ladar ltd

FILLING THE OFFSHORE FACILITY AND WINDFARM SECURITY PROXIMITY GAP

As we look to offshore energy infrastructure and windfarm security, let us consider the expanded use of 'smart sensor' technology originally conceived for AI-supported remote maritime surveillance in situ at offshore facilities. There has, in recent times, been an uptick in global conflicts, most notably witnessed on September 26, 2022 with the Nord Stream 1-2 pipeline incident and in early August 2023, with the low profile, fast-moving, semi-autonomous operated drones that severely damaged two ships while at anchor/in the harbor. Other notable incidents include a military Ro-Ro ship, a coastal chemical/product tanker, Organized crime threats, Piracy and Terrorism. Considering all these threats and the inherent risks, offshore infrastructure security has quickly become a much higher EU and industry priority.

With this heightened security importance, the EU focuses on improving its well-established, interconnected, and unified border security network headed by the European Border and Coast Guard Agency (also known as FRONTEX) and cooperating with other EU agencies in the different member and associated countries.

Terrorists and potentially government-sponsored groups have planned and conducted successful attacks on critical maritime energy infrastructure; many were successful, while intelligence, observation, and on-scene interdiction prevented other lesser-known attacks. To a great degree, all rely on receiving real-time, on-scene observational information, of which the most accurate is currently obtained from air surveillance, satellite observation, and on-scene patrol boats.

At risk are billions of euros in costs and the global interruption of critical economic activities and energy security. The EU security agencies, such as Frontex, Coast Guards, Border police, and Interpol (International Criminal Police Organization), to name a few, have raised the importance of local surveillance and are active and advanced in preparing for coastal and near-shore security.

Enhanced Surveillance to Safeguard Offshore Facilities and Windfarms

What is 'smart sensor' technology? It can be described as a fusion of highly accurate optical, thermal, and lidar sensors, that operate autonomously, providing alerts, object detection information, and assessment. Smart sensor technology is most effective when interconnected to coastal security command and control capability. Using Artificial Intelligence, object identification and threat assessment become a reality and enable risk assessment upon which further actions can be decided.

Offshore facilities have been with us for many decades. Now, similar Windfarms and the Floating Storage and Regasification Units (FSRU) for LNG downstream to Europe are becoming increasingly common in remote areas and near major ports and heavy traffic shipping routes. Concurrently, we must include the security risks of underwater gas pipelines, power cables, and data networks that often extend across national borders and span oceans.

The European Union has recognised this as a pan-national security risk and has established the 'European Maritime Security Strategy,' which aims "to ensure a peaceful use of the seas and safeguard the maritime domain against new threats." These types of EU initiatives have taken

on much higher importance by the recent incident to the Nord Stream 1-2 gas pipelines in the Baltic Sea, which the Swedish Security Service has termed an act of "gross sabotage." While underwater and seabed security had been a concern for governments prior to this incident, the Nord Stream explosion has sharpened international focus on the vulnerability of underwater energy and communication networks.

The next stage of 'smart technology,' or something we can call an "underwater coastguard," includes coastal networks of sensors that detect, alert, and have advanced threat analysis capabilities. The coverage of this security network must be capable of detecting submerged, semi-submerged, and floating constructed human-made objects, as well as divers. Bad actors adopting autonomous and semi-autonomous fast-speed and semi-submerged drone technology has increased the success of these threats.

The need for offshore facilities to augment the Coast Guard's broad coastal surveillance has also increased in conjunction with government-sponsored security. Until now, security depended on the border agencies to alert risks and left the commercial facility operators to implement security, either staffed, local, or remote technology-based, to the structures. The commercial security application varies when considering cost and whether the facility is operational, in production, staffed full-time or partial, or unmanned. As a result, there are minimal security detection capabilities and only mandated emergency response capabilities.

We have conducted research about offshore safety and security, you may reference Safety of offshore oil and gas operations - Energy (europa.eu) for related EU directives, as well as an August 2022 summary report "National Approaches Marine Uses" by HaskoningDHV Nederland B.V. which addresses the many aspects of marine security and safety. What we have found is that there are no requirements or guidance on how to address security guidelines nor are there standards regarding facility related security-threat detection. We support the notion that the most effective security measures must be a joint effort and involve cooperation between the government and commercial sectors. Although improving coastal security is stated, it is restricted by limited government security surveillance and patrol resources and the national security prioritizing of maritime threats. My interest lies in understanding what we are doing about the new threats.

The fact remains that coastal security is based on shore-based long-range radar and AIS for ship traffic management and other port/maritime traffic control priorities. Shore-based radar has served us well for decades, and its accuracy has proven a reliable tool for ship traffic management. There are two primary areas that we need to address when working with radar: first, radar has some well-known limitations that we have learned to work with. It is a 'line of sight' detection technology, so the near proximity and far distance limit its detection accuracy; it relies on the quality of the object to reflect the radio waves, and its accuracy is susceptible to weather and sea state.

Securing Offshore Facilities and Windfarms Against Potential Risk

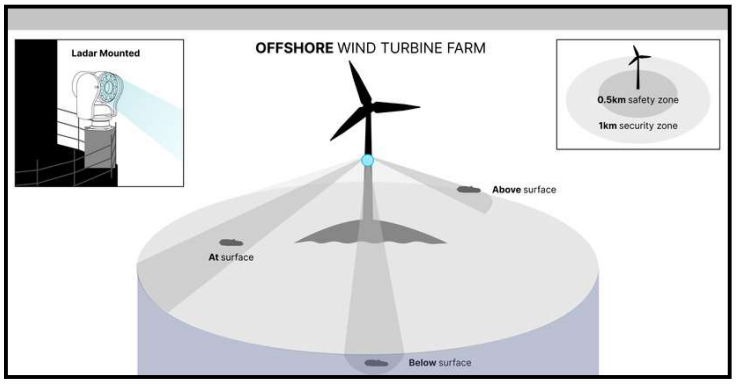
So, what is the risk at a local floating energy facility or windfarm? If we rely solely on offshore facility-based radar and AIS, we can be sure that routine traffic can be identified, and security notifications can be observed and followed. The gap lies in the water interface and below-water security threats. Radar, thermal, and optical sensor technology do not detect semi-submerged objects well and cannot detect underwater objects at all.

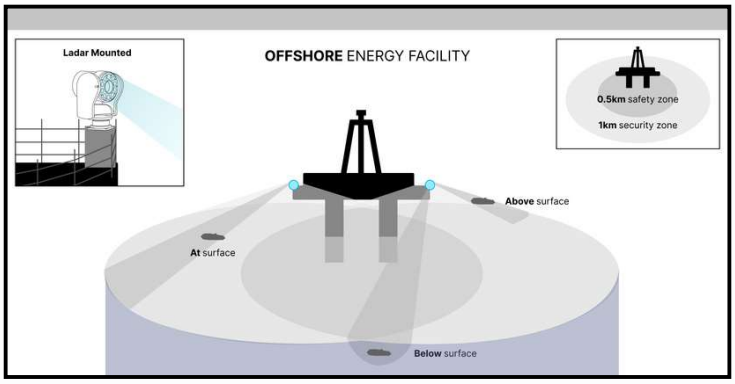
Autonomous underwater and semi-submerged vehicles or 'drones' intentionally deployed with harmful intent pose a significant threat to offshore critical floating energy infrastructures and wind farms. The threat of malicious intent drones is broad and includes port facilities, ship anchorages, and LNG, FSRU & OIL energy terminals, with possibly disastrous effects. Here are some considerations regarding the potential risks: an underwater drone could be used to deliberately collide with a platform and cause extensive physical damage. Such actions could disrupt operations, compromise physical integrity, and lead to costly repairs. Sabotage is another concern: In the wrong hands, underwater drones could be used for sabotage, deploying explosive devices, or attaching damaging objects to the infrastructure, potentially causing significant harm or disruption.

Proximity 'Gap' Enhanced Detection

So, where is the 'proximity gap'? The gap includes the radar coverage area, which is not designed for or is effective at detecting the near proximity area below the radar "line of sight," where submerged or semi-submerged objects are not detected. When I consider near proximity object detection, what does it mean?

With this risk 'gap' in mind, I found a direct adaptation of sensor AI and data fusion technology in the Ladar™ Sensor Suite as a near proximity detection technology to fill the object detection gap of submerged and semi-submerged objects and works well together with the radar's near proximity detection limitation. In other words, the gap refers to the proximity of 100 meters (about 328.08 ft) and beyond three nautical miles.





By using area scanning and multiple sensors such as Lidar laser, high-definition Optical, and Thermal cameras, and the sensors are AI-assisted for the assessment, detection, and precise location of objects, threats, mammals (whales), semi-submerged objects (containers or drones), human-made debris, and small boats (fishing boats and gear). This information activates an appropriate level of communication or alarm to the security control room facilities ashore, the bridge on a rig, FSRU, floating infrastructure, or a control room team at a shoreside control station. By adopting the latest detection technology, we can close the 'gap' of proximity detection and reduce reliance on the functions and limitations of radar.

While initially developed to aid shipping and navigation activities, CEO Jorgen Grindevoll of Ladar Ltd says, "LADAR has smart technology that is directly applicable to monitor the security zones offshore autonomously." Grindevoll also highlights that the demand for remote 'smart' security sensing features is pushing technology innovation ahead. The latest area we have seen an increased demand for is now the floating windmill farms for green change, and the other critical energy infrastructure such as Floating Storage and Regasification Units (FSRU) are now fueling Europe with natural gas.

Adopting the latest artificial intelligence-supported sensor detection technology closes the 'gap' of proximity detection and lessens the reliance on radar. Offshore facility operators and Windfarm operators need to leverage smart detection technology to address the detection and identification of objects above the water, the surface interface, and below water.

Reinforcing Offshore Infrastructure with 'Smart Sensor' Technology

Overall, due to the increasing conflicts and security risks in the world, maritime security has gained prominence, especially in the context of safeguarding offshore infrastructure. The vast and remote European coastline necessitates a unified approach to border security, which is being addressed through the establishment of FRONTEX and the use of 'smart sensor' technologies.

In conclusion, there is a need for improved maritime security, especially in protecting critical energy infrastructure. The solution can effectively involve utilizing 'smart sensor technologies' and adopting advanced detection methods to address security gaps. To achieve this, cooperation between government agencies and commercial sectors is necessary to tackle maritime security challenges effectively.

Captain Jorgen Grindevoll, CEO, encourages you to look to future developments and imagine innovative technologies with us. We can be reached at info@ladar.co.uk.

> "LADAR has smart technology that is **directly applicable to monitor the security zones offshore autonomously.**"
>
> **Jorgen Grindevoll, CEO**