P/V valves) in tankers and gas carriers could result in severe consequences.

In general, the damage caused by a UAS attack with explosives depends more on the targeted area of the ship than on the size of the UAS or the payload of explosives. A small well-placed and well-timed charge could have severe impact, while there have been cases of attacks on ships with military-grade drones that caused limited damage. However, this implies a deep understanding of the ship's construction, making the attack more complex and difficult to execute. In this regard, uncrewed surface vessels (USVs) also known as sea drones might be more effective in conducting attacks on manoeuvring systems or to affect the structural integrity of the ship. This risk will be evaluated in future research.

4. RISK ASSESSMENT METHODOLOGY

The primary objective of the security risk assessment is to quantify the risks associated with the different vulnerabilities and assist decision-makers in taking informed decisions on deterrence and mitigation strategies minimising exposure and developing an effective emergency management plan. These vulnerabilities are the intrinsic weaknesses of port facilities and ships that make them susceptible to the consequences of, for example, a terrorist attack. The risk quantification is based on attack scenarios tailored to the assets and their vulnerabilities.

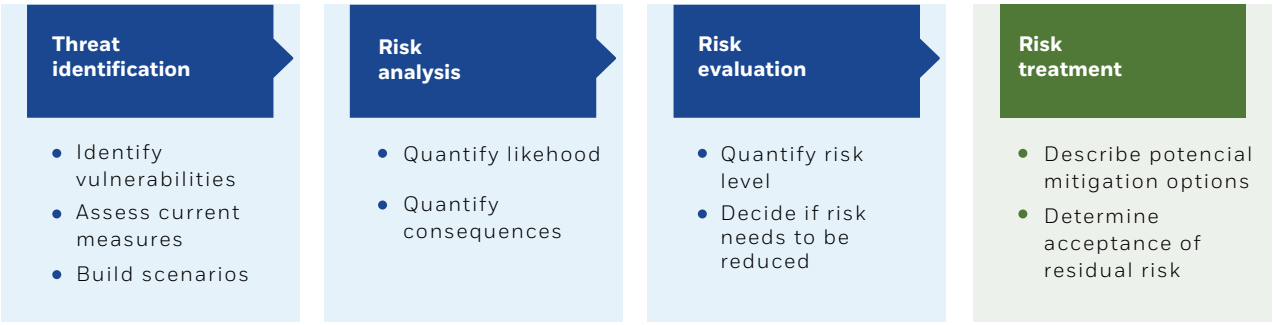
This structured approach to assessing the risks concerning attacks using UAS is based on the generic definition of risk assessment in the International Organization for Standardization (ISO) 31000:2018 standard, "Risk assessment is the overall process of risk identification, risk analysis and risk evaluation" as adapted by the Join Research Centre (JRC) in the technical report "Protection against Unmanned Aircraft Systems. Handbook on UAS risk assessment and principles for physical hardening of buildings and sites". It also complies with the requirements of Regulation (EC) 725/2004[11].

The proposed methodology is specifically designed to assess the risk of the malicious use of UAS to attack port facilities and ships. Nevertheless, its generic approach could be used to assess attack scenarios originating from other human-induced events. While this methodology shares similarities with those used to quantify safety risks, it differs on estimating the likelihood of infrequent human-induced events and quantifying the consequences to the human/social domain. Whilst historical data on safety risk assessments can be used to define likelihood, this is impossible when attack scenarios depend on human decisions and the consequences are intentionally severe.

The implementation of the proposed methodology is, to some extent, subjective. Usually, there is insufficient data to quantify the likelihood of the attack scenario and the resulting consequences; therefore, a qualitative approach should be adopted. Consequently, the result of the risk assessment may differ depending on the background, experience and goals of the person performing the assessment. To reduce bias, the people conducting the assessment should possess expertise in security risk assessments, have no conflicts of interest and should maintain impartiality. According to the Regulation, the CSO is responsible for conducting the security risk assessment for ships while the National Administration must do it for PFs. This responsibility might be delegated to a specialised company in the case of ships or to a recognised security organisation (RSO) for PFs. In addition, particularly for PFs, other stakeholders could be involved to expand the fields of expertise available and enable consensual results. If not already involved in the risk assessment process, the results can then be communicated to the owners/operators of the PF (i.e. Port Facility Security Officer (PFSO) or ship managers (i.e. CSO).

[11] Regulation 725/2004 Annex II Part A 8.4 (Ships) and 15.5 (Port Facilities).

The following figure shows the stages that comprise the risk-assessment process.



1. **Threat identification** involves identifying which potential actors, means and methods of attack could be employed against a ship or PF. This also include the assets that might require protection or potential targets in the PF or on the ship. Finally, it should assess any existing protective measures and identify vulnerabilities. The outcome is the development of attack scenarios specific to the infrastructure's unique circumstances at that moment.

2. **Risk analysis** includes quantifying the likelihood and potential consequences of the occurrence of each identified attack scenario.

3. **Risk evaluation** includes quantifying the level of risk for each attack scenario based on the values determined in the previous step and deciding whether they are acceptable or not.

4. **Risk treatment** includes describing and, if deemed appropriate, selecting potential measures to reduce the likelihood and/or minimise the potential consequences of the assessed risk. This stage also determines whether the residual risk is acceptable. The resulting measures should be defined for each of the three security levels established by the competent authority.

Each of these stages is explained in detail in the following subsections.

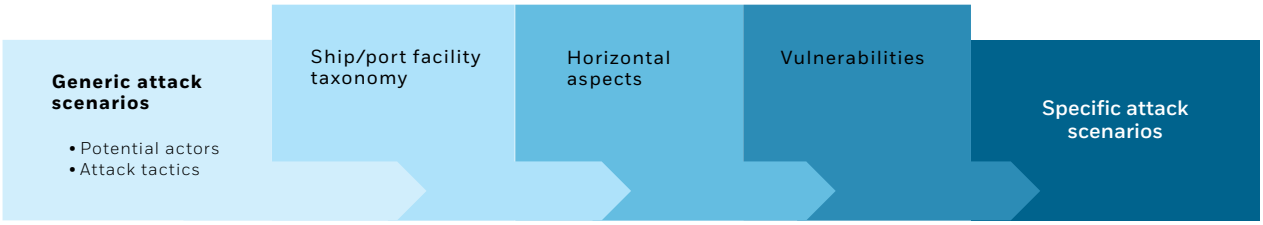
4.1. THREAT IDENTIFICATION

The first step in the risk assessment process is to identify the assets and operations that might require protection and the relevant threats associated with them. This requires an on-site survey involving personnel familiar with the operations. The use of drawings, maps and geographic information systems is highly recommended to locate these assets and their access points. When assessing threats involving the use of UAS, the use of 3-D models can be beneficial in accounting for surrounding areas, potential UAS launch locations and approach routes, and physical vulnerabilities.

A threat is directed at a specific target, in this case a PF or a ship. Identifying the threats applicable to each type of PF or ship can be challenging due to the scarcity of available data. Data related to man-made threats, contrary to natural hazards, are limited. Therefore, a certain degree of subjectivity is usually involved when trying to link a specific threat to a potential target. Data relating to current and emerging threats, the intent of an attack and other related sensitive information may be requested from intelligence services and law enforcement units. Various commercial data providers may also have such information[12], but the quantity and quality of this data is not always guaranteed, especially at the local level.

To implement this methodology, generic attack scenarios are developed considering the potential actors and their tactics for an attack. These scenarios are tailored to the characteristics, assets and vulnerabilities of the different types of PF or ship as well as the existing measures in place. Attack scenarios are developed to consider these vulnerabilities in a practical context using reasonable assumptions. As shown in the figure, these generic scenarios are adapted into specific attack scenarios by the end users, who consider the unique circumstances, existing measures and the vulnerabilities of the infrastructure at the time of the assessment. Finally, these specific attack scenarios should also consider horizontal aspects that might affect other factors such as the designation as critical infrastructure, associated symbolic value or level of automation among others.

Attack scenarios should be plausible, specific and presented in a clear, schematic structure that facilitates educated decisions on any potential actions that are required. They should be presented in a concise and easy to understand manner.



Vulnerabilities to consider in the development of the specific attack scenarios

Vulnerabilities are inherent weaknesses in potential targets that may render them susceptible to the consequences of an attack. The following aspects should be considered to develop specific attack scenarios:

Location and surrounding area. The location and surroundings of a PF or ship can significantly impact its vulnerability to an attack. For ships, the location and surrounding area may change constantly due to their trading area, requiring different scenarios for various situations such as under navigation, both in normal circumstances and in sensitive areas (e.g. canals, straits) and when stationary, either alongside or at anchor. For PFs some factors to consider are surrounding obstacles (e.g. trees, antennas), surrounding areas (e.g. buildings, forest, open spaces) and existing no-fly zones.

Operational liabilities. The types of ship/PF and the way they interface can create vulnerabilities that should be considered. For example, liquid bulk operations are focused on a single point (the loading arm), whereas passenger operations require waiting areas with high densities of people at certain times.

[12] European Union Agency for Law Enforcement Cooperation's annual European Union terrorism situation and trend report EU Terrorism Situation & Trend Report (TE-SAT) | Europol (europa.eu)
Global Terrorism Database https://www.start.umd.edu/
UAS incident tracker https://d-fendsolutions.com/drone-incident-tracker/

Characteristics and location of assets that may need to be protected within a PF. The characteristics and exposure of assets that may need to be protected (e.g. loading arms, piping, antennas, storage tanks, data centres, cranes, passengers waiting areas) should be considered.

Examples of vulnerabilities to consider.

Specific attack scenarios should be developed taking in account any vulnerabilities in the existing security measures that could be exploited to perpetrate an attack. Some examples include:

1. **Exposed facilities:** Traditional security measures might be focused on controlling access at ground level. However, the use of UAS introduces a 3rd dimension allowing access to vulnerable areas, such as roofs with ventilation or air conditioning intakes, telecommunication antennas, electricity grids and other sensitive elements.

2. **People accumulation and flow:** Areas where people congregate, such as waiting areas should be taken into account as they may be targeted by an attack.

3. **Surrounding obstacles:** Gaps between trees or architectural elements providing a line of sight and easy access for a UAS should be considered as potential vulnerabilities for attack scenarios using UAS.

4. **Surrounding areas:** The potential take-off locations should be identified to develop the specific attack scenarios. In some cases, surrounding areas might be particularly exposed to the use of recreational UAS (e.g. beaches, parks) making it difficult to differentiate between hostile and non-hostile activities.

5. **Structural characteristics:** Certain materials (e.g. glass) that may cause injuries in case of an explosion may be considered a vulnerability, particularly in areas where people transit or gather. In addition, the presence of structural elements that may absorb, reflect and channel the shockwave from an explosion amplifying its effects and damage needs to be taken into account. For example, reflected blast waves are more harmful to the human body than the initial overpressure if the person is standing next to a wall. As a result, the injuries and victims of an explosion in an enclosed space are likely to be significantly higher than in an open space.

6. **Inadequate security technology:** Relying on outdated or insufficient security technology may allow vulnerable points. Investing in modern, integrated security solutions that consider current threats is necessary for effective monitoring and response.

7. **Organisational vulnerabilities:** Vulnerabilities in organisational procedures, such as the lack of response procedures to certain threats, the absence of management at certain times, gaps in the warning system, the absence of a cybersecurity plan, can be identified during drills and exercises and introduced into the specific attack scenarios to evaluate their impact.

8. **Lack of security awareness and training:** Port personnel play a crucial role in detecting threats. Insufficient security awareness and training can lead to failure in detecting, responding and reporting suspicious activities. Therefore, it is important to include UAS driven threats in training and exercises.

9. **Corruption and insider threats:** Corruption and insider threats from port personnel can facilitate the circumvention of existing security measures facilitating illicit activities such as theft and smuggling. Internal threats can be particularly damaging, especially those linked to terrorism and radicalisation. Implementing proper vetting, training and monitoring of personnel can help mitigate these risks.

Horizontal aspects to consider in the development of specific attack scenarios

The security risk assessment should take into consideration several horizontal aspects that affect the definition of attack scenarios. A non-exhaustive list of these horizontal aspects includes:

Critical maritime infrastructure

A PF or a shipping service might be essential for the functioning of a community or the economy at a regional, national or international level. This criticality can be down to the PF's importance or the dependency of critical infrastructure on it. Critical maritime infrastructures may be high complex and interdependent. Therefore, their protection needs to be based not only individual elements but the whole system with all associated elements. For example, a power plant which was considered critical infrastructure would not be properly protected if the associated PF where the fuel was received was not also protected as critical infrastructure.

The incapacitation or destruction of critical maritime infrastructure can have a debilitating impact on security, economic security, public health and safety. Therefore, they require special protection for national security. Some of the indicators to quantify this include the handling of essential goods (e.g. energy, food), a lack of redundancy (e.g. a single PF on an island), strategic location (e.g. a PF at a location that could block the entrance to a port, a ship trading in a location that could block infrastructure relevant to international trade) or their significance to a critical system or network (e.g. a PF supporting an essential industry). Some examples of critical maritime infrastructure are a PF handling a significant percentage of the country's liquefied natural gas exports, the only RO-RO terminal ensuring food security on an island, or the only PF exporting essential goods for the car industry, crucial to the local economy.

Attack scenarios involving critical infrastructure should be focused on attack tactics that may affect this criticality (e.g. sabotage). The security risk assessment should consider how the different attack scenarios might result in the incapacitation or destruction of the infrastructure and the consequences for security, economic security, public health and safety. This aspect affects both the consequences and the likelihood of such a potential attack, since critical infrastructure is a more likely target. Therefore, this factor will be introduced in the quantification of the likelihood of an attack, as part of the motivation for it in the next subsection. Finally, it is worth noting that ports considered critical maritime infrastructure are also subject to other legislative requirements[13].

Level of automation and connectivity

Port facilities are becoming increasingly automated to enhance efficiency, safety and productivity. This automation is being implemented in cargo handling equipment (e.g. automated trucks and staking cranes in container terminals) and terminal control systems to manage workflow, scheduling and real-time monitoring. The automation of PFs relies heavily on connectivity and data integration.

[13]Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/ECa

Highly automated systems require protection from physical interference and cyberattacks. Attack scenarios should consider the disruptive consequences of attacks to these systems and the inherent vulnerabilities.

Subsequent effects

Attacks against certain infrastructures may result in **subsequent effects** (e.g. the release of a toxic cloud from chemical plants, further explosions from gas storage tanks). Attack scenarios should consider these effects taking into account the potential conditions at the time of an attack (e.g. prevailing winds moving or dispersing a toxic cloud). This aspect should also be considered in the quantification of the likelihood (motivation factor) and the consequences of the attack.

Symbolic value

Symbolic value refers to the intangible significance or importance of a PF or ship beyond its functional purpose. When assessing the symbolic value of the examined assets, aspects to consider may be cultural, social, historical, psychological or emotional. The symbolic value can be derived from society's perception of the asset being targeted and from the perspective of the attackers. For example, the ownership or flag of a ship could make it a more symbolic target for attack by certain actors (e.g. an Israeli owned ship in the context of regional conflict). This value should also be applied to the PF where such ships operate. In the development of attack scenarios, this aspect affects who the attackers are (terrorists and social groups) and their tactics. In the risk analysis, symbolic value makes a PF or ship a more likely target. Therefore, this aspect is quantified within the motivation factor when quantifying the likelihood of an attack.

Presentation of attack scenarios

The following tables are examples of how to present potential attack scenarios. Once generic attack scenarios relevant to a PF or ship are defined, specific attack scenarios are established for each one. The generic attack scenarios should consider horizontal factors such as critical infrastructure, automation, subsequent effects and symbolic value. For example, only critical infrastructures that would suffer from extreme subsequential effects or with symbolic value should consider terrorist attack scenarios. Those generic scenarios are then adapted to be specific to each PF or ship considering their particularities such as potential take-off locations, frequency and time of the operations, etc.

Generic Scenarios	Actor	Tactic	Comments
1.			
2.			
3.			

Specific Scenario	Asset	Existing measures	Existing vulnerabilities	Circumstances (time & operation)	Attack
1.A					
1.B					
2.A					

4.2. RISK ANALYSIS

In this stage, the objective is to quantify the risk for each scenario enabling decision-makers to determine whether the risk is acceptable or security measures are needed to mitigate it. As it is usually impossible to eliminate risks entirely, the goal is to reduce them to tolerable levels by implementing adequate measures to reduce the likelihood of occurrence or minimise the potential consequences. It is important to realise that risk assessments are a snapshot of the situation at a specific point in time. As circumstances change so does the assessment. Therefore, the risk assessment should be periodically revised and reviewed as required to confirm its validity.

The risk analysis process is a combination of the **likelihood** and **consequences** of each attack scenario.

4.2.1. LIKELIHOOD

For each attack scenario, it is essential to quantify the likelihood of its occurrence. This likelihood depends on the threat level. Ideally, a precise evaluation from intelligence services or relevant authorities would be provided to define the threat level. However, since such information is not always available, an alternative method is needed to assist stakeholders to quantify the likelihood. For PFs and ships the competent authority defines the security level (1 to 3) as established by the Regulation and the ISPS Code[14]. However, this is a generic level of awareness and definition of security measures and does not provide specific information on the likelihood of a specific attack scenario in the context of this risk assessment. Therefore, the likelihood should be defined by considering other factors. For each scenario the likelihood is quantified using the **vulnerability assessment** and **the threat rating.**

[14] Regulation 725/2004 Annex II Part A 4.1 […] *Higher security levels indicate greater likelihood of occurrence of a security incident […] and Regulation725/2004 Annex II Part A 2.1*

9 Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

10 Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

11 Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

Vulnerability rating

As already mentioned, during the development of specific attack scenarios, vulnerabilities are the inherent weaknesses of potential targets that may render them susceptible to the consequences of an attack. The efficiency and effectiveness of existing measures affects the likelihood of an attack. Therefore, at this stage, the vulnerability rating is directly linked to the presence, absence or effectiveness of existing security measures. Any existing protective measures and procedures included in the current Port Facility Security Plan (PFSP) or Ship Security Plan (SSP) should be considered at this stage (e.g. entry checks, video surveillance, UAS detection and identification equipment, security guards, perimeter physical protection, interception measures, personnel training and qualification etc.). These measures must be identified and appraised. Some of the elements that should be considered while evaluating existing measures include technical requirements, compliance with manufacturer's operational requirements, procedures for equipment maintenance and operation, training and potential insider threats. Ultimately, the final results of the risk assessment will determine whether these measures are sufficient or require improvement.

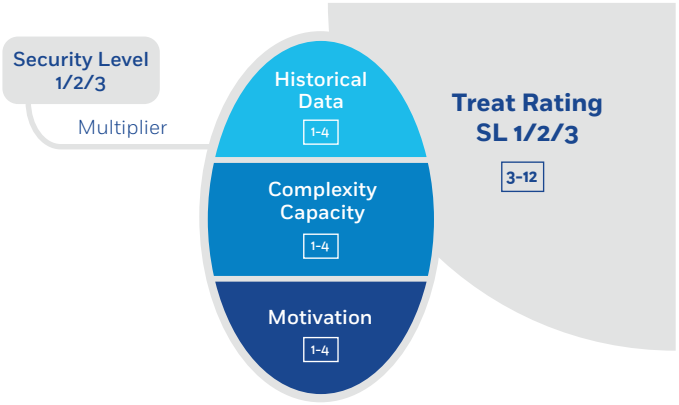
The results of the vulnerability assessment may be visualised in the form of a rating system as presented below.

Vulnerability Rating	Description
Very low	A variety of protective measures (e.g., detection, mitigation, interception) are present, providing sufficient protection against the examined attack scenario.
Low	Several protective measures (e.g., detection, mitigation, interception) are present, though some weaknesses have been identified that may be exploited by an aggressor using the examined attack scenario.
Medium	Some protective measures (e.g., detection, mitigation, interception) are present, though considerable (e.g., lower protection than anticipated) weaknesses have been identified that may be exploited by an aggressor using the examined attack scenario.
High	Existing protective measures (e.g., detection, mitigation, interception) are insufficient (e.g., ineffective systems) and aggressors may easily exploit the identified weaknesses.
Very high	Protective measures (e.g., detection, mitigation, interception) are either missing or are highly insufficient (e.g., completely ineffective systems) and aggressors may very easily exploit the identified weaknesses

For each attack scenario, the results of the vulnerability assessment should be combined with the threat rating described in the next section to determine the relative likelihood.

The threat rating is a combination of three independent indicators (threat history, attack complexity/capability and attractiveness/motivation). Each indicator is rated on a four-level scale. The total score ranging from 3 to 12, defines the relative threat rating as shown in the figure.

In addition, to fulfil the requirements of the Regulation, the results of the assessment should address measures for the three security levels defined by the national authority. To achieve this, a multiplier is introduced for each security level which affects the likelihood and consequently the risk evaluation. Therefore, the subsequent measures to mitigate the risk, if needed, would be defined for each security level.



Threat history considers previous successful or failed attacks, as well as threats and statements made by the actors about potential targets. It is specific for each location, tactic and target typology. However, it is important to be cautious when using open-source databases, as they may lead to an overestimation of risk and subsequently the employment of excessive security measures.

Rate	1	2	3	4
Threat history	• Threats at international level • No previous international incident	• Threats at national level • Past international incident	• General threats at local level • Past national security incident	• Concrete threats at local level • Past local security incident

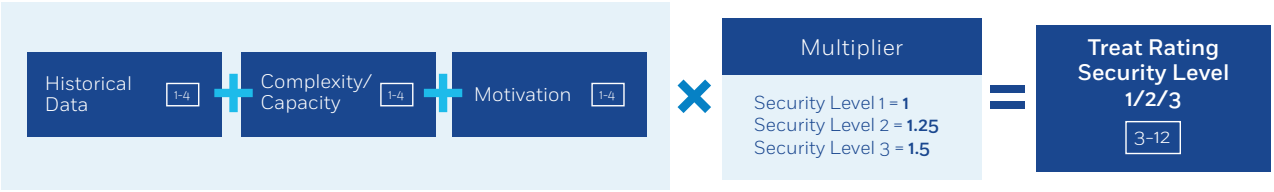
Attack complexity/capability estimates how easy or difficult it is to carry out the attack considering the technical, financial and operative resources required for each scenario in relation to the capabilities of potential actors. It considers a combination of three factors: practical/technical expertise including knowledge of the target, UAS acquisition/utilisation (this factor is specified in a table in section 2.2 of the UAS typology) and obtaining/manufacturing the weapon or its components.

Rate	1	2	3	4
Attack complexity capability	• Advanced expertise required • Very difficult to produce/acquire weapon • High cost of materials • Great number of resources required	• Medium expertise required • Difficult to produce weapon • Relatively high cost of materials • Significant number of resources required	• Low expertise required • Easy to produce weapon • Low cost of materials • Small number of resources required	• No expertise required • Readily available weapon • Very low cost of materials • Minimum number of resources required

Attractiveness/motivation depends on the perceived value or importance of the target to the actor (e.g. cultural/religious/symbolic significance, number of people present). This factor should also consider the potential impact of a successful attack (e.g. disruption of critical infrastructure, subsequent effects, interdependencies with other facilities, collateral consequences for the state and society, public and/or sensitive data breach).

Rate	1	2	3	4
Attractiveness /Motivation	• Insignificant impact at national level • Very small potential collateral damage • Unattractive target	• Some impact at national level in the event of an attack • Low potential collateral damage (e.g., adjacent facilities) • Low target attractiveness	• Significant impact at national level in the event of an attack • Moderate potential collateral damage (e.g., adjacent facilities) • Attractive target	• Very big impact at national level in the event of an attack • High potential collateral damage (e.g., adjacent facilities) • Very attractive target

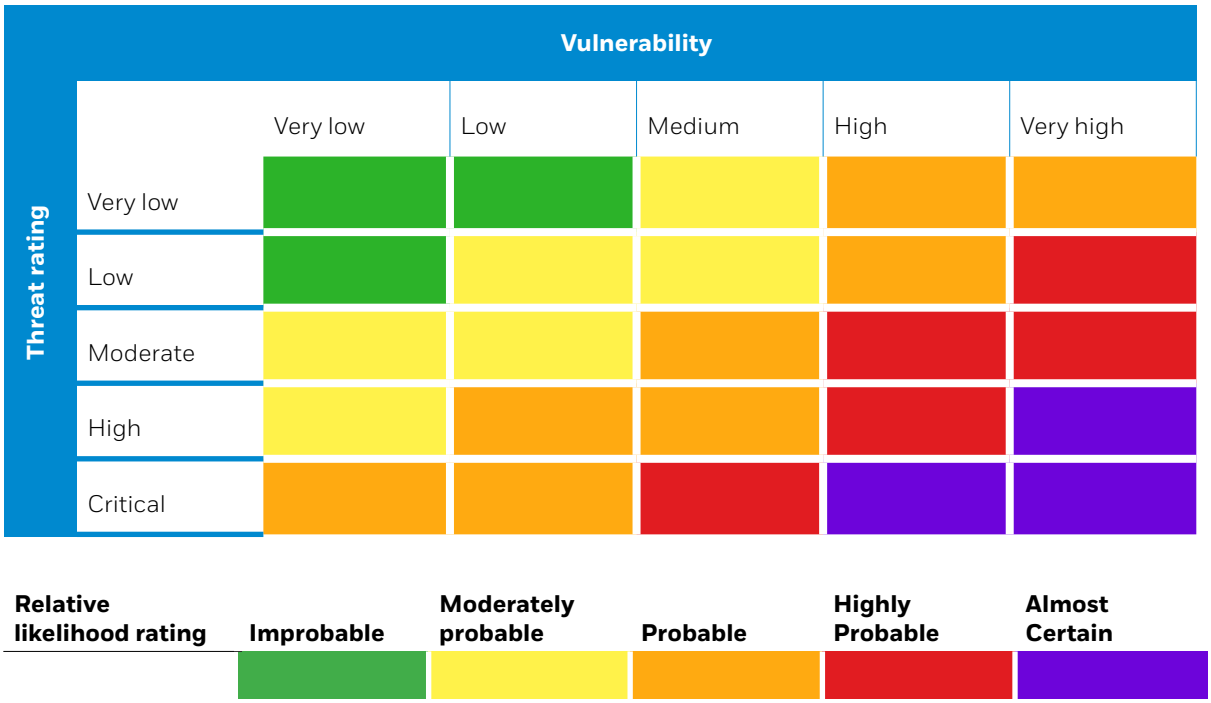
Once the values of the three independent factors have been defined, the **security level multiplier** is applied to the total score. This multiplier is used to adjust the threat rating based on the current security level, with security level 1 as the baseline. To consider the increased likelihood of an attack, at higher security levels a conditional probability is applied. Specifically, the threat rating is increased by 25% at security level 2 and 50% at security level 3. In practical terms, this increase is introduced by applying a multiplier to the threat rating (1.25x at security level 2 and 1.5x at security level 3): decimals should be rounded up to the nearest whole number. The maximum threat rated is capped at 12, regardless of the effect the multiplier. Thus, any resulting value of 11 or more is considered critical. This adjustment may result in underscoring threats at level 2 and particularly at level 3. Therefore, it is recommended that additional countermeasures are always taken at level 3, particularly for those threats with a higher score.



The result is a threat rating score ranging from 3 to 12 for each of the three security levels.

Threat rating	Very Low	Low	Moderate	High	Critical
Total score	3-4	5-6	7-8	9-10	11-12

The relative likelihood of an attack is determined by combining the **vulnerability and threat rating** as shown in the table.



This result will be combined with the potential consequences rating of the attack to complete the risk evaluation for each attack scenario.

4.2.2. CONSEQUENCES

Evaluating the consequences of an attack scenario requires a deep knowledge of the different threats and targets. Consequences depend on the definition of the threat (actor and attack tactic), the characteristics of the target and the conditions at the time of the attack. When selecting these conditions, it is essential to consider the reasonable worst-case scenario for each type of threat. Consequences range from the effect on human life and the environment to economic and political/social impacts. These effects may be immediate or long-term, direct or indirect. While the quantification of some consequences is relatively straight forward (e.g. fatalities) others may be more subjective (e.g. the effect on the population's psychology, reputational impact). To accurately quantify these consequences, it is important to involve relevant stakeholders since they may have a better understanding of the different aspects that affect them.

This quantification may require a specialised knowledge of the threat, such as understanding the consequences for attack scenarios of improvised explosive device (IED) attacks, including blast and fragmentation. The blast has two phases: shockwave and rarefaction wave which is the area of low relative pressure following a shockwave. There are several tools to estimate the effects of explosives[15]. However, these tools are simplifications that do not consider the complexity of the location and surrounding structures. Therefore, it is recommended to involve experts from relevant fields (e.g. law-enforcement, military), to provide a more comprehensive evaluation.

[15] https://counterterrorism.ec.europa.eu/

Considering the subjectivity and technical complexity of some effects it is advisable to evaluate the consequences in a workshop setting, involving stakeholders and experts with knowledge of the threats being considered. This evaluation does not need to be performed for each ship and PF but at a national/ regional level with the results then adapted to the local circumstances.

When quantifying the consequences of an attack some of the aspects to be considered include:

- Human impact: people injured or killed.
- Infrastructure damage: cost and duration of repairs, availability of replacements.
- Disruption of services: duration, availability of backups, cost of repairs.
- Criticality and sensitivity: utilities and information.
- Potential cascading effects.
- Political or reputational damage.
- Indirect economic costs.
- Implications to population's psychology.

In order to facilitate the quantification of the consequences, a severity-based point system is employed, where each of the six indicators is assigned a score encompassing the magnitude of the resulting impact, so that the severer the consequences the higher the score. To determine the consequences rating for each individual scenario, the points assigned to the individual indicators are added together and compared with the scale provided in the table.

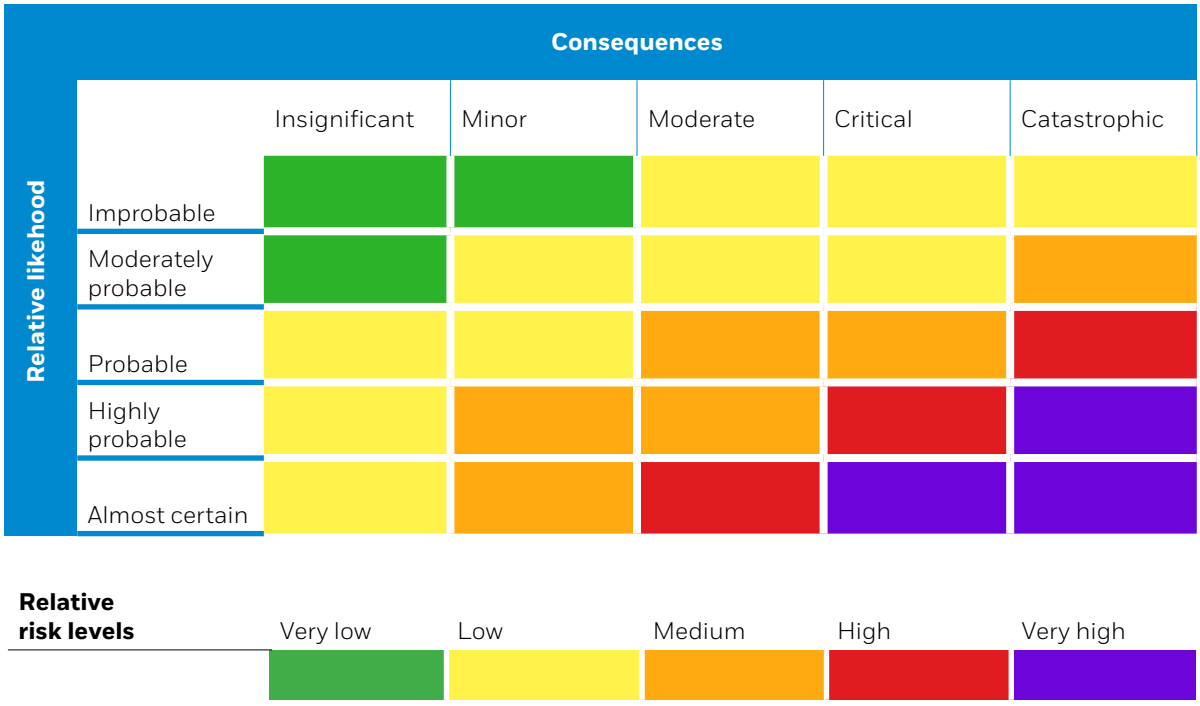
The results of the consequence quantification should be categorised into a 5-level factor as shown in the table, considering that the points for human injuries should be counted twice.

Consequences Indicators						
Human injuries (2x)	**Operation disruption**	**Reputation**	**Material damage**	**Economic**	**Information/ data**	**Points**
Insignificant injuries	Minor disruption	Very small reputational damage (internal)	Minor material damages	Insignificant economic impact (<15.000€)	Intrusion in the IT systems without apparent data leakage	**1**
Serious injuries (no life loss)	Short-term disruption of services	Small reputational damage (Port level)	Moderate material damage (does not pose an immediate danger to PF's installations or ship's structure or stability)	Limited economic impact (<150.000€)	Some data leakage (non-sensitive)	**2**
Serious injuries and limited loss of life	Medium-term disruption of services	Significant reputational damage (local level)	Substantial material damage (to PF's installations or ship without affecting structure or stability)	Considerable economic impact (<1.500.000€)	Significant data leakage (sensitive personal and/or confidential information)	**3**
Serious injuries and significant loss of life	Long-term disruption of services requiring immediate corrective actions	Extensive reputational damage (National level)	Extensive material damage requiring immediate intervention (affecting ship's structure and stability)	High economic impact (<3.000.000€)	IT systems blocked (e.g., ransomware)	**4**
Serious injuries and extensive loss of life	Total loss of services and unacceptable long-term disruption	Extensive eputational damage/ political consequences (EU and international level)	Catastrophic damage to the PF or total loss of the ship	Very high economic impact (>3.000.000€)	Attacks affects IT/ OT systems impacting operations	**5**

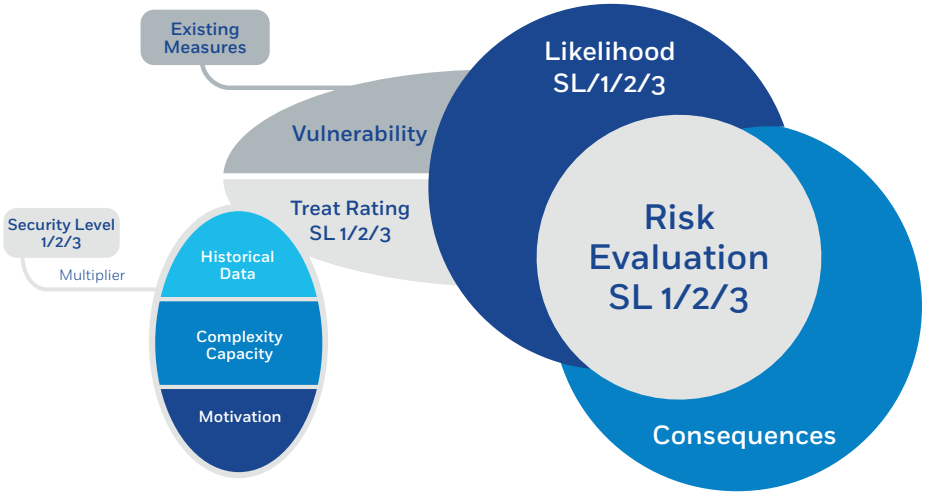
Total score	**<10**	**11-15**	**16-20**	**21-25**	**> 26**
Consequences	Insignificant	Minor	Moderate	Critical	Catastrophic

4.3. EVALUATION OF RISK

The evaluation of risk is the combination of the previous stages, combining the results to produce a 5-level risk assessment with three variants corresponding to the three security levels. For example, a risk may be classified as low at security level 1, medium at level 2 and high at level 3. This distinction is crucial as different mitigation measures may need to be implemented at each security level.



The following graphic aggregates the various factors and stages discussed above within a comprehensive risk analysis and evaluation framework.



4.4. TREATMENT OF RISK

Once the risk has been evaluated as part of the PFSA or SSA, the PF or ship managers in coordination with the national authority or flag administration respectively, should decide the acceptable level of risk. Risks that exceed this threshold will require counter measures to reduce their likelihood or mitigate the consequences.

For PFs, the risk analysis conducted by the national administration, or at least approved by it if the task has been delegated to an RSO, should be properly communicated to the PF's managers. Clear instructions should be provided to facilitate the interpretation of the results, including explanations to highlight the degree of uncertainty associated with them. The measures to mitigate the risk as established by the PF should be included in the PFSP, which will subsequently be approved by the national authority. Therefore, it is advisable that these measures are consensual and adopted through a process involving open communication among stakeholders.

Similarly, the CSO should reflect the risk evaluation in the SSA. Subsequent measures should be reflected in the SSP, which must be approved by the flag State administration or by an RSO on its behalf. Therefore, it is advisable that the flag State provides the CSOs with a sound methodology and reliable information to ensure a consistent approach across the fleet.

It is particularly difficult to establish an acceptable level of risk. A threshold to identify risks requiring attention should be established previously to the assessment. Therefore, national authorities and flag State administrations should provide clear instructions in this respect based on the available intelligence. The case scenarios at the end of this document provide some examples of the types of instruction for acceptable thresholds.

5. MEASURES

When measures are required to treat the risk, they focus on reducing the likelihood and/or mitigating the consequences. These security measures may be categorised into three main types: detection, active measures and passive measures. They may also be electronic (soft-kill) or physical/kinetic (hard-kill). These countermeasures, also known as effectors, are based on the UAS functions and technical characteristics. The combination of detection and countermeasures is usually referred to as an anti-drone system which may be fixed or mobile.

The first step in addressing UAS threats is **detection** and identification of those that pose a threat to a PF or ship. This can be achieved using various sensors, including radar, acoustic and optical sensors which may be supported by artificial intelligence (AI) processing and radio frequency (RF) analysers together with direction finders. Optical sensors include ultra long-range high-resolution cameras and multi-spectral cameras operating on the visible and thermal range. RF analysers also include cyber software defined radio (SDR) detection, which extracts GPS data from communication transmissions. A ship's radar may be able to detect larger UAS to some extent.

These detection systems have limitations. Acoustic sensors are only effective at close range while optical sensors may have blind spots. Radar systems do not work well with low-flying UAS and may mistakenly identify birds, making the use of micro-Doppler effects necessary to differentiate targets. Some UAS are preprogramed, thereby eliminating detectable RF communications. RF detection relies on the quality and update of the RF library and may not always be effective in detecting drones controlled over 5G networks. In some cases, a combination of detection methods might be necessary to overcome individual limitations.

Visual identification is also a valid detection measure particularly during daylight. Some UAS used to attack merchant ships (i.e. Shahed models) make a distinct noise allowing for acoustic detection. This implies procedures that allow personnel to identify them and raise the alarm, and the adequate training and exercising of such procedures.

Active countermeasures include jammers that disrupt communication or GNSS signals. As well as Directed Energy Weapons (DEWs) using highly focused radiation such as lasers, microwaves or particle beams. In this category electromagnetic pulse (EMP) and intentional electromagnetic interference (IEMI) might also be included. In addition, cyber hacking SDR on a flight can be used to take control of UAS, often used in combination with cyber SDR detection (packet analyser or 'sniffer'). Physical or kinetic solutions such us falconry, other UAS, net launchers, water cannons, or anti-aircraft weapons are also available.

However, there are limitations to the use of these active measures. In general, they are expensive, require complex design and installation and extensive training. Most are limited to the military (i.e. anti-aircraft weapons or DEWs) or law enforcement use making them unavailable for private use. In addition, GNSS jammers do not discriminate and affect not only hostile UAS but also other GNSS devises in the surrounding area. RF signal jammers can target communications on 90-degree quadrants for short periods making them more efficient. Lasers are only effective against UAS that are in the line of sight and do not work in rain or heavy fog. SDR hacking relies on the library of radio frequencies used. Moreover, fibre-optic controlled UAS are immune to electronic warfare. Also integrating AI in the control of the drone would allow for targeting autonomy eliminating communication with the operator and limiting the effectiveness of those measures based on radio signals.

The majority of commercially available UAS are manufactured by one company (DJI from China with 70% of the market in 2024) and they operate on a known frequency range that can be hacked. However, hostile UAS can be custom made or manipulated to operate on a different RF, potentially incorporating encrypted controller communications or frequency hopping capabilities. In addition, SDR hacking takes time making

it ineffective against swarms of UAS. Net launchers, whether handheld or vehicle-mounted, only work for low-flying UAS. Additionally, falconry is not only time-consuming to train but also raises concerns about the well-being of the birds of prey involved, making it a questionable activity.

Passive countermeasures against UAS threats include establishing no-fly zones and flight permits. No-fly zones should be coordinated with the relevant authorities, clearly marked, and communicated to stakeholders. No-fly zones through an area-denial service are typically embedded in the off-the-self UAS software. Nevertheless, UAS can be manipulated to evade geofencing making this measure less effective.

Hardening is an effective and practical passive countermeasure, which focuses on making PFs and ships more resilient to UAS attacks. Hardening is a cost-effective, low-tech solution that may be implemented without legal issues or maintenance concerns. Physical hardening involves the integration of security features in the design of new facilities, such as using reinforced construction (particularly windows), blast-resistant design, natural barriers such as plants and green roofs, and other strategies to reduce the impact of explosions. For existing facilities, hardening is achieved through the use of protective barriers like fences, nets and roofs, to increase the distance between the potential UAS detonation point and the vulnerable target. For example, a fence or a net can ensure that the target is out of the direct reach of the UAS, therefore mitigating the consequences of a potential blast. A roof can prevent a direct hit from a grenade or an IED. Additionally, using trees and other obstacles to limit the visibility of line-of-sight piloted UAS can also be considered a form of hardening. The implementation of hardening measures depends on the specific risk being considered. For example, if the attack scenario considers a UAS carrying an 82 mm explosive mortar round and it is decided to use hardening through a net, it should provide a safe distance to the vulnerable target (in this case considering a 14-meter lethal radius and a danger zone due to fragmentation up to 50-100 meters away). If the scenario considers the same explosive being dropped, the measure required to mitigate the risk would be a roof.

Electronic hardening involves the protection against electronic warfare and UAS-driven cyberattacks. Implementing redundancy into communications and control systems can improve resilience to jamming, while securing communications through encryption and authentication for wireless systems reduces their vulnerability to cyberattacks.

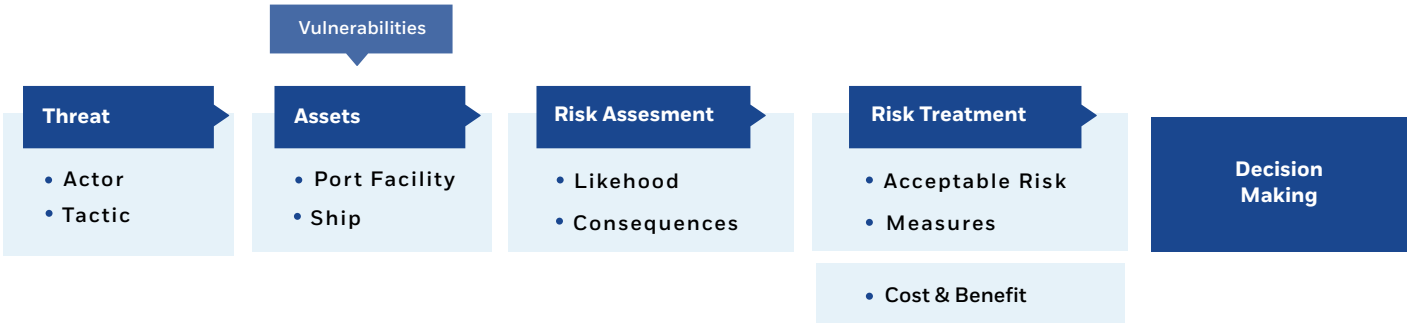
Procedural hardening involves improving procedures and preparedness. Security plans should include response procedures to UAS threats related to a PF or ship. These procedures may include simple tactics such as switching off the AIS to complicate being targeted, avoidance manoeuvres upon imminent impact, or entirely avoiding areas under attack. Training should include information about these threats and response procedures. Drills and exercises can facilitate testing the effectiveness of these procedures. A first step in procedural hardening might be recording and reporting incidents involving UAS as security incidents, including those caused by careless users without criminal intent.

The implementation of measures should consider a cost-benefit analysis. The consequences can be quantified as economic cost with a certain level of likelihood and compared to the cost of implementing the risk treatment measures over a period of time. Some factors that affect the quantification of the consequences are relatively straightforward to assign an economic cost (i.e. material damage, disruption, economic impact) while others may be more difficult (i.e. reputational damage, information/data and human injuries). The IMO Guidelines for Formal Safety Assessment (FSA) provide methodologies to assign economic cost and to conduct cost-benefit analysis. Nevertheless, this approach has limitations. In addition to the challenge to assign a monetary value to these factors, it does not consider the value of the perception of increased security that the implementation of security measures has in the local community.

6. RISK ASSESSMENT IMPLEMENTATION

To comply with the Regulation, the SSA and PFSA should include a description of the assets that may need to be protected, potential threats, the likelihood of their occurrence and the consequences if they do. The evaluation of specific attack scenarios is a practical way to support the decision-making process for establishing security measures to protect a ship or a port facility. Implementing a robust risk assessment methodology provides decision-makers with the necessary information to select effective security measures and discard unnecessary ones.

The following graphic presents the different steps of the process leading to an informed decision-making.



The resulting assessment is a snapshot of the situation at a given time and should be reassessed regularly to integrate newly acquired knowledge, trends and technological developments, as well as changes in circumstances. For PFs, the minimum requirement is to be reassessed at least every five years17. For ships, while there is no explicit frequency requirement, it is advisable to follow the same pattern.

The risk assessment should include an on-site survey to identify assets that might need to be protected, existing measures and vulnerabilities. The survey will serve as the foundation for developing specific attack scenarios. The presentation of the survey, particularly for PFs, should include maps and geographical information systems to locate the assets that might need to be protected and the access points to reach them. These maps should include surrounding areas, potential UAS launch locations and approach routes, and physical vulnerabilities, potentially requiring consideration of three-dimensional aspects. Personnel familiar with the operation and management of the PF or ship should be involved in this survey.

Step 1 – Definition of generic and specific attack scenarios relevant to the case.

The first step in the risk assessment process is to define relevant generic attack scenarios that result from combining actors and attack tactics. The following table shows a list of generic attack scenarios common to port facilities and ships which may not always be relevant to all cases.

Attack tactic	Terrorist groups	Criminal organisations	Activist groups
Transportation of hazardous substances for terrorism and sabotage	✓		
Smuggling	✓	✓	
Intelligence	✓	✓	✓
Cyberattack	✓	✓	✓
Jamming	✓	✓	✓
Disruption	✓		✓
Propaganda	✓		✓

This information can be also presented in the following format to define the generic scenarios.

Generic Scenarios	Actor	Tactic
1.	Terrorist	Transportation of hazardous substances for terrorism and sabotage
2.	Terrorist	Smuggling
3.	Terrorist	Intelligence
4.	Terrorist	Cyberattack
5.	Terrorist	Jamming
6.	Terrorist	Disruption
7.	Terrorist	Propaganda
8.	Criminal organisations	Smuggling
9.	Criminal organisations	Intelligence
10.	Criminal organisations	Cyberattack
11.	Criminal organisations	Jamming
12.	Activist groups	Intelligence
13.	Activist groups	Cyberattack
14.	Activist groups	Jamming
15.	Activist groups	Disruption
16.	Activist groups	Propaganda

The type of PF or ship being assessed determines the actors that should be considered in the risk assessment. Each case should be assessed considering the local context and specific characteristics of the infrastructure. The following tables show a suggested approach for the definition of generic attack scenarios.

Type of PF	Terrorist groups	Criminal organisations	Activist groups
Dry bulk terminals **Break-bulk terminals** **Container terminals** **Ro-Ro terminals**		✓	
Liquid bulk terminals	✓		✓
Passenger terminals	✓		✓

Type of Ship	Terrorist groups	Criminal organisations	Activist groups
Dry bulk terminals **Break-bulk terminals** **Container terminals** **Ro-Ro terminals**		✓	
Liquid bulk terminals	✓		✓
Passenger	✓		✓
Other			✓

The generic attack scenarios that are relevant to the PF or ship being assessed should be further developed into specific attack scenarios considering the assets that might need to be protected, the existing security measures and any vulnerabilities identified during the on-site survey. The specific attack scenarios should also consider the possible knowledge of the attackers of those measures and vulnerabilities since that may greatly influence the impact of the attack. Other circumstances should be considered in the design of the specific attack scenarios, such as potential take-off locations, the time of day which would affect the visibility of the UAS, existing obstacles and the frequency of the operations, etc. The resulting list of specific attack scenarios should be comprehensive but avoid duplication of scenarios that might require a similar risk treatment. Appendix 1 includes examples on how to present specific attack scenarios.

Appendix. Practical examples

The following table shows 2 examples of specific attack scenarios for the generic scenario "Transportation of hazardous substances for terrorist attack and sabotage".

Port Facility - LNG xxxx					
Generic Scenario 1. Transportation of hazardous substances for terrorist attack and sabotage					
Specific Scenarios	Asset	Existing measures	Existing vulnerabilities	Circumstances (time & operation)	Attack
1.A	Loading arm	Unprotected	Only 2 berths with loading arms at the terminal	Ship unloading at night-time. Criticality: Terminal is entry point for 70% of country LNG needs.	Sabotage with hand grenade dropped by medium size VLOS multicopter UAS
1.B	Loading arm	Unprotected	Only 2 berths with loading arms at the terminal	Ship unloading at night-time. Criticality: Terminal is entry point for 70% of country LNG needs.	Sabotage with explo-sives loaded on a medium size FPV OWA multicopter UAS
1.C					

Example 1 – PF

Step 2 - Risk evaluation.

Each specific attack scenario is evaluated following the methodology previously described. This risk evaluation can be conducted in a workshop setting, where the knowledge and expertise of different stakeholders are used to quantify the different factors.

The following table provides an example of how to present the risk assessment for each specific scenario. The facilitator of the workshop may prefill the factors that do not require qualitative assessment, such as the threat rating for the three security levels. The vulnerability assessment, which is based on the study of existing measures, can also be prefilled. The resulting likelihood assessment should be acknowledged and agreed by the workshop participants. Finally, the consequences of each scenario could be determined through collaboration, leveraging the diverse knowledge and expertise of the participants.

Specific scenario 1.A					
Historical data (1-4)	Complexity (1-4)	Motivation (1-4)	Threat Rating SL1 (1-12)	Threat Rating SL2 (1-12)	Threat Rating SL3 (1-12)
2	2	3	7 Moderate	9 (8.75) High	11 (10.5) Critical
Vulnerability (5-levels)			High		
Likelihood (5-levels)			Highly probable	Highly probable	Almost certain
Consequences (5-levels)			Critical		
Risk level (5-levels) SL1/SL2/SL3			High	High	Very high

This evaluation considers the following circumstances:

- There are several types of hand grenade that could potentially be carried by a UAS. A regular grenade weights around 600 gr and could have an impact equivalent to 60 gr. TNT with a lethal radius of 5 meters with casualties up to 15 meters away. Despite grenades being designed as anti-personnel weapons they might cause damage to infrastructure at close range (which in the case of a grenade in the example is approximately 2 meters).

- There are usually two or three staff members present during the connection/disconnection of the loading arm and one additional staff member on standby on-site during operations.

The factors have been evaluated based on the following assumptions:

- **Historical data:** There have been threats at an international level but there have been no incidents.

- **Complexity:** The type of UAS used in the attack is readily available off-the-self and relatively simple to pilot. Obtaining a grenade would require contacts in underground circles that only certain groups have access to. The moment and location of the attack requires knowledge of liquefied gas operations. Therefore, in this case the limiting factors in terms of complexity would be obtaining the grenade and knowing when and where to use it.

- **Motivation:** The attack could have a significant impact at national level if the PF is the main entrance for LNG in the country. The potential damage may be extended to the storage tank and the ship, making it an attractive target for terrorists. However, the country is not involved in regional conflicts.

- **Vulnerability:** Access control measures are in place, and the loading area is considered restricted. Automatic shutdown valves that would prevent the explosion extending to the storage tanks already exist. Ships are also fitted with automatic shutdown valves that would act in case of an explosion. There are existing procedures to respond to an explosion during operations including fire and gas release. Staff are trained to respond to such incidents following these procedures. However, there are no measures or specific training in place to detect UAS or identify hostile approaches. The loading arms are easily accessible from above.

- **Consequences:** The explosion would damage the loading arm that can only be repaired/replaced within one month (from the consequences table the following factors should be scored: material damage 4, economic impact 3 and operation disruption 3). The blast may cause significant damage to the ship's loading equipment. The staff member on standby in the loading area may be killed by fragmentation from the grenade (human injuries 2x3, total 6). The gas supply to the country may be affected causing significant psychological impact on society and financial markets (economic impact rise to 5 and reputation 4). This impact would be temporary with no long-term effects. Total consequences score is 22 (critical).

Step 3 - Definition of security measures and re-evaluation.

A threshold for the acceptable risk should be defined beforehand. Risks exceeding this threshold would necessitate the implementation of appropriate security measures. Following this methodology, decision makers address only those risks that are relevant. Therefore, the security measures implemented are proportional, appropriate and tailored to the specific needs, ultimately providing cost-effective measures that improve the security of the PF or ship. In this case, installing a roof that partially covers the loading arms is considered, so it does not interfere with the operations. A procedure for the staff to raise the alarm in case a UAS is identified is introduced and a training plan established. The procedure also includes security patrols checking an area adjacent to the PF identified as a likely take-off point.

For the evaluation of scenario 1.A. only the resulting risks medium, low and very low were considered acceptable by the evaluators. The installation of a roof covering part of the loading arms would prevent direct blast damage to the equipment and limit the expand of the fragmentation upwards from the location of the PF staff. It should be considered that the explosion on the roof may cause blast and fragmentation that has an impact at the level of the ship's deck potentially causing injuries to crew members and damage to the manifold. In addition, the procedures established to sound the alarm and stop operations in case of a UAS is detected in the vicinity, mitigating the potential consequences. As presented in the table, the re-assessment with the new measures (roof, procedures and training) indicated a reduction in the attack consequences from critical to moderate. These measures would also reduce the vulnerability from medium to low. The resulting relative likelihood rating would be moderately probable at SL1 and SL2 and highly probable at SL3. The resulting risk level would be medium-low at SL1 and SL2. However, at SL3 the risk level would be high exceeding the acceptable threshold. Therefore, at SL3 all operations would be halted as an additional measure. This would reduce the consequences to minor and bring the risk within the acceptable threshold.

Specific scenario 1.A after measures are in place					
Historical data (1-4)	Complexity (1-4)	Motivation (1-4)	Threat Rating SL1 (1-12)	Threat Rating SL2 (1-12)	Threat Rating SL3 (1-12)
2	2	3	7 Moderate	9 (8.75) High	11 (10.5) Critical
Vulnerability (5-levels)			Medium		
Likelihood (5-levels)			Probable	Probable	Highly probable
Consequences (5-levels)			Moderate		
Risk level (5-levels) SL1/SL2/SL3			Medium	Medium	High

The risk assessment for scenario 1.B has similar results. In this case, the type of UAS and attack tactic can be mitigated by establishing a security perimeter around the loading arms through the installation of a net or fence.

Step 4 - Presentation of conclusions.

The conclusions of the risk assessment should provide a clear summary for each of the three security levels, including the initial risk, any required risk treatment and the resulting accepted residual risk. The identified vulnerabilities associated with the examined attack tactic should also be described. The following table is an example of a way to present these conclusions effectively.

Scenario	Security level	Risk level	Risk treatment	Residual acceptable Risk
	SL1	High	Roof, procedures, and training	Medium
	SL2	High	Roof, procedures, and training	Medium
1.A	SL3	Very high	Stop operations	Medium
	SL1	High	Protective net	Medium
	SL2	High	Protective net	Medium
1.B	SL3	Very high	Stop operations	Medium

It is important to highlight that the Regulation explicitly mandates additional security measures at level 2, with further enhancements required at level 3. According to the methodology described, the risks associated with various specific scenarios may exhibit similar levels of quantification across security levels 1 and 2, or levels 2 and 3. Consequently, the countermeasures for these security levels might also be comparable and apparently not fulfilling the requirement identified. However, when considering the overall risk profile encompassing all attack scenarios, the implementation of countermeasures should be proportionally increased in accordance with the security level.

Example 2 – PF

The following table shows an example of specific attack scenario for the generic scenario 'Criminal gang cyberattack'.

Port Facility – Container terminal xxxx					
Generic Scenario 10. Criminal gang cyberattack					
Specific Scenarios	Asset	Existing measures	Existing vulnerabilities	Circumstances (time & operation)	Attack
10.A	Computer system and networks	Cybersecurity plan	Highly automatised. PFSP does not mention risks by UAS	Not relevant PF operating high pace 24/7. The devise can be placed at night.	UAS is used to get access to the WIFI network from the roof of the office building

Specific scenario 10.A					
Historical data (1-4)	Complexity (1-4)	Motivation (1-4)	Threat Rating SL1 (1-12)	Threat Rating SL2 (1-12)	Threat Rating SL3 (1-12)
2	2	2	6 Low	8 (7.5) Moderate	9 High
Vulnerability (5-levels)			Low		
Likelihood (5-levels)			Moderately probable	Moderately probable	Probable
Consequences (5-levels)			Moderate		
Risk level (5-levels) SL1/SL2/SL3			Low	Low	Medium

The existing cybersecurity plan already addresses a similar hybrid attack vector even if not directly associated with a UAS attack. Therefore, the risk assessed for this specific attack scenario is considered acceptable for all three security levels and the treatment of risk is not necessary. Nevertheless, to address other risks identified during the assessment, a procedure for alerting personnel in case UAS are spotted in the area has been included in the PFSP. This procedure would also be included in the staff training. The implementation of these measures does not affect the residual risk which remains within acceptable levels.

Scenario	Security level	Risk level	Risk treatment	Residual acceptable Risk
	SL1	Low	Procedures and training	Low
	SL2	Low	Procedures and training	Low
10.A	SL3	Medium	Procedures and training	Medium

Example 3 – ship

The following table presents an example of specific attack scenario for the generic scenario "Transportation of hazardous substances for terrorist attack and sabotage". As in previous examples, it has been agreed, that only the resulting risks medium, low, and very low are acceptable.

Tanker - xxxx					
Generic Scenario 1. Transportation of hazardous substances for terrorist attack and sabotage					
Specific Scenario	Asset	Existing measures	Existing vulnerabilities	Circumstances	Attack
1.A	Control and manoeuvring	None	Single rudder exposed when draft is low	Lisbon river entrance early morning low draft and low speed (top of rudder bearing out of the water)	Sabotage with explosives transported by a medium FPV OWA multicopter UAS

Specific scenario 1.A					
Historical data (1-4)	Complexity (1-4)	Motivation (1-4)	Threat Rating SL1 (1-12)	Threat Rating SL2 (1-12)	Threat Rating SL3 (1-12)
1	2	2	5 Low	6 (6.25) Low	8 (7.5) Moderate
Vulnerability (5-levels)			High		
Likelihood (5-levels)			Probable	Probable	Highly probable
Consequences (5-levels)			Moderate		
Risk level (5-levels) SL1/SL2/SL3			Medium	Medium	Medium

Considering the acceptable risk, no additional risk treatment is required at any security level. The assumption is that an attack employing this tactic would only disable the manoeuvring of the ship without harm to personnel. The availability of tugboats at Lisbon port would ensure that the ship could be towed away, thereby preventing any disruption to traffic in and out of the port.

Scenario	Security level	Risk level	Risk treatment	Residual acceptable Risk
	SL1	Medium	No needed	Medium
	SL2	Medium	No needed	Medium
1.A	SL3	Medium	No needed	Medium

Example 4 – ship

Cruise Ship - xxxx					
Generic Scenario 1. Transportation of hazardous substances for terrorist attack and sabotage					
Specific Scenario	**Asset**	**Existing measures**	**Existing vulnerabilities**	**Circumstance (time & operation)**	**Attack**
1.A					
1.B	Upper deck with swimming pool	Open without security measures	Israeli citizens commonly among the passengers	Port entrance in a European country	Sabotage with explosives (hand grenade) carried by a medium size FPV multicopter UAS
1.C					

Specific scenario 1.B					
Historical data (1-4)	Complexity (1-4)	Motivation (1-4)	Threat Rating SL1 (1-12)	Threat Rating SL2 (1-12)	Threat Rating SL3 (1-12)
1	2	3	6 Low	8 (7.5) Moderate	9 High
Vulnerability (5-levels)			High		
Likelihood (5-levels)			Probable	Probable	Highly probable
Consequences (5-levels)			Catastrophic		
Risk level (5-levels) SL1/SL2/SL3			High	High	Very high

The evaluation of this risk assumes that the initial shock wave of a hand grenade in a relatively closed pool deck area (metal and glass walls surround the area) would be amplified by wall reflections causing significant blast damage in addition to injuries caused by the fragmentation. The resulting risk requires treatment. As a result, a procedure is introduced restricting access to the pool deck once the ship approaches 10 miles from the nearest land. This creates two scenarios. Scenario 1 where the ship is more than 10 miles from land and an attack would require a large UAS with extended range thereby increasing the complexity of the attack and reducing the treatment rating. The vulnerability would also be decreased. The resulting risk is medium (acceptable) at security levels 1 and 2. However, at security level 3 the resulting risk remains high. Therefore, access to the pool deck should be closed at this level regardless of the position of the ship.

Specific scenario 1.B After measures further than 10 miles from the coast.					
Historical data (1-4)	Complexity (1-4)	Motivation (1-4)	Threat Rating SL1 (1-12)	Threat Rating SL2 (1-12)	Threat Rating SL3 (1-12)
1	1	3	5 Low	6 (6.25) Low	8 (7.5) Moderate
Vulnerability (5-levels)			Medium		
Likelihood (5-levels)			Moderately probable	Moderately probable	Probable
Consequences (5-levels)			Catastrophic		
Risk level (5-levels) SL1/SL2/SL3			Medium	Medium	High

Scenario 2 where the ship is within 10 miles of land presents a reduced risk, as access to the pool deck is already restricted and there would be no passengers or crew on deck, thereby minimising the potential consequences. In this case the motivation and vulnerability associated with an attack would also be reduced. Therefore, the resulting risk is acceptable at all security levels.

Specific scenario 1.B. After measures closer than 10 miles from the coast.					
Historical data (1-4)	Complexity (1-4)	Motivation (1-4)	Threat Rating SL1 (1-12)	Threat Rating SL2 (1-12)	Threat Rating SL3 (1-12)
1	2	2	5 Low	6 (6.25) Low	8 (7.5) Moderate
Vulnerability (5-levels)			Medium		
Likelihood (5-levels)			Moderately probable	Moderately probable	Probable
Consequences (5-levels)			Moderate		
Risk level (5-levels) SL1/SL2/SL3			Low	Low	Medium

The results for the specific scenarios assessed in the example 4 are presented in the following table.

Scenario	Security level	Risk level	Risk treatment	Residual acceptable Risk
	SL1	High	Procedure in place	Medium
	SL2	High	Procedure in place	Medium
1.B.1	SL3	Very high	Pool deck closed	Medium
	SL1	High	Pool deck closed	Low
	SL2	High	Pool deck closed	Low
1.B.2	SL3	Very high	Pool deck closed	Medium

ABOUT THE EUROPEAN MARITIME SAFETY AGENCY

The European Maritime Safety Agency is one of the European Union's decentralised agencies. Based in Lisbon, the Agency provides technical assistance and support to the European Commission and Member States in the development and implementation of EU legislation on maritime safety, pollution by ships and maritime security. It has also been given operational tasks in the field of oil pollution response, vessel monitoring and in long-range identification and tracking of vessels.

European Maritime Safety Agency
Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu

EMSA