TERMA
ALLIES IN INNOVATION

Terma White Paper - Offshore wind farm security concept

April 2026

Terma White Paper – Offshore wind farm security concept

Published in April 2026

TERMA

ALLIES IN INNOVATION

ABOUT THE AUTHOR:

TERMA
ALLIES IN INNOVATION

Terma A/S

Terma A/S is an internationally recognised provider of advanced surveillance and security solutions for the protection of critical infrastructure, civilian authorities and defence stakeholders for mitigation, safety and operational purposes. With decades of operational experience in complex air and maritime domains, Terma delivers mature sensor and system technologies that enhance situational awareness, support rapid decision-making and enable effective cooperation with national authorities. Terma is a WindEurope member and, for the WindEurope policy paper, has shared its technological expertise, operational insight and practical system-design experience for layered physical security in offshore environments through a technical white paper.

TEXT AND ANALYSIS:

Christian Heidemann Ladefoged, *Director, Commercial Insights (Terma)*
Lars Nørregaard, *Senior Solution Engineer (Terma)*
Jesper Tolstrup, *Chief Specialist, Radar (Terma)*
Henrik Bendix Nielsen, *Senior Sales Manager (Terma)*

MORE INFORMATION:

https://itl.ink/terma-white-paper-owfsc

DISCLAIMER

This publication contains opinions collated from discussions with WindEurope members, partners and other organisations. Neither WindEurope nor its members or partners, nor their related entities or other organisations are, by means of this publication, rendering professional advice or services. Neither WindEurope nor its members or partners shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

The technical concepts referenced in this publication, including those set out in the Terma White Paper, are illustrative in nature and do not constitute a WindEurope-endorsed security standard, minimum requirement or prescribed solution. They represent one possible approach among several for structuring layered, civilian physical security measures for offshore wind infrastructure. Terma is a WindEurope member company and developed its technical paper independently. The illustrative concept forms the analytical basis for the indicative cost calculations used in the policy paper to qualify and quantify potential financial implications under defined assumptions. These figures are intended solely to inform discussions on proportionality, governance and funding frameworks and should not be interpreted as binding requirements.

Contents

1. Reference document - Terma White Paper 5

1.1 Introduction to offshore wind farm security concept 5
1.2 Detect, classify, report and act 5
1.3 Security zones 6
1.4 Methodological framework 8
1.5 Air domain 8
1.6 Surface and ground domain 8
1.7 Subsea domain 9
1.8 Seabed domain 9
1.9 Technologies and sensors to achieve situational awareness 9
1.10 Considerations regarding sensors 11

2. The functional chain in a security solution 15

3. Use cases 19

3.1 Use case 1 – 500 MW wind farm in the Mediterranean 20
3.2 Use case 2 – 1.5 GW wind farm in the Baltic or North sea 22

4. Annexes 25

Annex A – Security zones 25
Annex B – Operational system and sensor descriptions 27
Annex C – Cost breakdown 43

1.

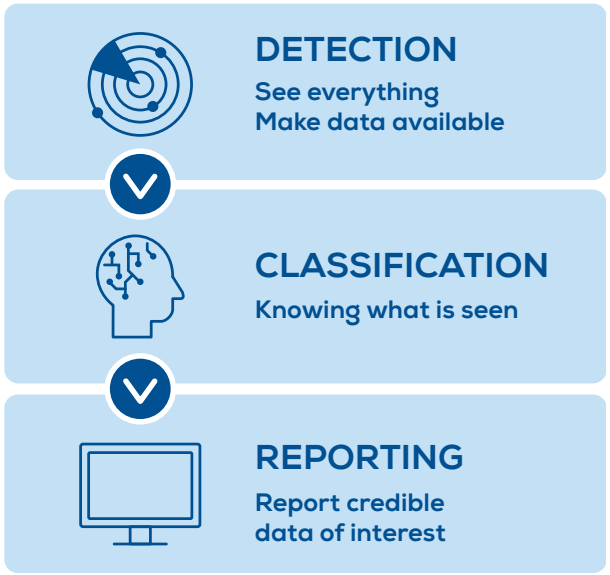
Terma White Paper – Offshore wind farm security Concept

Terma White Paper

1.1 Introduction to offshore wind farm security concept

The offshore wind farm security concept presented in this white paper has been developed by Terma A/S based on Terma's long-standing professional experience in both civilian and military surveillance, situational awareness and integrated sensor systems. The concept draws on operational knowledge from maritime, air and subsea monitoring, as well as practical trials and engagements with offshore wind farm developers in the North Sea and the Baltic Sea. The aim is to show how mature, civilian and dual-use technologies can be combined into a proportionate, scalable and non-military security approach for offshore wind assets, providing a financial estimate (rough order of magnitude) for the WindEurope financial impact estimation.

FIGURE 1. Functional chain for physical security



Source: Terma

1.2 Detect, classify, report and act

The principles behind a security concept for critical infrastructure follow a straightforward sequence: detect, classify, report and act. The final step — act — depends on who is assessing the situation. For a wind farm operator, acting may involve logging the incident, preserving data and notifying the competent authority. For a national authority, it may involve deploying assets, investigating, or exercising the legitimate use of force and other state instruments in line with the nature of the incident and the political response. The security concept focuses on the first three steps, and on how they enable and support effective action when an incident occurs.

The top priority is early detection of anything that deviates from normal operations. This requires a high level of situational awareness that provides a clear baseline "pattern-of-life" in and around the asset. This way any anomalies will stand out. Once an event is logged, it must be classified and reported to operators in a clear, actionable format, enabling a timely and proportionate response.

To support the principles of the security concept a suite of sensors is required. This will provide situational awareness and enable detection and classification of events that may be malicious activities. Furthermore, a security system, in the form of an operational system, is needed to ensure that anomalies are flagged and reported to the operator when action is required.

FIGURE 2. The relationship and difference between a threat and a risk

Source: WindEurope

The security concept is rooted in a vulnerability and risk assessment for a generic offshore wind farm layout. This is used to guide the security solution design. It involves delineating security zones within and around the installations, evaluating the criticality and exposure of each component within the energy production facility.

The assessment of vulnerability is focused on identifying the weakness in an asset that makes harm more likely or more severe in case of malicious activity. In an offshore wind farm, there are various vulnerabilities spanning from physical to digital. The focus should be on single-point-of-failure vulnerabilities.

The risk assessment focuses on the expected effect of a threat exploiting a specific vulnerability by analysing likelihood and impact. The likelihood of malicious activities toward critical infrastructure has been growing over the last few years – the Nord Stream 2 attack being the most recent evidence.

The impact is seen in relation to the wind farm operation and generation of electricity where a full shutdown has a substantial impact on the revenue generation for the operator and a potential critical impact on the wider public through massive power outages. The effort needed to repair any incidents and get a wind farm back into operation is also a factor that is taken into consideration. Here the focus is on the cost of repairs but also, and more importantly, the time of repairs.

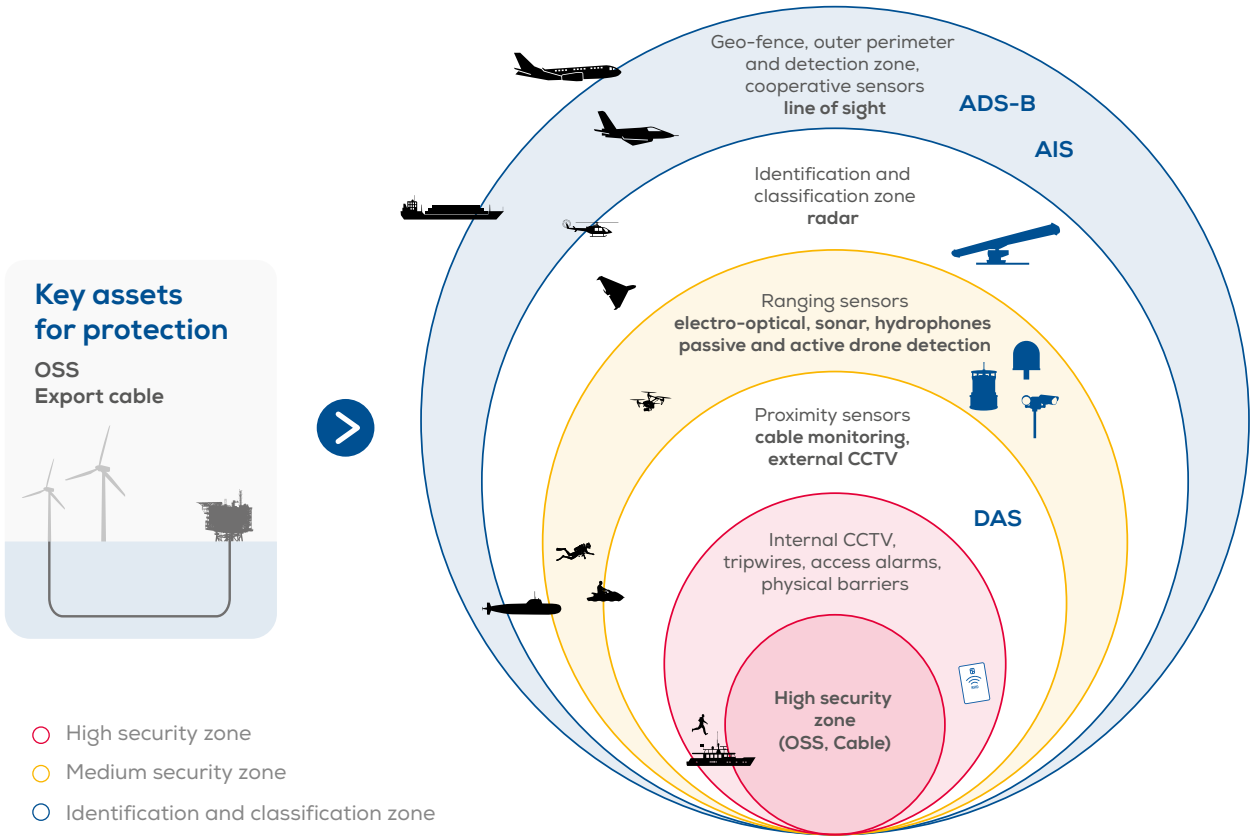
The single-point-of-failures in a generic offshore wind farm layout are the offshore substation (OSS) and export cables. This means they must be managed with the highest level of security in a security concept. Based on vulnerability and risk assessment the security layout for an offshore asset can be divided into three types of zones; the High security zone; the Medium security zone; and the Identification and classification zone.

1.3 Security zones

The introduction of the security-zone concept aims to establish a comprehensive, component-level understanding of offshore asset vulnerabilities. For each site, a tailored assessment is carried out to define operational zones based on local conditions such as seabed topography, maritime traffic density, environmental characteristics and applicable regulatory frameworks. This approach ensures that security measures are proportionate, risk-informed and aligned with both national and regional requirements.

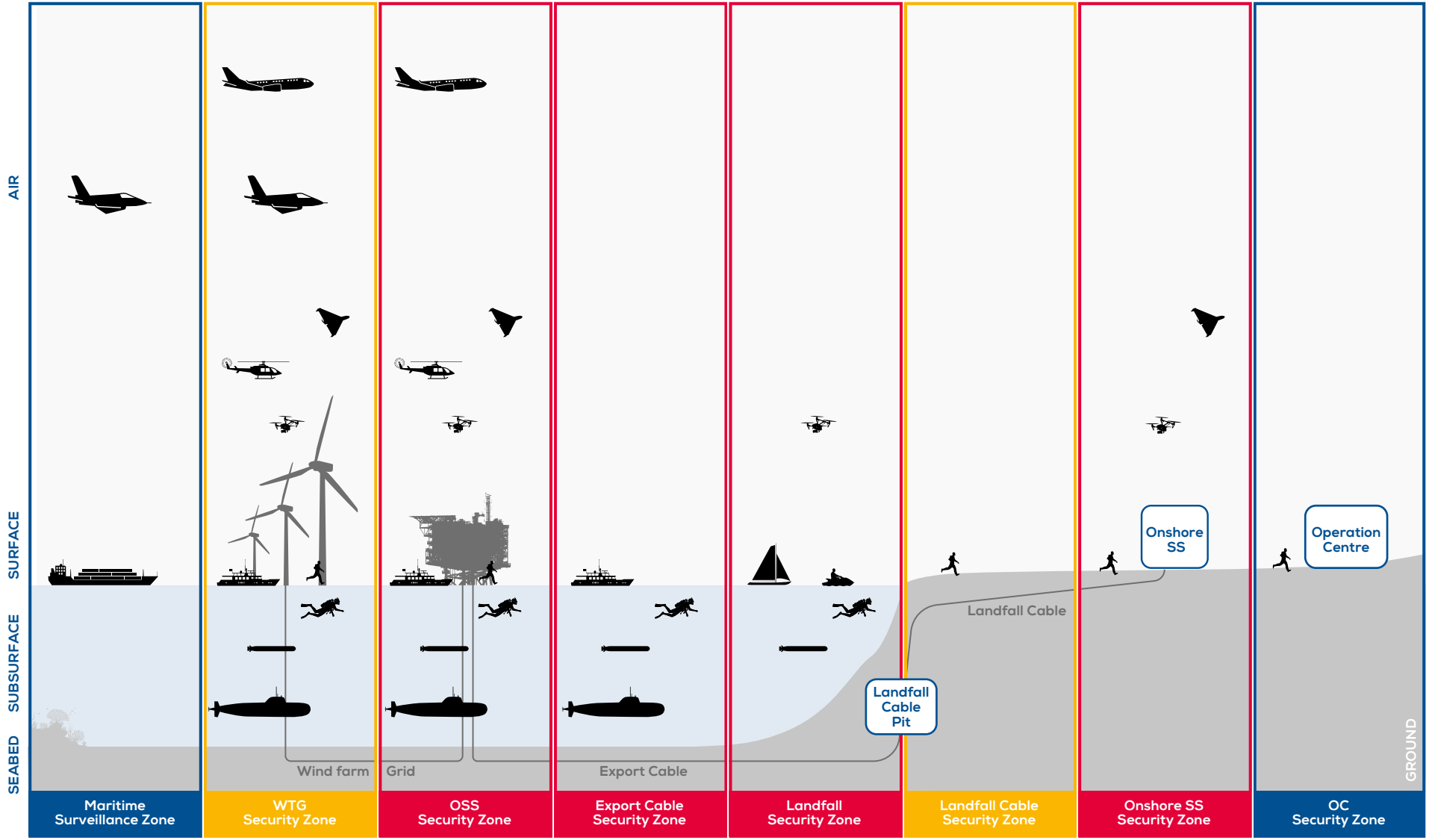
The assessment delivers the granularity necessary to specify appropriate security measures, including the configuration of sensor systems needed to maintain effective situational awareness. It also supports the definition of detection capability requirements—identifying which sensor types or sensor suites are needed, their optimal placement and the performance parameters they must meet (e.g. covering geometry, range and detection thresholds) to mitigate the identified risks effectively.

FIGURE 3. Layered security detection



Source: Terma

FIGURE 4. Security zone concept



Source: Terma

1.4 Methodological framework

The underlying methodology systematically examines the individual components of an offshore wind farm— turbines, substations, export cables, foundations and control systems, to evaluate their vulnerabilities and operational criticality. For each component, the analysis identifies the full spectrum of potential physical threat vectors across the domains. These threat scenarios are then mapped against the most suitable detection and monitoring technologies. Based on this structured analysis, specific sensor solutions are selected to detect, classify and respond to potential intrusions or anomalies in real time.

To enable practical implementation, the defined security zones are categorised into four operational domains, allowing for layered protection and graduated response measures across the offshore environment. This zone-based framework ensures that detection, response and deterrence measures are harmonised, scalable and adapted to the evolving maritime risk landscape.

1.5 Air domain

The primary concern across wind farm zones in the air domain is unmanned aircraft (drones), with growth expected to continue as part of hybrid activity. If the security solution can reliably detect drones, larger aircraft and helicopters will also be detectable.

Sensors and roles:

- **RF drone detectors**: Radio Frequency (RF) drone detectors detect consumer (COTS) drones by their radio signatures (control links/telemetry). They do not detect aircraft in general and cannot detect “dark” drones that fly autonomously without RF emissions or that use non-standard links (e.g. fibre-tethered).
- **Radar:** Detects cooperative and non-cooperative aerial targets (performance depends on radar type, frequency and clutter environment). This is the main sensor for guaranteed air-domain situational awareness against both regular aircraft and drones.
- **ADS-B receivers:** Used to detect cooperative manned aircraft equipped with ADS-B. Non-ADS-B aircraft are effectively non-cooperative and must be detected by radar.

Because non-cooperative aerial threats exist, radar should be the backbone of air-domain awareness. RF sensors and ADS-B are valuable adjuncts for classification and context but cannot replace radar.

1.6 Surface and ground domain

1.6.1 Sea surface

The focus is on vessels of varying sizes (or surfacing divers/ Unmanned Surface Vehicles - USVs) inside the wind farm boundary, along export-cable routes, or loitering near wind farm perimeters. Surface platforms can deploy other threats (drones, UUVs, divers), so early vessel detection is pivotal.

Sensors and roles:

- **AIS receivers**[1]**:** Identify cooperative vessels.
- **Marine radar:** Detects cooperative and non-cooperative surface objects, providing the primary situational awareness layer at sea.
- **EO/IR cameras**[2]**:** Support identification and behaviour assessment once a contact is cued by radar.

As with the air domain, radar is primarily for the sea surface. AIS enriches the picture for compliant traffic. EO/IR– helps classify radar targets and verify AIS signature along with creating the evidence of documented abnormal patterns or actions on the surface (random loitering, cable-corridor shadowing, repeated boundary probing).

1.6.2 Land surface (ground)

The focus is on people on foot or vehicles approaching onshore substations, cable-landing sites, or control centres. Onshore assets are smaller and more constrained than offshore structures, making physical barriers very effective.

Sensors and roles:

- Physical barriers (fencing, gates, controlled entry) form the first line of defence.
- EO/IR cameras provide persistent monitoring and verification.
- Ground-surveillance radar (as needed) can be added for wide-area coverage when perimeters are large or cluttered.

1. AIS — Automatic Identification System: A maritime tracking system used by ships and coastal authorities to identify and locate vessels automatically by electronically exchanging data such as vessel identity, position, course, and speed. It improves navigation safety and maritime domain awareness.
2. EO/IR cameras — Electro-Optical / Infrared cameras: These are advanced imaging systems that combine electro-optical (EO) sensors, which capture visual-spectrum (daylight) images, with infrared (IR) sensors, which detect heat signatures and enable imaging in low-light or night-time conditions. In security and surveillance applications — such as for offshore wind farms, naval operations, or border monitoring — EO/IR cameras provide continuous, all-weather situational awareness.

- DAS[3] (Distributed Acoustic Sensing) for monitoring cable tampering – this is critical in the landfall zone where cables go from sea to land

A barrier + EO/IR baseline will typically counter any security concerns on land, while in some cases – where the protected area or approach routes warrant earlier detection and warning – ground radar is needed.

1.7 Subsea domain

The focus is on divers and UUVs that usually require a surface deployment platform, and therefore correlate with sea-surface activity. Submarines are an exception, with long-range underwater mobility.

Sensors and roles:

- **Active/passive sonar and hydrophones:** Detect and track subsea contacts in defined sectors or choke points around the most critical installations.
- **DAS (Distributed Acoustic Sensing):** When available on fibre along cable routes, provides wide-area vibration/acoustic change detection.

Many subsea threats start at the sea surface. By first covering the surface with radar and electrooptical cameras and then monitoring high-risk corridors and asset areas with sonar, hydrophones and DAS, one can quickly achieve situational awareness. Subsea sensing should be targeted to where the risk is highest, not applied uniformly everywhere.

3. DAS — Distributed Acoustic Sensing: A fibre-optic sensing technology that uses standard optical cables to detect vibrations, acoustic signals and disturbances along their length. By analysing backscattered light within the fibre, DAS can identify and localise events such as vessel movement, cable interference or ground disturbance, enhancing subsea and terrestrial infrastructure monitoring and situational awareness.

1.8 Seabed domain

Focuses on tampering or damage to export cables beyond the wind farm boundary. Cable corridors can extend up to tens to hundreds of kilometres, making uniform sensing impractical.

Sensors and roles:

- DAS is the main monitoring tool for long cable spans, enabling localisation of disturbances to specific segments for rapid investigation.
- Coastal surveillance and authority feeds (Vessel Traffic Service, maritime patrols) augment your forensic trail and speed incident reporting.

Implication: The goal is rapid pinpointing of anomalies rather than continuous high-fidelity surveillance along the entire route. Combining DAS alerts with surface-domain situational awareness (radar/AIS) and authority data can close the loop from detection to response.

1.9 Technologies and sensors to achieve situational awareness

Effective situational awareness counts on deploying the right mix of sensors matched to the specific vulnerabilities and risks of each asset and zone (e.g. the wind farm perimeter, approaches, the export-cable corridor, landing sites).

Because situational awareness covers several domains, it depends on multiple sensors—far more than a human operator can track effectively in real time. The operational system must therefore automate detection, correlation, and prioritisation, and present a single, clear situational picture backed up by standardised workflows so that any operator can manage incidents confidently and consistently.

Equally important is transforming raw sensor data into meaningful, actionable insight. Operators need early warning that something is approaching and an indication of whether it is likely to develop into an incident. Rather than displaying all activity within the security zones, the system should automatically filter anomalies and only highlight behaviour that deviates from the normal pattern—activities that appear unusual, suspicious, or potentially threatening.

Vulnerability and risk assessment are key to sensor selection. To configure the right suite of sensors, it is vital to understand sensor capabilities and how to design a layered, multi-domain setup.

Two cross-cutting points guide all domains:

- **Cooperative vs. non-cooperative targets:** Cooperative targets broadcast (e.g. ADS-B for aircraft, AIS for vessels), whereas non-cooperative targets do not and therefore need active sensing (typically radar, sonar, hydrophones, DAS) to detect.
- **Multi-domain fusion:** Situational awareness should be assessed across air, surface/ground, subsea and seabed/export cable domains, using sensor fusion and behaviour analytics to spot anomalies early, e.g. a vessel detected in the maritime surveillance zone stops and deploys a diver or UUV that enters the subsea domain.

To build a robust security solution, the core should be a set of sensors that can detect non-cooperative targets. Above and at the sea surface this means radar; below the surface it means sonar, hydrophones and DAS. This sensor backbone sets the standard for the rest of the system and determines how well additional sensors will perform.

To best achieve a layered multi-sensor system, it is necessary to understand the specifics on sensor capabilities and performance (e.g. range, RCS[49] and clutter parameters)

4. RCS – Radar Cross Section is a way to quantify how detectable an object is by radar.

TABLE 1. Matrix of security zones and threats

Zone		Maritime Surveillance Zone	WTG Security Zone	OSS Security Zone	Export Cable Security Zone	Landfall Security Zone	Landfall Cable Security Zone	Onshore SS/Onshore Control Centre/ Warehouse Security Zone	OC Security Zone
Threat Methodology	Air Domain	• Intelligence, Surveillance and Reconnaissance activities over turbines and offshore substations. • Payload delivery or deliberate interference during maintenance windows. • Support to cyber operations (e.g. Wi-Fi/Bluetooth proximity attacks).							
	Surface domain	**Sea:** • Shadow fleet loitering in proximity or inside wind farm boundaries for reconnaissance and staging for other threats. • Vessels loitering along export-cable corridors for reconnaissance. • Suspicious patterns near ports, landing sites, or interconnectors. • Damage to export/array cables, offshore substations.				**Land:** • Damage to onshore converter/landing stations. • Arson or intrusion at onshore facilities(substations, control centres).			
	Subsea/ Seabed domain	• Cable tampering, seabed package placement, or sensor interference near cables and foundations. • UUV mapping of cable routes, OSS approaches, or landing zones. • Covert mapping or interference with subsea power and data interconnectors beyond wind farm perimeters.					NOT Applicable		
Threat types		• Aircraft • Vessel	• Aircraft, Drones • Human • Vessel, Jet skis, • Surface drones, Submarines, Divers, UUVs	• Aircraft, Drones • Human • Vessel, Jet skis, • Surface drones, Submarines, Divers, UUVs	• Vessel with ROV, anchors, • Submarines, Divers, UUVs	• Divers, UUVs	• Human	• Human • Drones	• Human
Sensor Technology vs. Threat type		• Combined Surface & Air radar • ADS-B, AIS • Radar for mitigation of wind farm shadow effects.	• Combined Surface & Air radar, ADS-B, Drone RF Sensors • EO/IR Cameras • Access Control, CCTV[4], PIR[5] • AIS, DAS, Hydrophones	• Combined Surface & Air radar, Drone RF Sensor, ADS-B • EO/IR Cameras • Access Control, CCTV, PIR • DAS, AIS • Sonar and Hydrophones	• (Surface Radar) • DAS (Full surveillance on entire cable), Hydrophones	• DAS, Hydrophones	• Access Control, CCTV, PIR • DAS, Hydrophones	• Ground Surveillance Radar • Drone RF Sensor, • Drone radar (option) • EO/IR Cameras • Access Control, CCTV, PIR	• Access Control, CCTV, PIR

5. CCTV- Closed-Circuit Television, which refers to a system of cameras and monitors used for surveillance.
6. PIR – Passive Infrared, a type of sensor used in motion detectors.

1.10 Considerations regarding sensors

As shown in the table above, a wide range of sensors all contribute to the situational awareness achieved through the security concept. Other considerations are also important in terms of choosing which sensors to use.

Today's offshore wind farms already include a wide range of technologies that can monitor the surroundings to a certain extent. These can be sensors measuring temperature, humidity, wind, pressure, CCTV for Health and Safety, radar for bird monitoring, light control of the aeronautical lights on top of the wind turbine generators (WTGs) etc. But these sensors and the technology behind them have a primary function related to the operation of a wind farm – and any surveillance and monitoring capabilities will be secondary. As such this can only be a supportive layer to a security solution, but not the primary suite of sensors that gives the required level of situational awareness.

1.10.1 Sensor resilience and cross sensor coverage capabilities

The radar sensors can be remotely reconfigured to fit the operational situation if this changes over time. This can be in relation to achieving redundancy or focusing on drone, surface, or general air surveillance.

This use of drone radars gives some clear and distinct advantages in detecting drones near an offshore substation (OSS), taking the exceeding range capabilities into account. The drone radars will not be limited to detecting and classifying Unmanned Aerial Vehicles (UAVs) and Unmanned Surface Vessels (USVs), but also anything moving within the coverage volume.

The security solutions' operational performance benefits by integrating the available sensors, providing detection of the genuine objects present in the coverage volume from different angles from:

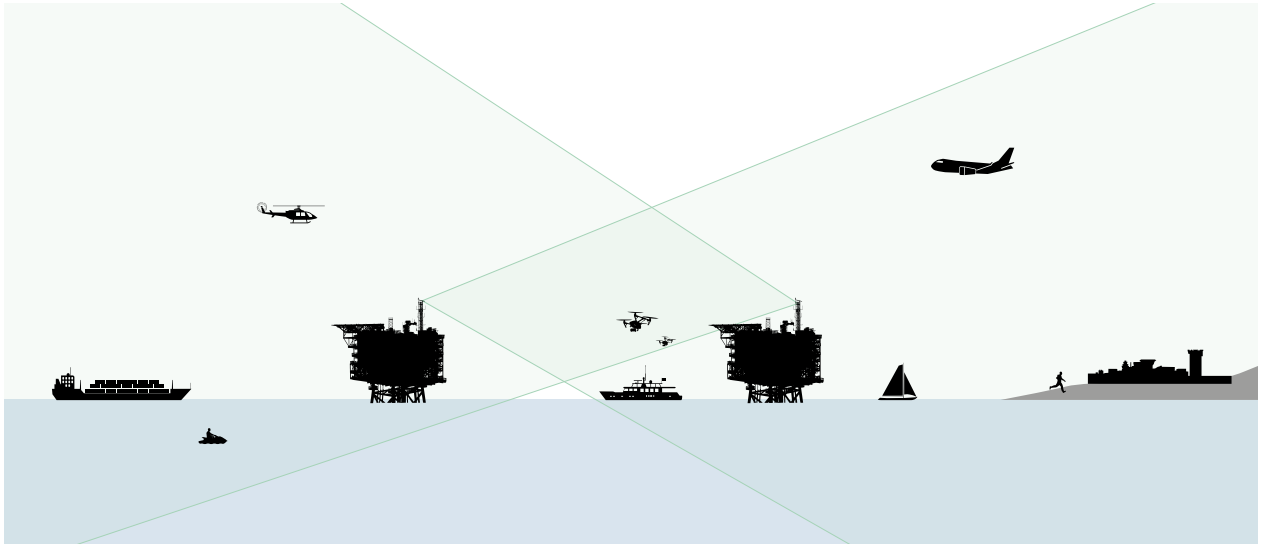
- Decorrelation of static and dynamic appearing ghost-targets caused by reflections/bounces of the microwave energy between WTGs and activities taking place within the wind farm boundary.
- Reducing the close-in coverage near the surface, as neighbouring radars will provide detection all the way to the foot of the offshore substation (OSS), opposed to a radar installed on an offshore substation (OSS) at a height of e.g. 55 m. (See figure 8 below).
- Height information can come from 3D radars or be derived by correlating the available 2D radar data, which makes height information available in addition to range and bearing of elevated objects within the area covered by multiple sensors.
- 3D information from the radar sensors is needed, as this will reduce the camera search time and boost the success of acquiring small objects at large distances.

1.10.2 Sensor degradation considerations

Another important aspect to be aware of is that the overlapping sensor coverage also enhances system resilience. Specifically, if one of the drone radars is taken out of service, drone detection capability is not entirely lost.

While full coverage cannot be maintained, the overlapping fields of view ensure that most of the area surrounding the offshore substation (OSS) remains under effective drone surveillance.

FIGURE 5. Inter-offshore substation radar coverage



Source: Terma

1.10.3 Sensor reconfiguration capabilities

As mentioned above, the radars can be managed and reconfigured for different operational objectives remotely if needed i.e. as drone/surveillance – air or surface as redundancy and always optimising the coverage with the assets available.

The resilience features this offers give the sensor system in-theatre configurability. In response to a specific threat scenario requiring extended surface and air coverage, one of the drone radars can be temporarily reconfigured to adopt the surveillance profile used by another radar within the system.

Similarly, the surveillance radar can be configured for drone detection if the situation calls for it.

This reconfiguration should be carried out remotely with a support team or locally by a qualified Security Supervisor at the O&M base.

During this period, drone detection capability is still active - albeit at reduced capacity - with one drone radar continuing in its dedicated role. Once the elevated threat subsides, the radar configuration can be restored to its default settings, resuming standard operational coverage.

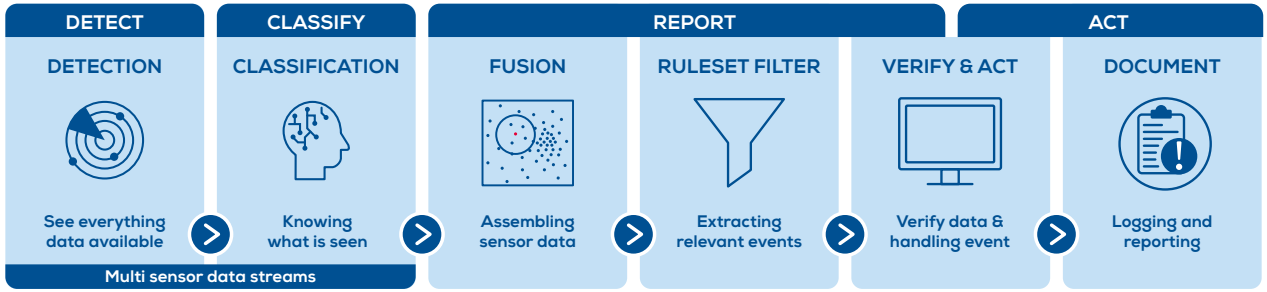
2. The functional chain in a security solution

The functional chain in a security solution

To effectively support threat response and the security solution, Terma recommends a structured, six-stage functional chain. This framework helps operators maintain situational awareness, identify anomalies and coordinate appropriate response actions. A key objective is to detect abnormal activity. To do so, operators must first have a clear situational picture of the normal “pattern-of-life” in the area, enabling them to recognise, classify and act on irregular events.

The functional chain shows how the system’s core components are integrated and how data from multiple sources is fused. The operational system is built on proven, readily available components and subsystems that collectively deliver the required functionality. It is designed to be operated by non-specialists through standardised, largely automated incident handling, which significantly cuts down on operator workload and minimises reliance on highly specialised knowledge. Beyond deploying a multi-layer, multi-domain sensor suite, it is essential to have a unified operational system integrating sensor data and actively supporting the operator. This system highlights abnormal events, prioritises anything requiring attention and assists in guiding an effective and timely response.

FIGURE 6. Six-stage functional chain



Source: Terma

2.1 Functional chain description

2.1.1 Detection

Detection of any activity within the coverage area is the basic starting point as without detection, further processing of possible threats is not possible.

The sensors supporting the detection objectives are:

- The surveillance sensors operating with a maximum coverage range of 30NM ;
- Two drone radars operating with a maximum coverage range of 12NM each; and
- Two 360-degree radio frequency/direction finders.

The sensor suite is tailored to the requirements of each security zone across the air, surface and sub-surface domains. By combining the strengths of multiple sensor types, the system delivers comprehensive surveillance adapted to the wind farm environment and its potential threats.

Each sensor does more than carrying out detections, but also provides sensor-specific metadata for tracking, classification and the overall autonomy strategy. As a result, multiple independent sensors operate in parallel, feeding synchronised data streams into the operational system to ensure a robust and resilient situational picture.

FIGURE 7. Summary of tracked targets before application of classification. In total, 1.48 million track updates were recorded and summarised in this image.

FIGURE 8. The tracked targets the radar automatically classified as drones. The number of track updates is now 19,460 and illustrates the actual drone trajectories.

Source: Terma

2.1.2 Classification

Target classification of all objects automatically detected and tracked by the sensor suite is key in enabling the next step in the functional chain to prioritise focus on potential threats to confirm/identify an intrusion, by excluding nuisance objects e.g., wildlife from drawing attention.

The classification will allow the operational system to automatically focus its attention on any “man-made-object” detected, tracked and classified with a high probability – regardless of whether it is a vessel, aircraft drone or dinghy. This system would and not waste valuable reaction time in confirming the identity of an intrusion.

In the drone radar as well as the surveillance radar instance, this is embedded in the radar classifier using AI on all available track attributes. To achieve the best classification with the minimum false positive the classification must be an integrated part of any radar sensor.

The RF/DF sensors will similarly provide automated target information and classification, generated through the security solutions AI capabilities. To demonstrate the necessary capability of a radar classification function and how this directly affects a security solution, see an example in figs. 13 and 14.

2.1.3 Fusion

Data from all sensors is fused within the operational system to create a consolidated system track. By combining independent sensor inputs, the system enhances situational awareness and strengthens resilience against disturbances such as turbine reflections and ongoing activities within the wind farm.

The security solution should therefore be capable of multi-sensor data fusion in a distributed configuration. This ensures that all sensor outputs are merged in a controlled manner, leading to a shared, coherent picture of air, surface and sub-surface activity.

The fused data is retained throughout the entire workflow, from detection to documentation and reporting. Through sensor fusion, the resulting track information becomes more accurate and reliable than any individual sensor can provide on its own, ultimately strengthening operator decision-making when assessing potential threats.

2.1.4 Ruleset filtering

A detected, tracked and classified object near a wind farm does not necessarily require an immediate response. It will only trigger action if a predefined rule is violated—for example, entering a turbine security zone or, in more critical cases, the offshore substation (OSS) security zone. Whether an object is considered a threat or non-threat depends on several factors, including intelligence data, its position, course, speed, whether it is inside a critical area, or if the wind farm is in a heightened state of alert.

To manage this, the operational system must include a fully customisable rule-set engine, effectively operating as a configurable “what-if” logic framework. This allows threat response actions to be tailored to each site’s risk and vulnerability assessment. Because threats evolve over time, these rules must be continuously maintained and adjusted by the wind farm’s security operators.

For example, in a rule-based scenario, if a radar-classified drone enters a designated critical zone, the rule-set engine will automatically assign and steer the most suitable available camera toward the object. This enables rapid visual

confirmation through AI-based image recognition, ensuring a precise and timely response.

2.1.5 Verify and act

When a rule is triggered, the operator must receive one clear, consolidated event/alarm through the operational system. At this stage of the functional chain, it is critical that only validated and relevant alarms are reported, preventing an operator overload from false alerts or normal operational activity.

Once an alarm is raised, the system will guide the operator using predefined procedures, tailored to the event type, the current security level and relevant operational parameters. Alongside the live video feed from the automatically assigned tracking camera, the operator must also have access to the object's historical track, ensuring full situational awareness.

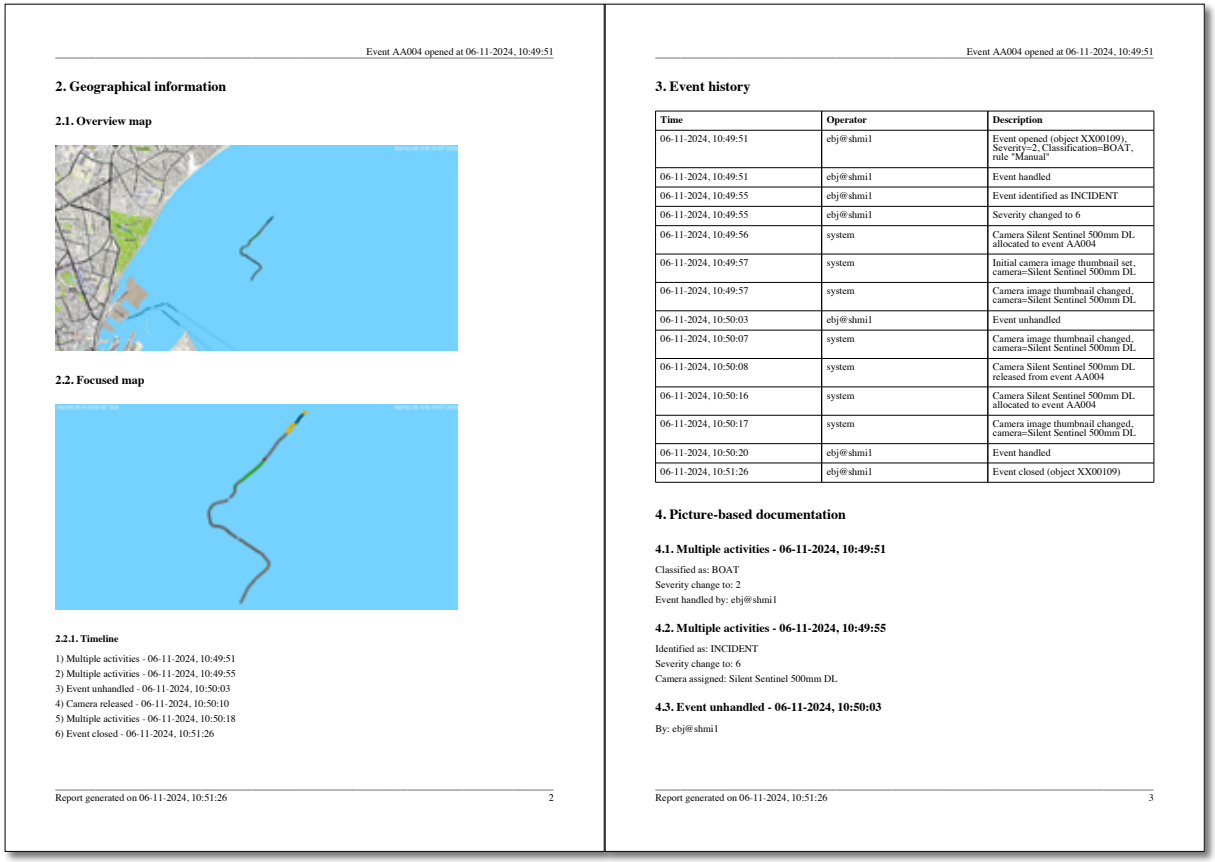
All processes leading up to the alarm must be fully automatic, with no operator intervention required—regardless of time of day or environmental conditions.

2.1.6 Document

The security solution must ensure the event sequence is automatically documented in its entirety in a forensic-grade event report that is stored in the operational system.

This allows the wind farm owner/operator's security team to clearly generate and submit evidence internally as well as externally to the full extent of what was experienced e.g. by means of automatically sending out e-mails to predefined individuals and/or security agencies. See extract example from a standard report below in fig. 15.

FIGURE 9. Event report example for forensics and documenting the incident



2. Geographical information

2.1. Overview map

2.2. Focused map

2.2.1. Timeline

1) Multiple activities - 06-11-2024, 10:49:51
2) Multiple activities - 06-11-2024, 10:49:55
3) Event unhandled - 06-11-2024, 10:50:03
4) Camera released - 06-11-2024, 10:50:10
5) Multiple activities - 06-11-2024, 10:50:18
6) Event closed - 06-11-2024, 10:51:26

3. Event history

Time	Operator	Description
06-11-2024, 10:49:51	ebj@shmi1	Event opened (object XX00109), Severity=2, Classification=BOAT, rule "Manual"
06-11-2024, 10:49:51	ebj@shmi1	Event handled
06-11-2024, 10:49:55	ebj@shmi1	Event identified as INCIDENT
06-11-2024, 10:49:55	ebj@shmi1	Severity changed to 6
06-11-2024, 10:49:56	system	Camera Silent Sentinel 500mm DL allocated to event AA004
06-11-2024, 10:49:57	system	Initial camera image thumbnail set, camera=Silent Sentinel 500mm DL
06-11-2024, 10:49:57	system	Camera image thumbnail changed, camera=Silent Sentinel 500mm DL
06-11-2024, 10:50:03	ebj@shmi1	Event unhandled
06-11-2024, 10:50:07	system	Camera image thumbnail changed, camera=Silent Sentinel 500mm DL
06-11-2024, 10:50:08	system	Camera Silent Sentinel 500mm DL released from event AA004
06-11-2024, 10:50:16	system	Camera Silent Sentinel 500mm DL allocated to event AA004
06-11-2024, 10:50:17	system	Camera image thumbnail changed, camera=Silent Sentinel 500mm DL
06-11-2024, 10:50:20	ebj@shmi1	Event handled
06-11-2024, 10:51:26	ebj@shmi1	Event closed (object XX00109)

4. Picture-based documentation

4.1. Multiple activities - 06-11-2024, 10:49:51

Classified as: BOAT
Severity change to: 2
Event handled by: ebj@shmi1

4.2. Multiple activities - 06-11-2024, 10:49:55

Identified as: INCIDENT
Severity change to: 6
Camera assigned: Silent Sentinel 500mm DL

4.3. Event unhandled - 06-11-2024, 10:50:03

By: ebj@shmi1

Source: Terma

3. Use cases

Use cases

The configuration of an offshore wind farm varies significantly as a function of geography, bathymetry, meteorological conditions, distance to shore, infrastructure layout and national regulatory requirements. So the offshore security concept is designed as a scalable and modular architecture that can be configured to meet security demands across a broad spectrum of wind farm types – independent of size, location, or jurisdiction. To show how a security solution can be engineered—and how system complexity and cost drivers may differ—two representative use cases are applied.

Use Case 1 is located in the Mediterranean, while Use Case 2 is in the North Sea and Baltic Sea. These locations have been deliberately selected to reflect distinct environmental and operational conditions, including differences in weather patterns, sea states and regulatory frameworks.

The use cases also represent variations in wind farm layout, including near-shore and far-offshore deployments, as well as configurations with and without offshore substations (OSS). Although these scenarios do not cover the full range of possible offshore wind farm designs worldwide, they are an indicative cross-section of typical design differences. The objective is to illustrate how geographical conditions, infrastructure topology and operational requirements influence the engineering of a security solution—from sensor selection and placement to system integration, ruleset configuration and response architecture.

© Terma

3.1 Use case 1 – 500 MW wind farm in the Mediterranean

For this use case, the layout consists of twenty-five 20 MW WTGs, four export cables and no offshore substation (OSS). A wind farm in the Mediterranean will typically be located relatively close to shore, due to the region's deep waters, tight continental shelf and coastal permitting constraints. As a result, these wind farms are often smaller in scale and may not require an offshore substation (OSS), since export cable lengths, transmission losses and offshore grid complexity are reduced.

The operating environment is characterised by generally calmer sea states, higher water depths closer to shore, lower tidal variation, dense coastal traffic, proximity to ports, fishing activity and recreational vessels. These conditions drive a security approach focused on near-shore domain awareness, high vessel-density monitoring and rapid response coordination with coastal authorities. In this use case, it was found that there is no need for sonar or hydrophones as there is no offshore substation (OSS) installed. The monitoring of the export cables is covered by DAS.

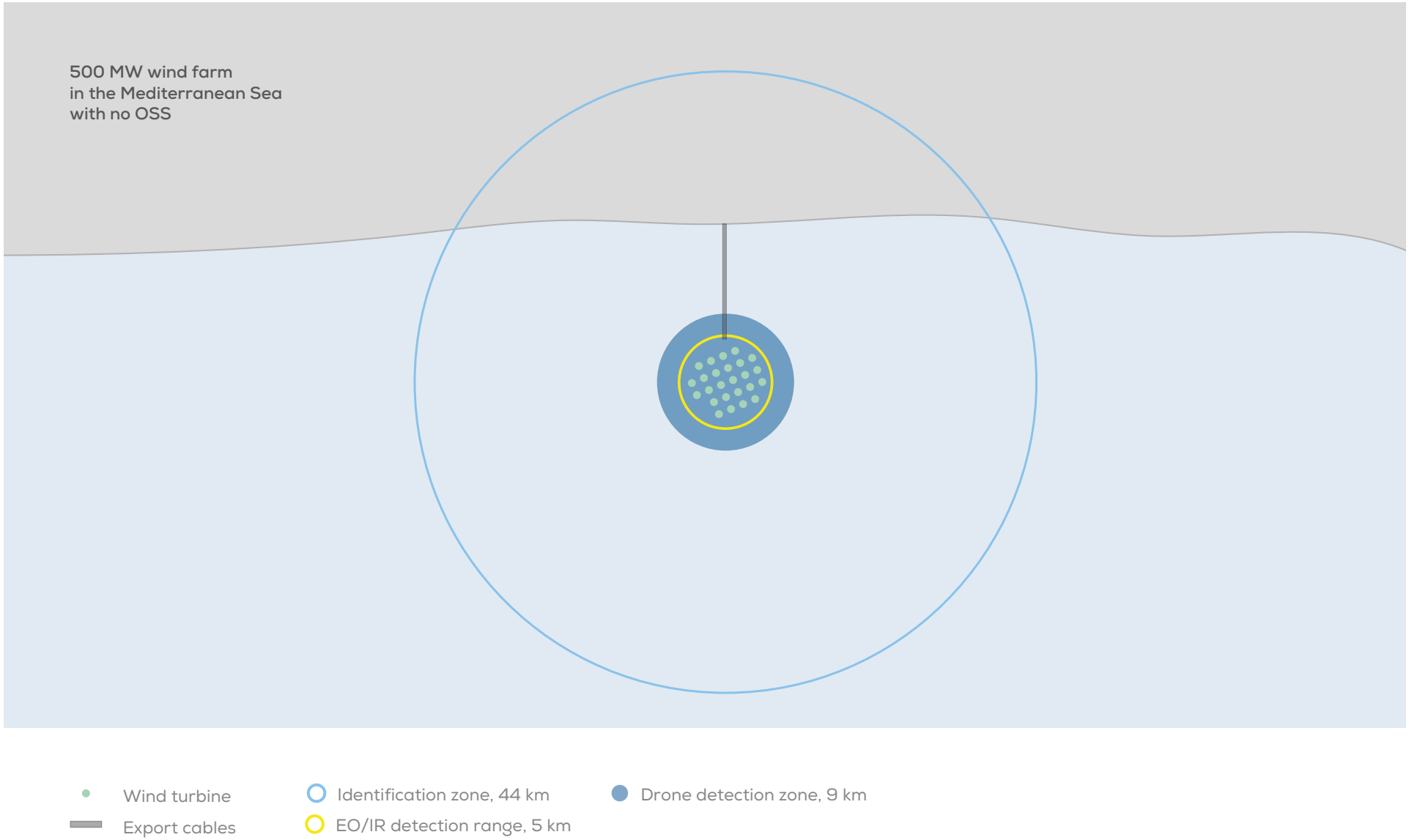
TABLE 2. Summarised security solution for use case 1 – 500 MW wind farm in the Mediterranean

Primary sensors	Combined surface & air radar (mounted on WTG); DAS on export cables; IR tracking on onshore substation; access control & CCTV at onshore substation and operations centre.
Optional	EO/IR cameras; AIS/ADS-B receivers; ground-surveillance radar at onshore substation; drone RF sensor (directional); additional radar to mitigate wind farm shadow or a coastal radar site.
Detection coverage	Radar ID/classification ~30NM (55 km) for vessels/aircraft; drone detection up to 9 km; EO/IR cued detection up to 5 km; DAS monitors seabed activity along cable route.
Strengths	Simple architecture with DAS coverage of export cables; broad maritime/air picture from combined radar.
Limitations	No sonar or hydrophone; limited early warning outside onshore substation perimeter without ground radar.
CAPEX	€4m (ROM[42]).
OPEX per year	€550k (ROM) – this includes: • Initial spares and replacement units when lifetime is reached. • Yearly service visit. • Only initial (1 year) warranty. • All necessary preventive maintenance on selected equipment.

TABLE 3. Detailed sensor configuration across the security zones (see figure 16 on p. 45)

Zone	Sensor Technologies	Optional Sensor Technologies
Maritime Surveillance Zone	Combined Surface & Air radar ADS-B, AIS	Radar for mitigation of wind farm shadow effects
WTG Security Zone	Combined Surface & Air radar EO/IR Cameras ADS-B, AIS, DAS	Drone RF Sensors Access Control, CCTV, PIR
OSS Security Zone	N/A	N/A
Export Cable Security Zone	Surface Radar DAS (Full surveillance on entire cable)	
Landfall Security Zone	DAS	
Landfall Cable Security Zone	DAS	Access Control, CCTV, PIR
Onshore SS Security Zone	Drone RF Sensor, EO/IR Cameras Access Control, CCTV, PIR	Ground Surveillance Radar, Drone radar (option)
OC Security Zone	Access Control, CCTV, PIR	

FIGURE 10. 500 MW wind farm in the Mediterranean Sea with no OSS



3.2 Use case 2 – 1.5 GW wind farm in the Baltic or North sea

A medium-to-large wind farm in the North Sea or Baltic Sea is typically located far offshore, where water depths are moderate and an extensive continental shelf allow for large-scale layouts. These regions are characterised by harsh weather conditions, high waves, strong winds, seasonal icing (primarily in the Baltic) and reduced accessibility during winter periods. At the same time, offshore energy activity is dense, with frequent commercial traffic, service operations and military presence. These operational and environmental conditions drive a security approach emphasising wide-area domain awareness, resilient sensor coverage and a robust response architecture capable of maintaining functionality in challenging sea states and low-visibility conditions.

In this use case, the wind farm consists of seventy-five 20 MW WTGs arranged in three clusters, supported by three offshore substations (OSS). Only the two outer clusters are equipped with combined surface- and air-surveillance radars, reflecting a distributed sensor strategy based on coverage, prevailing threat axes and functional redundancy.

The security solution is summarised here:

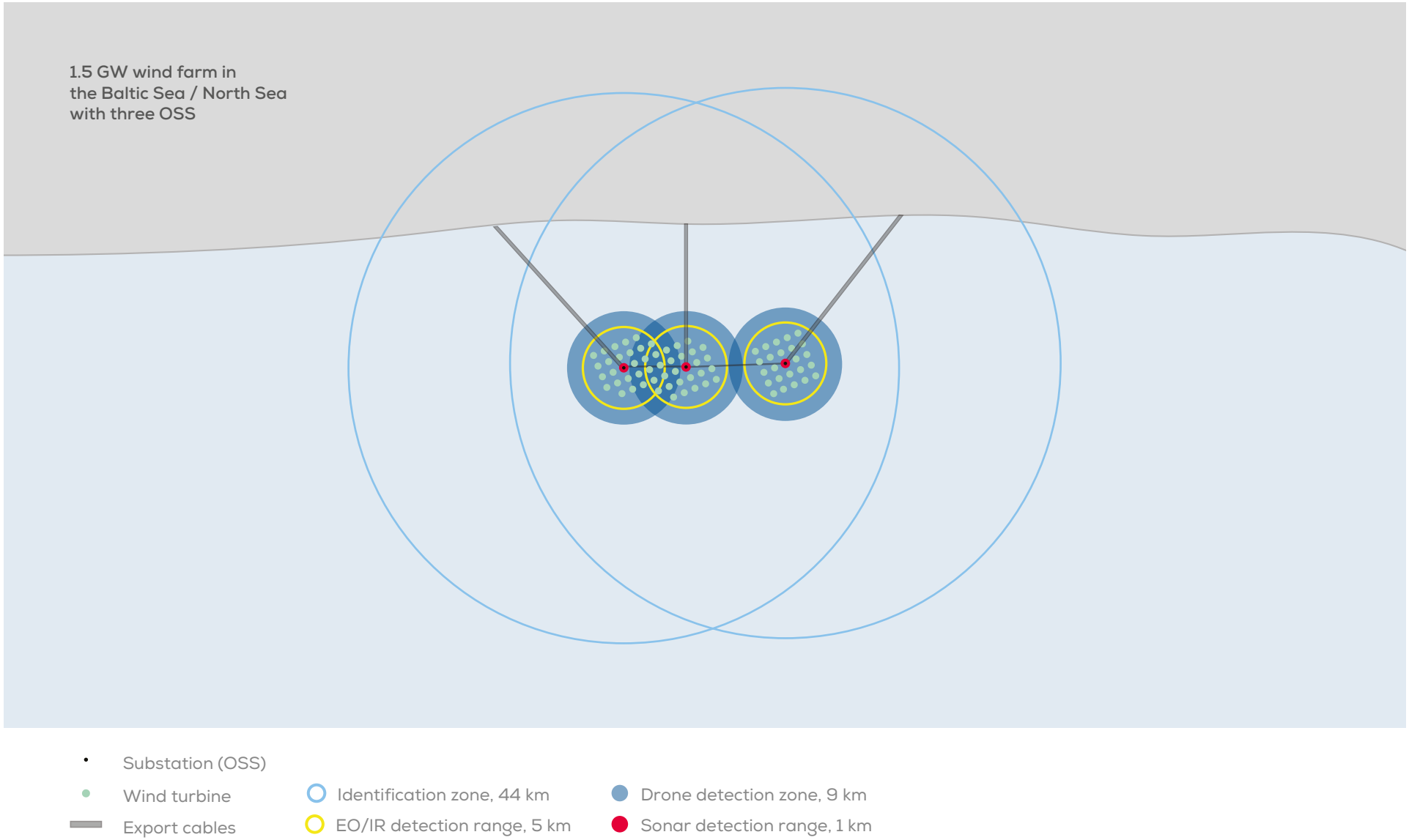
TABLE 4. Summarised security solution for use case 2 – 1.5 GW wind farm in the Baltic or North Sea

Primary sensors	Combined surface & air radar on two OSS; Additional drone radar on central OSS; AIS/ADS-B; long-range EO/IR; sonar/hydrophone at OSS; DAS on export cables; onshore substations with ground radar, IR tracking, EO/CCTV; access control at OSS/onshore/OC.
Optional	Drone RF sensors and direction-finders.
Detection coverage	Radar ID/classification ~ 30NM (44 km); drone detection ~9 km; EO/IR up to ~5 km; sonar up to ~1 km near OSS; DAS along cable corridor.
Strengths	Layered sensing at sea (radar+EO/IR+sonar) and strong onshore posture (ground radar + IR).
CAPEX	€11.5m (ROM)
OPEX per Year	€1.25m (ROM) – this includes: • Initial spares and replacement units when lifetime is reached. • Yearly service visit. • Only initial (1 year) warranty. • All necessary preventive maintenance on selected equipment.

TABLE 5. Detailed sensor configuration across the security zones (see figure 16 on p. 47)

Zone	Sensor Technologies	Optional Sensor Technologies
Maritime Surveillance Zone	Combined Surface & Air radar ADS-B, AIS	Radar for mitigation of wind farm shadow effects
WTG Security Zone	Combined Surface & Air radar EO/IR Cameras ADS-B, AIS, DAS	Drone RF Sensors Access Control, CCTV, PIR
OSS Security Zone	N/A	N/A
Export Cable Security Zone	Surface Radar DAS (Full surveillance on entire cable)	
Landfall Security Zone	DAS	
Landfall Cable Security Zone	DAS	Access Control, CCTV, PIR
Onshore SS Security Zone	Drone RF Sensor, EO/IR Cameras Access Control, CCTV, PIR	Ground Surveillance Radar, Drone radar (option)
OC Security Zone	Access Control, CCTV, PIR	

FIGURE 11. 1.5 GW wind farm in the Baltic Sea / North Sea with 3 OSS



Source: WindEurope

4. Annexes

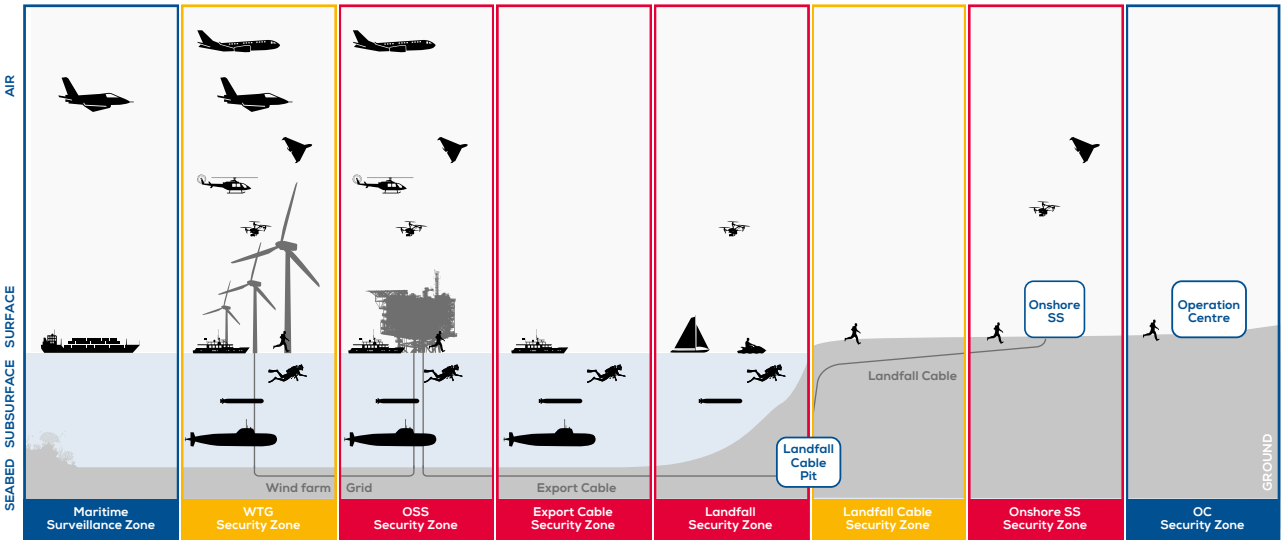
Annex A – security zones

Priority: 1 – High

Offshore Substation (OSS) Security Zone

Within the OSS Security Zone, the objective of the security system is to detect, track and identify all surface, subsurface and air-domain contacts operating in the immediate vicinity of the OSSs — i.e., from the OSS location out to a range of 500 m — to achieve enhanced situational awareness enabling an operator-initiated response.

The security priorities within the OSS Security Zone are divers, UUVs, the smallest boats, USVs, UAVs and aircraft identified as security threats.



Priority: 1 – High

Export Cable Security Zone

Within the Export Cable Security Zone, the objective of the security system is to detect, track and identify subsurface, surface and air-domain contacts operating along the entire export-cable route to potentially enable an operator-initiated response.

The zone should be considered as extending 500 m either side of the cable route until landfall and will partly overlap with the Maritime Surveillance Zone and WTG Security Zones as a high-priority area needing extra surveillance.

The primary security priorities within the Export Cable Security Zone are subsurface activities by UUVs and divers including anchor dragging and dropping, surface objects (boats, vessels, USVs) and secondarily aircraft activities.

Priority: 1 – High

Landfall Security Zone

Within the Landfall Zone, the objective of the security system is to detect, track and identify subsurface, surface and air-domain contacts to potentially enable an operator-initiated response.

The zone should be considered as extending 500 m from the shoreline and 50 m either side of the cable route.

The primary security priorities within the Landfall Zone are subsurface activities by UUVs and divers including anchor dragging and dropping, surface objects (leisure boats and USVs) and secondarily aircraft activities.

Priority: 1 – High

Onshore substation (ONSS) Security Zone

Within the Onshore SS Security Zone, the objective of the security system is to detect activities in the vicinity of the perimeter and UAV activity above the premises to potentially enable an operator-initiated response.

The zone should be considered as extending 50 m from the perimeter and 100 m above it.

The security priorities within the Onshore SS Security Zone are land-based activities by human beings, vehicles and UAVs.

Priority: 2 – Medium

Wind Turbine Generator (WTG) Security Zone

Within the WTG Security Zone, the objective of the security system is to detect, track and identify all surface, subsurface and air-domain contacts operating in the vicinity of the WTGs, thereby achieving enhanced situational awareness and potentially enabling an operator-initiated response.

Within this zone, detection ranges will be proportional to the size of the objects detected by the supporting sensors.

The security priorities within the WTG Security Zone are vessels, boats, USVs, UAVs and aircraft.

Priority: 2 – Medium

Landfall Cable Security Zone

Within the Landfall Cable Security Zone, the objective of the security system is to detect land-based activities in the vicinity of the cable route to potentially enable an operator-initiated response.

The zone should be considered as extending 10 m either side of the cable route along its entire length.

The primary security priorities within the Landfall Cable Security Zone are land-based activities primarily by machinery operating in the vicinity of the cable route/zone or the presence of humans, not animals, within the zone.

Priority: 3 – Low

Maritime Surveillance Zone

Within the Maritime Surveillance Zone, the objective of the security system is to detect, track, and identify surface and air-domain contacts operating beyond the boundaries of an offshore wind farm in order to achieve situational awareness.

Within this zone, detection ranges will be proportional to the size of the objects detected by the supporting sensors (radar and camera).

The security priorities within the Maritime Surveillance Zone are vessels, boats and aircraft.

Priority: 3 – Low

Operations Centre (OC) Security Zone

Within the OC Security Zone, the objective of the security system is to detect intrusion onto the premises to potentially enable an operator-initiated response.

The zone should be defined as the outer perimeter.

The security priorities within the OC Security Zone are land-based activities along the perimeter involving human beings and vehicles.

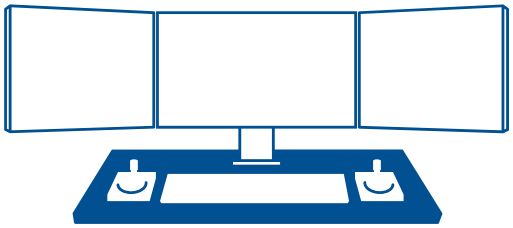
Annex B – Operational system and sensor descriptions

The annex is divided into sections describing the operational system and sensors that supports detection of non-cooperative active sensors, and cooperative passive sensors.

B.1 Operational system

B.1.1 Operation centre

FIGURE 12. Operation centre



In the design of the Operational System, simplicity is the most crucial factor to achieve situational awareness in situations where time to act is of critical importance.

To facilitate this, the operational system shall present relevant object information and camera video to the operator automatically, enabling instant understanding and one-touch fingertip control of the area of responsibility. The system automatically takes over the traditional operator role of selecting the cameras best suited to track objects breaching the security perimeter, including the fusion of data from multiple sensors and evaluation of camera performance given the location of the object. This automation simplifies the SMS operator's interface with the multitude of cameras and sensors, reducing time-consuming tasks that typically divert attention and depend on individual operator performance.

Thus, the system allows the operator to focus on responding to and mitigating the threat rather than controlling a conventional CCTV/VMS system, with manual override options available for camera control should it needed.

Managing the system shall be attained through a one-day training course. The system is thus the ultimate control solution for managing and high-security, wide area perimeter situations.

All security alarms in one place

A key aspect of ensuring a user-friendly SMS is to gather all alarms in one place, so the operator workflow remains focused on dealing with the most severe event(s) and following the predefined tasks (workflow) for the event. Events from surveillance (both air and sea), access control, and perimeter defence are all gathered in the same list to help the operator maintain an overview of the entire security situation.

Highly automated

The SMS shall be designed with highly automated features to simplify the operation for the SMS operator by lowering the number of interactions. Examples of features includes:

- Automatic correlation and fusion of detected objects from multiple sensors to present a simple, coherent picture of the site activity
- Automatic reporting of events to external stakeholders
- Automatic triggering of events on detected objects based on pre-defined rules and zones in all scopes: access control, air & sea surveillance, and perimeter security
- Ensuring that events are only generated by known whitelisted objects if they break pre-defined rules and zones and not generate general events.
- Automatic camera assignment to events based on built-in logics that account for event severity, camera availability, and optimal camera range,
- Automatic control of camera pan, tilt, zoom, and focus to facilitate smooth and efficient visual identification of objects by the operator,
- Automatic execution of pre-defined event tasks, in addition to manual event tasks (workflows) executed by the operator.

These and other features of the operational system enables the operator to focus on the primary task at hand: responding to any threat in the area of interest.

Camera and sensor independence

The system shall be designed to be as camera and sensor agnostic as possible. This means that object tracks and events are presented to the operator in a way that is independent of the specific sensor that has provided the information to the operational system. All information shall be correlated and fused automatically by the logic built into the system, with no required input from the operator. This approach to the system design ensures that the workflow for each event is based solely on the nature of the event (e.g., a ship or drone entering the perimeter, or an access request at one of the OSS doors).

For cameras, the built-in logic will similarly offload the operator's workload by automatically determining the best available cameras to assign to an event, independent of which sensors have provided data to the event. The independence between the detecting sensors and assigned cameras ensures that each camera can be installed completely independent of the installed sensors, and that each camera can be used for any event if the event occurs within the camera's coverage. These features of the system not only result in fewer cameras being required to cover the same area but also introduces a higher degree of redundancy between the installed cameras.

B.2 Non-cooperative and active sensors

B.2.1 The Surveillance Radar

The surveillance radar is the single most contributing sensor achieving surface and air domain situational awareness within the configured coverage volume, day, and night.

FIGURE 13. Surveillance radar

A surveillance radar is a so called "primary radar" which at the output will report presence of an object within the coverage volume i.e., non-cooperative objects, but will not classify the nature of the object i.e., whether a vessel, bird or something else. The sensor output is video and tracks representing the detected objects (vessels, boats, USVs, UAVs and aircraft) to ranges and altitudes proportional to the size they represent to the radar and the distance from the radar.

The surveillance sensor system should be able to classify objects inherently i.e., whether a vessel, aircraft, drone, bird or something else and publish the classification information integrated in each track message distributed for the security management data fusion processor.

Radars support several different applications ranging from leisure craft navigational aids to 3D air defence radars, either with rotating or electronically scanning antennas. The radar sensor architecture and system configuration shall support multiple simultaneous operational objectives, surface and air surveillance, without compromising either of the surveillance objectives.

In general, the most cost-effective radar system configuration achieving the largest possible coverage volume is a 2D radar with a rotating antenna. The radar system should operate in one mode providing simultaneous surface and air surveillance within the different security zones.

The surveillance sensors may operate in fixed but different modes depending on the operational objectives of each sensor. One may be configured for large area surveillance whereas another with reduced range but faster update rate for the objective of detecting smaller objects like e.g., USVs and UAVs.

Typical radar operational mode characteristics, or coverage volumes, may be

- General surface and air surveillance: Instrumented range >24 NM at 14 RPM
- Small object surface and air surveillance: Instrumented range <12 NM at >20 RPM

The surveillance radar shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:

- **TRL: 9** (sensor, surface and air simultaneously)
- **TRL: min. 8** (object classification)

Performance and environment

A wind farm comprises by nature several structures, WTGs and OSSs, which inevitable will reflect energy and potentially cause both dynamic and static reflections within the boundary of the wind farm and proximity to it. These reflections are called "ghosts" and echoes/tracks not representing a genuine real-world object.

A primary radar is unable to assess whether a received echo originates because of multiple reflections between structures being present within the wind farm (ghosts), or a genuine object. By fusing more radar data in the security management system, ghost-tracks are suppressed as these will be unique to a single sensor opposed to genuine objects will be detectable by more sensors simultaneously and reported at the same geographical position.

To achieve coverage backup capability in case of sensor is non-serviceable, means to eliminate false alarms caused by “ghosts” and generally enhance the surveillance of objects of all sized, more primary radar sensors should be simultaneously provide area surveillance and feed data for fusion taking place in the overarching security management system.

The achievable performance of any radar is subject to the environments where operating and impacted negatively by:

- Increasing precipitation (rain and wet show)
- Increasing sea state (function of wind force)
- Electromagnetic environment

The radar performance is not subject to any significant performance degradation due to:

- Ambient lighting (day and night)
- Fog
- Snow

The surveillance radar(s) shall by applied clutter processing maintain a constant false alarm rate with deteriorating environmental conditions to maintain the balance between detecting what is achievable without producing an unacceptable number of alarms to the user.

The sensor system characteristics shall enable the clutter processing to adapt to changing environmental conditions without the need for any user interaction.

Presence of electromagnetic interference, jamming, should be detected and reported by the radars sensors autonomously and reported to the overarching security management system where a warning is raised to the operator.

Radar performance is subject to the installation distance between antenna and transceiver. The interconnection (waveguide) introduces a loss, which impacts the performance envelope negatively. The separation distance should in general be kept as short as possible, especially should the surveillance operational objective also support bird monitoring.

Specification

Surface contacts

The IALA guideline for maritime surveillance applications is a comprehensive document specifying different environments and system characteristics and may serve as a usable guide to specify realistically achievable surface object operational detection and tracking requirements to the surveillance radar(s).

Airborne contacts

A similar realistically achievable performance guideline applicable to elevated objects, aircraft and UAVs, is not readily available in the public domain. However, in the following are realistic detection, tracking and classification examples achievable by affordable surveillance radars.

The airborne objects of interest to be specified when defining the CONOPS of an offshore wind farm are shown Table 7.

The operational environment and environmental conditions are maritime as elaborated in the IALA Guideline referenced above.

The 360° operational achievable concept by a surface and air surveillance radar is included in Table 8. The priority should be object classes T1, T2 and T3.

The surveillance radar should support track classification e.g., “suspected drone”, “aircraft”, “bird” as a minimum, with accuracy and prevision > 90%

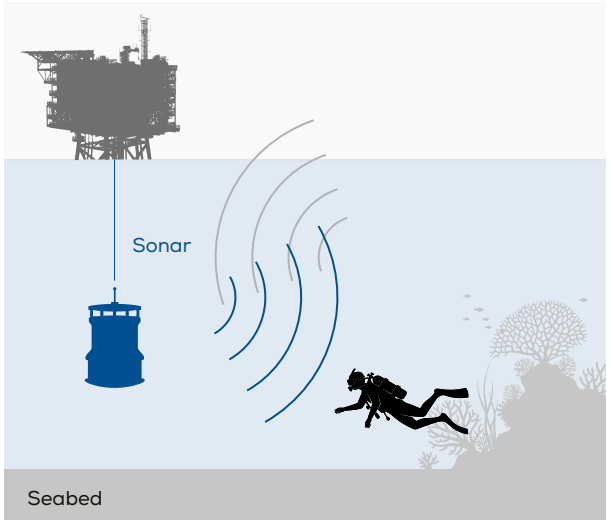
Class 1- Mini UAVs (weight <20 kg) are typically detectable to +10 km for the largest UAVs in this category and small aircraft +20km in environmental conditions without precipitation.

The kinematic object characteristics shall define a velocity span of 0 kts – 70 kts for surface objects and 0 kts – minimum 350 kts for elevated/airborne objects.

B.2.2 Sonar

Sonar head on OSS

FIGURE 14. Sonar head on OSS



A fixed-location sonar is a permanently installed underwater sensing system designed to monitor activity within a defined maritime area. It is typically mounted on the seabed, on piles/pylons, or integrated into offshore structures such as wind turbines or other infrastructure. Its core function is to

transmit acoustic pulses (active sonar) or listen for sound signatures (passive sonar) to detect, classify, and track objects underwater.

With proper frequency selection, power management, and adherence to environmental guidelines, sonars can operate safely and sustainably alongside marine wildlife, making them suitable for offshore infrastructure protection applications.

Sonar sensor systems should conform to regional environmental rules such as:

- Marine Mammal Protection guidelines
- Local environmental impact assessments
- EU MSFD (where applicable)

Sonars may incorporate automatic marine-mammal detection real-time monitoring of ambient noise and adaptive power control that reduces output when sensitive species are nearby.

If marine-mammal presence is high, passive-only or low-power modes can be used, which allow the system to continue surveillance without generating unnecessary noise.

The sonar sensor shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:

- **TRL: 9** (sensor)
- **TRL: min. 8** (object classification)

Performance and environment

A fixed-location sonar operates in a dynamic underwater environment where several interconnected factors influence its detection performance.

The acoustic conditions in the water column play a central role: temperature, salinity, and pressure variations shape the sound-velocity profile and can bend acoustic rays, creating shadow zones or ducts that alter the achievable detection range. Seasonal changes and the presence of thermoclines may further affect how sound propagates. These effects are usually mitigated through adaptive signal processing, continuous environmental measurements, and by selecting waveforms and frequencies that remain stable under varying conditions.

Both the seabed and the sea surface contribute to reverberation and clutter, especially in shallow or complex environments. Hard or uneven bottoms, combined with surface motion from wind and waves, introduce multipath reflections that can obscure weak targets. Modern sonar systems counter these effects with clutter-suppression algorithms, time-varying gain, and by applying beamforming techniques that focus acoustic energy and reduce interference from unwanted directions.

Ambient noise is another fundamental factor. Underwater noise originates from biological sources such as snapping shrimp or fish schools, from human activities including ship traffic or industrial installations, and from natural conditions like rainfall. Elevated noise levels reduce the signal-to-noise ratio and may limit the range at which small or quiet objects can be detected. Systems address this challenge through narrowband filtering, adaptive thresholding, directional receivers, and by adjusting operating frequencies to avoid noisy bands.

The characteristics of the target itself also shape sonar performance. Small, low-reflectivity objects, such as divers or lightweight underwater vehicles, present weaker echoes, and the orientation of the target relative to the sonar can strongly influence how much acoustic energy is reflected back. These variations are managed by employing wideband pulses that enhance the detectability of weak scatterers, using classification algorithms capable of distinguishing subtle signatures, and, in some cases, deploying multi-node or multi-static configurations that observe the target from more than one angle.

The physical surroundings in which the sonar is installed can introduce additional limitations. Piers, foundations, quay structures, and other underwater infrastructure can create persistent reflections or dead zones where detection is limited. These effects are typically mitigated by incorporating geometric models of the installation into the processing chain, defining exclusion areas, and ensuring that the transducer is mounted in a location that maximizes its free acoustic field.

Over time, marine growth can accumulate on underwater equipment, gradually degrading performance. Biofouling alters the acoustic properties of the transducer surface, reduces sensitivity, and increases attenuation. Routine cleaning, anti-fouling coatings, and in some cases self-cleaning technologies help maintain long-term system performance.

The sonar's own hardware configuration further influences overall capability. The choice of operating frequency determines the trade-off between range and resolution, while the quality of the electronics, the dynamic range of the receiver, and the beamwidth of the array shape the clarity and sensitivity of detections. These aspects are optimized through careful design, high-quality components, and periodic calibration.

Even the supporting infrastructure, such as cable runs and power distribution, can affect performance. Long underwater cables introduce attenuation or electrical noise, while electromagnetic interference from nearby systems can contaminate the signal. Fiber-optic links, proper shielding, and electrical isolation are commonly applied measures to maintain signal integrity.

Finally, coexistence with marine wildlife and compliance with environmental regulations influence how the sonar may operate. Power levels, frequency choices, and duty cycles are often constrained to avoid disturbing sensitive species. Adaptive power control, soft-start procedures, and the option to operate in passive or reduced-power modes ensure that the system maintains surveillance capability while remaining environmentally responsible.

In combination, these factors define the performance envelope of a fixed-location sonar. By understanding and actively mitigating environmental, acoustic, structural, and regulatory constraints, modern sonar systems achieve stable, reliable underwater situational awareness in complex maritime environments.

In the Baltic Sea as an example, a fixed-location security sonar can typically detect an open-circuit diver at 250–600 m, with best-case ranges approaching 800–1000 m, and worst-case conditions limiting detection to 80–200 m.

Larger targets such as rebreather divers, Diver Propulsion Vehicle assisted (DPV) swimmers, or Swimmer Delivery Vehicle (SDVs) may be detected from 600 m to 3 km, depending on environmental conditions and system configuration.

Specification

The sonar sensor system shall provide continuous underwater surveillance and be capable of detecting open-circuit divers, rebreather divers, DPV-assisted swimmers, and small SDVs within the performance envelope defined for brackish, shallow, and highly variable acoustic environments.

Under typical e.g., Baltic Sea conditions, the sonar is expected to detect an open-circuit diver at approximately 250–600 meters, with rebreather divers detectable at slightly longer ranges due to their larger and more reflective equipment profiles. DPV-assisted divers should be detectable between roughly 600 and 1,200 meters, while larger swimmer delivery vehicles may be tracked at distances from 1.5 to 3 kilometres depending on aspect and environmental stability.

The sonar shall operate reliably in waters characterized by low salinity, strong and seasonally shifting thermoclines, shallow bathymetry, and high seabed and surface reverberation.

These conditions require the system to employ adaptive signal processing, robust clutter suppression, and beamforming that maintains performance even in multipath-dominated environments. In high-noise areas such as busy ports or harbour approaches, the sonar must compensate for elevated ambient noise levels using dynamic thresholding, narrowband filtering, and directional receiver techniques to preserve target detectability.

The installation location must be assessed carefully, as local seabed type, expected noise sources, depth, and the presence underwater structures directly influence detection geometry and create potential shadow sectors. Seasonal changes in water column stratification can alter detection range significantly, and the system should therefore be capable of maintaining stable performance through environmental monitoring and adaptive processing. Long-term operation requires mitigation of biofouling and steady performance despite varying marine growth, suspended sediment, and local biological activity.

Where marine wildlife is present, the sonar shall operate within environmentally responsible limits, applying power adaptation, ramp-up procedures, and the ability to operate in reduced-power or passive modes when required by regulatory or environmental constraints. Overall, the system must deliver stable, geographically informed performance aligned with the acoustic conditions typical of the Baltic region, ensuring dependable detection of underwater intrusions across a range of diver types and threat profiles.

B.2.3 Ground surveillance / perimeter radar

Ground surveillance radar

FIGURE 15. Ground surveillance radar

A ground-surveillance, or perimeter radar, is a low-power, short- to medium-range sensor designed to detect and track moving objects around a fixed site, such as a critical infrastructure facility e.g., the OnSS or Operational/ Command Centre perimeters.

It scans the surrounding area continuously, typically using a fast-rotating antenna or an electronically steered array, to form a real-time picture of motion on the ground. The radar distinguishes moving targets from stationary background clutter by exploiting Doppler processing and carefully designed waveforms, allowing it to highlight pedestrians, vehicles, and low-flying drones even in environments where visual sensors struggle with darkness, fog, or vegetation.

The ground surveillance/perimeter sensor shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:

- TRL: 9 (sensor)

Performance and environment

Because it operates close to the ground, its performance is shaped by terrain, local vegetation, buildings, and other obstructions that can mask or scatter the radar signal. Atmospheric conditions, ground moisture, and the electrical properties of the soil also influence how well targets stand out from the background. Modern systems mitigate these limitations through advanced signal processing, adaptive clutter suppression, and track-fusion algorithms that stabilise detections over time and reduce false alarms. The perimeter radar is integrated with cameras through the security management system, so that each radar cue can automatically slew an EO/IR sensor to the point of interest for visual confirmation of activities along the perimeter.

In practical use, the radar provides continuous wide-area awareness without depending on light or weather. It delivers early warning of intruders approaching the fence line, identifies movement along access roads or pathways, and supports security personnel by presenting a clear, persistent picture of activity around the protected area. Through its combination of rapid scanning, robust detection in poor visibility, and automated tracking, a ground-surveillance radar becomes a central element in layered site protection, ensuring that potential threats are recognised and acted upon before they reach the perimeter.

Specification

The achievable performance of a ground-surveillance radar against a human is shaped by how the radar interacts with a relatively small, slow-moving object close to the ground, where clutter is strongest.

'Under favourable conditions e.g., flat terrain, low vegetation, stable weather, and an unobstructed line of sight—a modern perimeter radar can typically detect a walking person at distances between roughly 1.5 and 3 km.

Ground clutter is the main limiting factor, because the radar operates at shallow grazing angles where reflections from soil, stones, bushes, and fences can easily mask a weak target.

Advanced Doppler filtering, moving-target indication, and adaptive clutter maps are therefore essential to maintain detection in environments with wind-driven grass, swaying trees, or passing cars outside the fence line. In calm environments the radar can reliably detect a walking intruder even when the person's radial speed briefly drops to near zero, but in difficult areas the radar benefits from continuous micro-Doppler signatures generated by arm and leg movement.

Weather also has an influence, though less dramatically than on optical systems. Heavy rain or wet ground can shorten the effective range slightly, while fog and darkness have no real impact. The type of waveform matters as well: FMCW radars are sensitive to very slow motion and offer fine range resolution, while pulsed Doppler radars provide better long-range detection and stronger clutter suppression.

In practical terms, an operator can expect stable tracking of a person well before the intruder reaches the critical perimeter line. Even at the lower end of performance—dense vegetation, uneven terrain, or strong wind loading the clutter—the radar will typically provide detection between a few hundred metres to around one kilometre, which still gives valuable warning time. In open, controlled areas, the detection distance is long enough that the radar can serve as an outer security layer, cueing cameras for verification long before the intruder becomes visible optically.

B.3 Non-cooperative passive sensors

B.3.1 Surveillance Cameras

Cameras play a central role in the protection of critical infrastructure by providing continuous visual awareness, positive identification, and actionable evidence in both routine and emergency conditions.

The security system architecture shall rely on electro-optical (EO) and infrared (IR) imaging to complement radar, RF-sensors, and access-control systems, creating a multi-sensor solution that detects, tracks, verifies, and documents potential threats at all hours and in all weather.

EO cameras deliver high-resolution daylight imagery that supports long-range observation, target recognition, and forensic-quality recording.

IR cameras extend this capability into darkness, adverse weather, and complex backgrounds by revealing thermal signatures that are independent of ambient light.

When combined on a single gimbal, EO/IR sensor heads provide a persistent 24/7 identification capability, ensuring that any object detected by cueing radar or RF sensors can be quickly assessed by the security system operator.

In an offshore windfarm infrastructure environment cameras enable operators to:

- Verify alarms and distinguish legitimate threats from nuisance activations.
- Identify detected objects such as drones, vessels, or unauthorized personnel.
- Maintain situational awareness across large, complex perimeters and approach routes.

- Record and document events for investigations, regulatory compliance, and incident response.
- Support coordinated response by providing live imagery to command centres and patrol units.

Cameras shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:

- TRL: 9 (sensors)
- TRL: min. 8 (object classification)

Long Range Surveillance Cameras

Long-range combined EO/IR camera systems unite high-resolution electro-optical imaging with powerful thermal infrared sensing on a single stabilized platform.

FIGURE 16. Long Range Surveillance Camera

This dual-sensor approach delivers versatility, persistence, and identification capability across the full spectrum of critical-infrastructure protection, maritime surveillance and C-UAV operations.

Dual-SpecDual-Spectrum Imaging for 24/7 Awareness

- EO (Electro-Optical / Visible Light):
  Provides daylight-quality images with high pixel density, enabling clear detection, recognition, and identification of distant objects, including UAVs, small boats, vehicles, and personnel.
- IR (Thermal Infrared):
  Detects heat signatures independent of ambient light, allowing operators to see in complete darkness, through haze, smoke, and light fog, and in cluttered backgrounds where visible-light contrast is poor.

Performance and environment

The camera performance may be impacted by several factors

Atmospheric & Environmental Factors (EO channel)

- Haze, fog, humidity, dust reduce contrast and limit detection range
- Low sun angles and backscatter can saturate the sensor
- Nighttime performance depends entirely on artificial lighting or starlight/moonlight

Atmospheric absorption & turbulence (IR channel)

- Water vapor and CO_2 absorption bands affect MWIR and LWIR transmission
- Atmospheric turbulence (scintillation) causes image shimmer, especially at long ranges and overheated surfaces (e.g. sea).
- Rain and snow attenuate both EO and IR wavelengths.
- IR imaging relies on thermal contrast. Low ΔT (day-night transitions, cloudy conditions, maritime scenes) reduce detection range of small objects like UAVs.

Lens quality & aperture

- Larger apertures collect more photons → better low-light and long-range clarity.
- High-quality glass and coatings reduce chromatic and spherical aberrations.

Sensor resolution & pixel pitch

- Higher resolution improves recognition/identification.
- Smaller pixel pitch yields more detail but may reduce low-light sensitivity.

Zoom range & optical magnification

- Large optical zoom ratios allow long-range identification but increase sensitivity to vibration and atmospheric distortion.

Cooled vs uncooled IR

- Cooled MWIR sensors: Better sensitivity, longer range, superior small-target detection. More expensive, heavier, require maintenance.
- Uncooled LWIR sensors: Lower cost, no cryocoolers, high reliability. Shorter range and poorer performance against small UAVs, especially in precipitation and snow.

Frame rate & dynamic range

- Higher frame rates improve tracking of fast or erratic UAVs.
- Dynamic range affects performance in mixed lighting (shadows + bright sky).

Specification

The EO/IR camera system shall be capable of detecting a Class-1 mini-UAV, or large bird, at ≥ 5 km when cued by one of the primary security system sensors (surveillance radar or RF-detector) and to allow AI-based video analytics to recognise the object for positive identification by achieving:

- ≥ 25 pixels on the shortest object of interest dimension in the EO channel
- ≥ 15 pixels on the shortest object of interest in the IR channel.

Short Range Surveillance Camera

Short-range electro-optical (EO) cameras form a vital layer the critical infrastructure protection system by providing close-in visual surveillance, rapid verification of alarms, and reliable identification of potential threats.

FIGURE 17. Short Range Surveillance Camera

Positioned along perimeters, access points, rooftops, and sensitive facility zones, these cameras deliver high-resolution imagery that enables operators and automated analytics to detect, classify, and track suspicious activity within the immediate security envelope.

Unlike long-range multi-sensor gimbals, short-range cameras are optimized for high-clarity imaging at distances typically below one kilometre, where detail and responsiveness are more important than extreme stand-off range.

These cameras may operate purely in the visible spectrum or be equipped with NIR/IR illuminators, enabling effective monitoring during low-light or night-time conditions without the need for a dedicated thermal infrared channel.

This allows the system to maintain 24/7 visual coverage while keeping hardware, cost, and power consumption low.

In critical-infrastructure environments short-range cameras support:

- Alarm verification of perimeter sensors, radars, or access-control events.
- Detection and recognition of small intruders, drones, and vehicles within near-field zones.
- Enhanced night-time visibility using IR/NIR illumination for covert or low-light monitoring.
- Accurate tracking and classification through video-analytics and AI algorithms.
- Evidence collection with high-resolution, time-stamped video recordings of incidents.

By combining high-quality EO imaging, responsive autofocus and zoom, and optional IR illumination, short-range cameras deliver dependable situational awareness where it matters most—the immediate vicinity of the infrastructure.

They function as an essential complement to long-range sensors, forming a layered, multi-modal security architecture that protects facilities against a wide range of ground-based and low-altitude aerial threats.

Performance and environment

Short-range EO cameras (with or without IR/NIR illumination) are constrained by a set of physical, optical, environmental, and system-level factors.

These factors define how well the camera can detect, track, and recognise intruders or drones within approximately 0–1000 m.

Low-Light Performance
- Standard EO cameras rely on visible light
- At dusk, night, or backlit conditions, image noise increases, and details disappear unless supported by IR illumination.

IR/NIR Illuminator Range
- IR illuminators have limited effective range (typically 100–500 m)
- Beam spread, atmospheric scattering, and eye-safe limits all reduce usable distance.

Weather, Fog, heavy rain, snow, and haze cause:
- Reduced contrast
- Lower detection probabilities

Specification

The following highlights summarise the key performance and functional specifications expected from a standard short-range EO security camera.
- Reliable detection of humans and small boats within 0–1000 m.
- Effective detection of UASs within 100–600 m, recognition within 50–300 m.
- Nighttime performance with IR/NIR illumination (100–500 m effective)

Hands-on tampering, equipment access, object removal can typically be expected to be identified at 5–20 m.

CCTV

Closed-Circuit Television (CCTV) refers to video surveillance systems that use fixed or pan–tilt – zoom (PTZ) cameras to capture live images for security, monitoring, and operational oversight.

Unlike broadcast television, CCTV transmits video to a restricted audience, such as a security control room, law enforcement, or site operators.

FIGURE 18. CCTV

Applications of CCTV include:
- Monitoring perimeters, gates, fences, and restricted areas
- Detecting unauthorized entry or suspicious movement
- Supporting alarm verification from sensors or access-control systems
- Monitoring key assets and operational zones

CCTVs shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:
- **TRL: 9**

B.3.2 Microphones

Microphone

Acoustic sensors use microphones, or microphone arrays, to detect, classify, and sometimes locate drones based on the sound signatures produced by e.g., UAV motors, propellers, aerodynamics but in general sound standing out from the ambient noise.

These systems listen passively to the surrounding environment and analyse characteristic acoustic patterns to identify abnormal activity.

FIGURE 19. Microphone

Acoustic detection is particularly useful for smaller Nano-UAVs that are difficult for radar or RF sensors to pick up.

Because sound propagation does not depend on visual or RF emissions, it provides an additional detection modality in a layered safety architecture.

Microphones shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:
- **TRL: 9** (sensors)
- **TRL: min. 8** (object classification)

Performance and environment

Acoustic sensors rely on detecting and analysing noise. Their performance depends on environmental conditions, sensor hardware, signal processing and site layout.

Wind turbulence is generally the single largest limiting factor drowning out drone acoustic signatures and reducing detection range from ~300 m to <100 m, but any source impacting the background audible sound will impact the performance.

Wind noise masks low-frequency propeller harmonics. At moderate wind (4–7 m/s) → range reduced by ~50% and at high wind (>10–12 m/s) → acoustic detection becomes unreliable.

Specification

Acoustic C-UAS sensors may realistically achieve:

Typical detection range (mini-UAV):
- 100–300 m (quiet conditions)
- 50–150 m (moderate noise)
- <50 m (industrial/high-wind conditions)

Bearing accuracy:
- ±5° to ±20°, heavily dependent on noise and reflections.

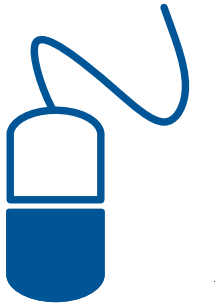
Classification accuracy:
- 70–90% in controlled environments
- 40–70% in noisy environments

B.3.3 Hydrophone

Hydrophone

A hydrophone is an underwater acoustic sensor designed to convert pressure variations in the water into electrical signals, allowing sound to be captured and analysed below the surface. It functions much like a microphone does in air but is engineered specifically for the very different acoustic environment found in the sea. Because sound travels faster and with far less attenuation in water, a hydrophone must be highly sensitive and able to operate across a wide dynamic range, detecting everything from faint biological noise to powerful low-frequency emissions from ships or underwater construction.

FIGURE 20. Figure 1 8 – Hydrophone



Hydrophones may be used individually or as part of an array, where multiple sensors form a spatially distributed listening system that can determine direction, range, and characteristics of sound sources.

They do not emit any sound of their own; they simply listen to pressure variations already present in the water and convert them into electrical signals. Because they don't transmit energy, they are inherently covert, have low power requirements, and are unaffected by the regulatory and environmental concerns that apply to active sonar systems.

Hydrophones shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:

- **TRL: 9** (sensors)
- **TRL: min. 8** (object classification)

Performance and environment

The performance of a hydrophone is ultimately shaped by how well it can distinguish useful acoustic signals from everything else happening in the underwater environment. One of the strongest influences is ambient noise, which may come from wind, waves, rain, ship traffic, biological activity, or distant low-frequency pressure fluctuations. When the natural background is high, faint signals simply disappear into the noise floor. The water itself also shapes performance: temperature layers, salinity gradients, and depth determine how sound bends and refracts, which can either guide sound efficiently toward the sensor or cause it to refract away, creating acoustic shadows.

At greater depths, increasing hydrostatic pressure can affect the sensor's linearity unless it is properly pressure-compensated.

The spectral content of the sound source itself matters: high-frequency signals attenuate quickly in water, making long-range detection difficult, while low-frequency sounds travel much farther but require a sensor with sufficient low-frequency response and stability. All of these factors combine to define the practical limits of what a hydrophone can detect and how reliably it can characterize an underwater sound source.

The distance at which a hydrophone can detect an underwater contact varies enormously because it depends on both the acoustic properties of the target and the surrounding environment. Large vessels such as cargo ships or naval surface ships radiate strong low-frequency noise from engines, propellers, and hull vibrations, and these frequencies travel efficiently through water. In deep, stable water layers with few thermocline disruptions, their signatures can often be detected tens of kilometres away and sometimes far beyond that when conditions are favourable.

Submarines present a very different picture. Modern submarines are engineered to be exceptionally quiet, producing far less broadband energy than commercial ships. Their detectable range may shrink to just a few kilometres, and in challenging acoustic conditions, such as shallow, noisy coastal areas, sometimes only a few hundred meters. Older or less well-maintained submarines can be audible at significantly longer ranges, especially if they operate at higher speeds where flow and machinery noise increase sharply.

Smaller sub-surface contacts, such as divers, swimmer delivery vehicles, or autonomous underwater vehicles, produce much weaker acoustic signatures. A diver using open-circuit breathing can sometimes be heard at modest ranges because the exhaust bubbles generate broadband noise, but even then, the range is usually short, often under a few hundred meters (100 – 200 m) and strongly dependent on background noise. Rebreather divers are far quieter, typically reducing the detection range to tens of meters or less unless the hydrophone is very close or the water is exceptionally still.

Mechanical systems like small Remotely Operated Vehicles (ROVs), Autonomous Underwater Vehicles (AUVs), or electric thrusters tend to sit somewhere in between. Their electric thrusters and propellers might be detected at a few hundred metres in calm water, but in the presence of wave noise

or shipping they often disappear into the background at distances beyond 100–200 m.

Overall, long-range detection is associated with large, loud, low-frequency sources in deep water, while short-range detection applies to small or deliberately quiet objects, especially in shallow or turbulent environments where the ambient noise masks subtle acoustic signatures.

Specification

A suitable hydrophone for detecting a range of subsurface contacts should be a passive, wide-band underwater acoustic sensor capable of capturing low- to mid-frequency sound with high sensitivity and low self-noise.

It should employ a pressure-tolerant piezoelectric element with an integrated low-noise preamplifier to preserve weak signals and maintain a usable dynamic range in both quiet and noisy environments.

The device must withstand long-term immersion at the intended operating depth and include proper mechanical isolation to minimise vibration-induced noise, while offering a frequency response that covers the dominant tonal and broadband components produced by ships, submarines, underwater vehicles, and divers.

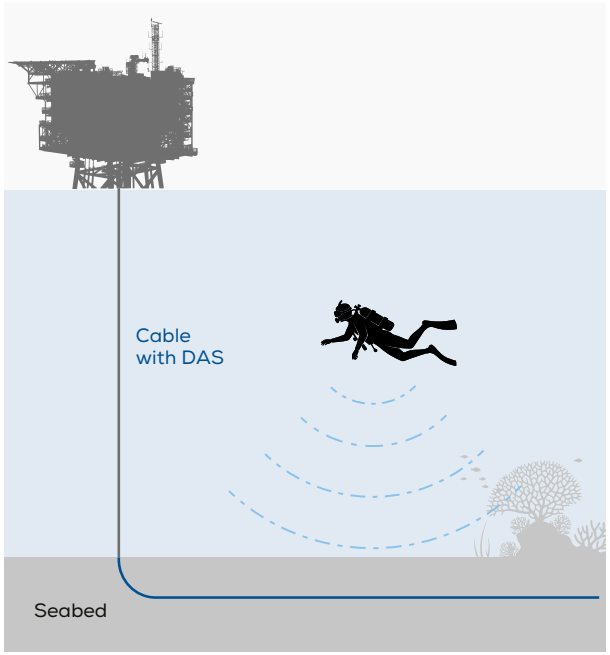
The processing shall enable stable calibration and predictable behaviour across the full range of temperatures, salinities, and pressures encountered in the operational area.

B.3.4 Distributed Audio Sensing (DAS)

DAS sensing on export cable

A Distributed Acoustic Sensing (DAS) sensor for sub-surface surveillance is, in essence, a very long and extremely sensitive “virtual array” created along an optical fibre (telecom-grade single-mode fibre with no excessive optical splices or bends).

FIGURE 21. DAS sensing on export cable



Instead of relying on discrete hydrophones or geophones, the fibre itself becomes the sensing element: tiny strain changes induced by sound or vibration, whether from a diver, swimmer, boat, vehicle, or other underwater/ underground activity, modulate the backscattered light inside the fibre. By interrogating the fibre at high speed, the system reconstructs a continuous line of thousands of sensing points, each behaving like an individual acoustic/ elastic sensor.

The readily available optical fibres within an offshore windfarm can be assigned as a distributed acoustic array and coupled to the data processing unit (interrogator)

In general terms, such a system provides persistent, passive-like monitoring of a large area without emitting any energy into the environment. The fibre can be buried shallowly in the seabed, placed in conduits, or laid directly on the bottom; its detection mechanism is based on elastic wave coupling between the surrounding medium and the fibre jacket. Because the fibre is continuous, the system naturally provides very fine spatial resolution, often metres or less, along lengths from a few kilometres to tens of kilometres. This gives a surveillance operator a detailed “picture” of where signals originate, how they move, and how they evolve in time.

A DAS sensor’s behaviour is characterised by its ability to detect minute vibrations, but its performance ultimately depends on how well the energy couples into the fibre. Soil type, sediment softness, burial depth, water depth, temperature fluctuations, and background ambient noise all influence the quality of the signal. When the environment is favourable, the system can detect subtle acoustic signatures, distinguishing, for example, the characteristic temporal patterns of a diver’s fin strokes, a swimmer’s movement, the cavitation of a small boat propeller, or the mechanical vibrations from underwater infrastructure.

For sub-surface security, the strength of a DAS system lies in its ability to cover large perimeters continuously with minimal infrastructure. It offers detection, localisation along the fibre, and often classification of events based on their

vibration signatures. Compared to traditional point sensors, it is less prone to single-point failure and can be integrated unobtrusively. At its core, a DAS sensor for sub-surface surveillance is therefore a silent, persistent, distributed "listening line" capable of detecting and tracking a wide spectrum of underwater or underground activities across long distances.

The DAS shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:

- TRL: 9 (sensors)
- TRL: min. 8 (object classification)

Performance and environment

The maturity of DAS for detecting small sub-surface objects is mixed: the core technology is very mature, but the application to very weak acoustic/vibration targets is still evolving.

DAS itself is a high-maturity, field-proven technology. Telecom-grade fibres, coherent interrogators, and signal-processing pipelines are fully industrialised and are routinely used in oil & gas, border security, rail monitoring, structural health monitoring, and pipeline protection. The ability to

detect large or high-energy sources—ships, vehicles, digging, pipeline impacts, is extremely robust and operationally deployed.

When it comes to small objects underwater is where maturity depends heavily on physics, not just technology.

Small acoustic or vibration signatures—like a diver, swimmer, small DPV, or a light object moving on the seabed, are detectable, but with constraints.

If the fibre is laid loosely on soft mud, coupling is weak and small signatures leak away. If the fibre is buried shallowly in sand or well pinned to a hard seabed, sensitivity increases dramatically. The best results come when the fibre is mechanically well bonded to the medium.

Unlike a hydrophone, which reacts to pressure waves in water, a DAS fibre reacts to strain in the fibre coating. This means: Low-frequency, high-energy events are very easy. High-frequency, small-amplitude diver noise is more challenging and range-limited.

TABLE 6. DAS performance overview

Object Type	Realistic detection maturity	Typical detection distance (m)
Small boat hull vibration	Very mature	Hundreds of metres to kilometres
DPV / SDV motor	Mature	200 – over 600
Open-circuit diver (bubbles, fin strokes)	Moderate maturity	50 – 200
Rebreather diver	Challenging	20 – 80
Slow-moving objects on seabed	Mature	50 – 300 (depending on contact)
Very small objects without direct fibre contact	Early-stage	Highly variable

Modern DAS interrogators can technically operate on tens of kilometres of fibre, but the effective detection of small sub-surface targets is only reliable over a much shorter portion of that range.

Long-range performance for strong signals for strong vibration sources such as:

- small/medium boats
- anchors and chains
- vehicles (if the fiber is buried)
- heavy tools or construction noise
  - › Effective range along the fiber: 20–50 km from the interrogator.

Performance for small sub-surface targets (divers, small DPVs, small disturbances)

- Open-circuit diver noise (fin strokes, bubbles, body movement)
  - › Effective range along the fiber: 3–8 km from the interrogator

- DPV / SDV electric motor
  - › Effective range along the fiber: 5–15 km depending on coupling and seabed type

- Rebreather diver (very weak acoustic/vibration signature)
  - › Effective range along the fiber: 1–4 km in the best cases

For small, low-energy underwater objects such as divers, rebreathers, and light seabed disturbances, only the first 5–15 km of the fibre (measured from the interrogator) provides reliable detection and classification.

For moderate-energy targets like DPVs or small electric motors, useful performance out to 5–15 km, sometimes a bit more if coupling is achievable.

For strong, high-energy events—boats, anchors, heavy machinery, DAS remains effective far beyond the small-target

zone, often out to 20–50 km on a single uninterrupted fibre, depending on interrogator quality and fibre condition. Beyond these ranges the system will still collect data, but weak signatures will be lost in optical noise.

The applied AI models are generally deemed mature enough to distinguish man-made noise from background noise in real time, provided:

- The fibre is well coupled
- The installation environment is characterized by a detailed understanding of how the local seabed, water, infrastructure, and ambient noise conditions interact with the fibre. This is necessary because DAS does not measure sound in the same way everywhere, the environment shapes the signal dramatically.
- and the model is trained or adapted to local conditions.

DAS is however still not a replacement for a dedicated hydrophone array when very weak, distant targets must be detected.

For very weak underwater signatures required for a comprehensive security management system, DAS is still considered a complementary sensor, not a primary one, in modern security systems.

Specification

A Distributed Acoustic Sensing system for offshore security shall use a continuous single-mode fibre integrated along the subsea cable and an interrogator capable of high-coherence operation, providing at least 5–15 km small-target sensitivity and 20–50 km large-event coverage.

The installation must ensure strong mechanical coupling to the seabed or cable armour, minimal splice losses, and stable thermal conditions. The solution shall characterise local seabed types, ambient noise, and anthropogenic activity to tune detection thresholds and AI classifiers.

The system shall reliably detect, localise, and classify man-made disturbances such as diver activity, cable tampering, anchors, dragging gear, and vessel intrusion, with real-time alarm generation and low false-alarm rates.

Operational limits, seasonal noise variation, weak-target performance, and zones of reduced fibre coupling must be clearly stated in the specification.

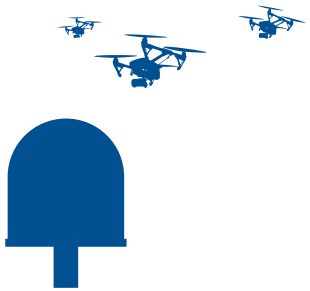
B.4 Cooperative passive sensors

B.4.1 RF Sensors

RF Sensor

RF (Radio Frequency) C-UAV sensors are designed to detect, identify, locate, and sometimes disrupt unmanned aerial vehicles by analysing the radio signals used for their control, navigation, and data transmission.

FIGURE 22. RF Sensor



Unlike radar or optical sensors, RF C-UAV sub-systems rely on passive listening, meaning they do not emit energy but instead monitor the electromagnetic environment for signals characteristic of drones and their operators.

Radio silent UAVs, or unknown UAVs, will not be detectable using this technology.

The RF sensor may be integrated with various effectors targeting either the UAV links or GPS. Effectors supporting countering UAV intrusion are not addressed in this paper.

An RF C-UAV sensor supports four main functions complementing the radar sensors in a security system:

Detection

- Continuously monitors the RF spectrum for signals associated with drone activity.
- Identifies common drone communication protocols, Wi-Fi links, telemetry channels, and remote-controller signals.
- Detects both the drone and, in many cases, the operator's remote controller.

Classification / Identification

- Matches detected signals against a library of known drone protocols and manufacturers.
- Determines whether the signal corresponds to:
  - A legitimate device (e.g., Wi-Fi, access point, industrial radio)
  - A consumer or commercial UAV
  - A custom/modified drone
- Identifies drone model families when possible.

Localization

- Uses direction-finding or time-difference-of-arrival (TDoA) techniques to determine the bearing and/or position of:
  - The drone
  - The drone pilot / remote controller

The RF sensor shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:

- **TRL: 9** (sensors)
- **TRL: min. 8** (link library)

Performance and environment

RF C-UAV systems operate in dynamic, heterogeneous radio-frequency environments and rely on receiving emissions from the drone or controller. Obstacles between the sensor and UAV influence signal strength, which is used to determine presence of a UAV or not.

The received signal strength emitted by a UAV is used to positively identify the presence. The permissible UAV radiated signal strength is mandated by regulations. UAVs operating legally within the European area must comply with ETSI requirements but a similar UAV but compliant with FCC legislation will radiate more energy and hence be detectable to extended ranges.

The performance is directly influenced by physical surroundings, RF congestion, propagation characteristics, atmospheric conditions, interference sources, and the deployment geometry of the sensors.

Unlike radar, or optical sensors, RF propagation is less sensitive to weather but still affected by:

- High humidity → increased absorption at certain microwave frequencies
- Heavy rain → attenuation in higher bands
- Temperature inversions → signal ducting or nulling
- Heat shimmer → minor effects on high-frequency line-of-sight links

Congested environments may create shadows and extensive reflection, scattering, and absorption of RF signals i.e., wind turbines, structures, can cause multipath effects, which like radars may generate ghost bearings, unstable angle-of-arrival (AoA), or “bouncing” signals that degrade localization accuracy. The mitigation solution is equal to radar by fusing more RF sensor sensors covering the same volume enabling decorrelating ghosts in the multi sensor fusion which is part of the overarching security management system.

Any transmitter e.g., Wi-Fi, Bluetooth, LTE/5G small cells, industrial wireless devices, and consumer electronics create constant background RF activity, which increases the noise floor, reducing the sensor’s ability to detect faint drone signals as the same frequency bands are utilized for these services as well as the drone radio control links.

The operational impact of a congested electromagnetic spectrum is misclassification, masked signals, and difficulty distinguishing UAV signatures from background activity.

The effectiveness of RF C-UAS sensors depend heavily on the height above ground and surrounding structures. A poor placement can reduce detection range by 50–80%.

As UAVs continuously evolve, new control protocols emerge which will be unknown to the RF sensor system, until trained to recognise. It is therefore imperative the model libraries are continuously updated up to 4 times a year to stay on par with the advances in UAV evolution.

Specification

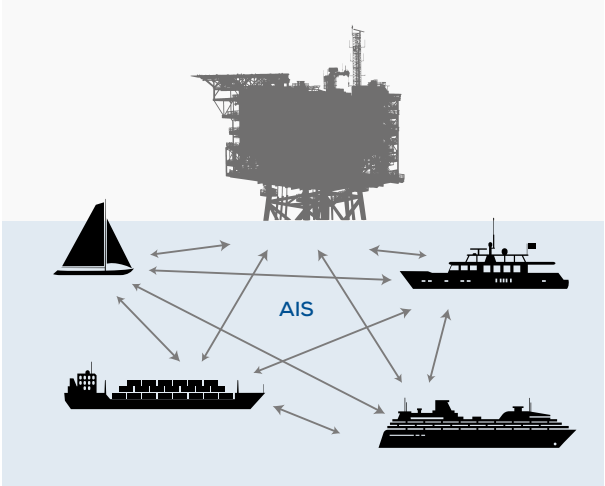
Typically, detection range is around 4km extending to 7km in best case for UAVs operating in accordance with the European ETSI legislation.

B.4.2 AIS

AIS receiver on OSS

The Automatic Identification System (AIS) is a maritime communication and tracking technology used to improve safety, situational awareness, and vessel coordination at sea. AIS-equipped ships and coastal stations automatically broadcast and receive information such as vessel identity, position, speed, course, and navigational status. These messages are transmitted over VHF radio channels and shared in real time with nearby vessels, ports, security management system and traffic-management authorities.

FIGURE 23. AIS receiver on OSS



AIS supports collision avoidance, traffic monitoring, coastal surveillance, and maritime security by providing a continuous electronic picture of vessel movements.

It forms an essential element of modern maritime domain awareness systems and integrates seamlessly with radar, camera systems, and vessel traffic services (VTS) to enhance operational decision-making.

An AIS receiver is considered an inexpensive sensor potentially confirming the identity of an object detected by one of the non-cooperative sensors.

The AIS receiver shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:

- TRL: 9

Performance and environment

AIS is considered useful, but:

- Performance is affected by VHF range, congestion, equipment quality, and environmental interference.
- Security is weak because AIS messages are unencrypted, unauthenticated, and easily manipulated.
- AIS alone cannot be trusted for security or surveillance. It must be validated using:
  - Radar
  - EO/IR cameras
  - RF direction-finding

AIS performance depends on several operational, environmental, and technical conditions:

- Weather inversions or ducting
- Sea clutter
- Traffic density as several vessels may transmit simultaneously with congestion as consequence
- Saturated or interfered by strong nearby transmitters
- Intermittent updates 2-30 sec. intervals
- Possible data manipulation
- Sensitive to GPS spoofing/jamming/hacking

AIS is best used as one layer in a multi-sensor security management system.

Specification

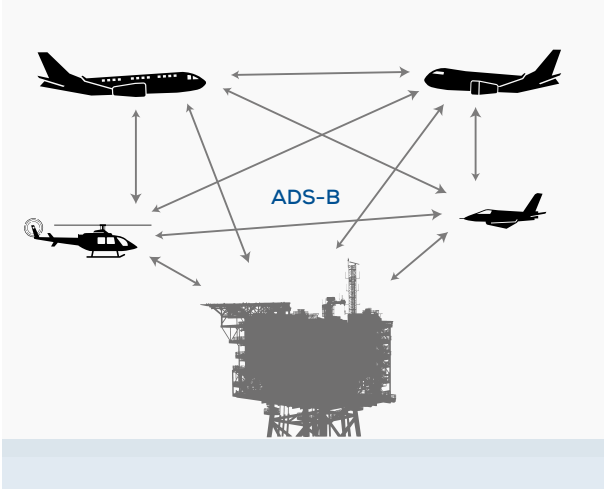
Typical coverage range: 10 - 20 nautical miles.

B.4.3 ADS-B

ADS-B receiver on OSS

Automatic Dependent Surveillance–Broadcast (ADS-B) is an aviation surveillance technology in which aircraft broadcast their own position, velocity, and identification information using onboard GPS and a dedicated transponder.

FIGURE 24. ADS-B receiver on OSS



ADS-B is a self-reporting system, meaning the aircraft continuously transmits its data without needing a ground request.

ADS-B is used by air traffic control, airports, air-defence units, and nearby aircraft to improve situational awareness, safety, and traffic separation.

An ADS-B receiver is considered an inexpensive sensor potentially confirming the identity of an object detected by one of the non-cooperative sensors.

The ADS-B receiver shall be fielded supporting similar operational objectives in a maritime environment and have a Technology Readiness Level of:

- TRL: 9

Performance and environment

ADS-B performance depends on RF propagation, equipment quality, antenna height, message characteristics, traffic density, and environmental conditions.

Since ADS-B is a broadcast technology, the receiver must extract data from a crowded RF environment with strict timing requirements.

The factors impacting ADS-B is largely like the ones applicable to AIS

Environmental Conditions

The environmental impact of humidity, rain, and atmospheric effects is generally minor, but noticeable in very long-range reception (>300 km)

Specification

Typical coverage range: 100 - 200 nautical miles.

B.5 Access Control & CCTV

Access Access Control and CCTV can be used for OSS', WTGs, Landfall cable wells, OnSS' and Operation Centre to allow access and give alarms in case of unauthorized access through a door or a virtual line.

B.5.1 Access Control

FIGURE 25. Access control credentials

Advanced access control with video and two-way voice at entry doors. Can give alarm in case of unauthorized access through a door.

Possible user credentials: Mobile phone, Access card, Key Fob.10

Annex C – Cost breakdown

The cost is organised into packages aligned with the equipment sets described in the use cases. Because multiple vendors can supply each sensor type and configurations vary by site, the figures are presented as percentage shares of the total system cost rather than fixed unit prices.

There is no one-size-fits-all solution. Final design and cost depend on site-specific parameters such as scale, coverage requirements, sensor mix, integration, installation conditions and support.

For itemised cost information, a bill of materials and a configuration tailored to your site, please contact Terma A/S to discuss scope and requirements.

C.1 Cost breakdown use case 1

Description	Percentage of total price
Operational system software + hardware, project management and services, training, warranty	10-20 %
Air and Surface domain- Radars, Cameras, CCTV and Access control package.	30-40 %
Subsea domain – DAS package.	40-50 %
Total ROM Price EUR (thousands)	**4,000**

C.2 Cost breakdown use case 2

Description	Percentage of total price
Operational system software + hardware, project management and services, training, warranty.	10-20 %
Air and Surface domain- Radars, Cameras, CCTV and Access control package.	40-50 %
Subsea domain – DAS package.	50-60 %
Total ROM Price EUR (thousands)	**11,500**

TERMA

ALLIES IN INNOVATION

Terma A/S
Hovmarken 4, DK-8520 Lystrup, Denmark
www.terma.com