CRITICAL INFRASTRUCTURE PROTECTION - ENERGY

COMPLETE SITUATIONAL AWARENESS ACROSS AIR, SURFACE, SUBSEA, AND PERIMETER

Offshore Energy Is Now Part of National Security

For decades, offshore installations were engineered to survive extreme weather, corrosive saltwater, and mechanical stress. The threats were environmental. The defenses were structural.

That era is over. Offshore wind farms, oil platforms, and subsea cable routes are now classified as critical national infrastructure across the globe. They are targets for sabotage, espionage, and hybrid operations that blend military tactics with plausible deniability.

Today, the challenge is not a single dramatic attack but coordinated threats that go under the radar – quite literally.

A vessel deviating from the shipping lane. A small drone approaching low over the water. Unusual activity beneath the surface. Each event, taken alone, appears routine. Together, they form a coordinated operation. And most security setups would display them as three separate, low-priority alerts on three separate screens. No correlation. No escalation. No time to respond.

The question for energy operators is no longer whether to protect these assets. It is how.

3,000+
sensors fused in a single deployment

Sensor agnostic
no vendor lock-in

Ultra-low false alarm rate
through intelligent sensor fusion

Multi-domain
multi-layer protection

Full Situational Awareness Across Every Domain

Protecting an offshore installation means monitoring threats with wide-area surveillance and long-range detection across domains: air, sea surface, and sub-surface. With no physical perimeter to rely on, our systems use geofencing to focus awareness and present the a comprehensive situational image of every event – in a single operator view, in real time.

T.react CIP is Terma's critical infrastructure protection platform. It fuses data from multiple sensor types into one operational picture, correlating events across domains so that a coordinated threat is visible as a coordinated threat.

The platform integrates surface and air surveillance radars, electro-optical and infrared cameras, AIS and ADS-B transponder data, hydrophones, sonar, and distributed acoustic sensing (DAS). Every source feed into one unified interface. The operator sees the tracks of flagged events tracing the object, and based on a customizable rule engine, our system classifies and prioritizes the events across all domains.

This multi-domain correlation is what separates genuine situational awareness from a collection of sensor feeds. A vessel, a drone, and a subsea anomaly are no longer three unrelated data points. They are one picture. And that picture gives the operator the time and context to identify, act, and document.

Your Sensors. Your Architecture.

Offshore energy operators rarely start from zero. Most facilities already have cameras, radar, AIS receivers, or access control systems in place. Replacing them is expensive, disruptive, and unnecessary.

T.react CIP is sensor agnostic.

It integrates the sensors you already have alongside any new additions, regardless of manufacturer. Open architecture means no vendor lock-in, no proprietary sensor requirements, and no forced upgrades.

The platform scales from a single installation to a distributed network of wind turbines, on- and offshore substations, and production platforms across hundreds of square kilometers.

Nautical Charts and Zone Intelligence

The system overlays live sensor data onto detailed nautical charts showing shipping lanes, buoys, depth contours, and exclusion zones.

Operators can define rules for specific areas: flag any vessel that leaves the shipping lane, escalate any approach from a designated direction, or whitelist known service traffic. Operators can setup virtual perimeters and multi-layer alarm zones that enable early notifications and differentiate normal from suspicious behavior while minizing false alarms.

These rules adapt to the threat picture. Instead of reconfiguring the system, the operator switches between pre-defined security profiles matched to the current threat level. Each profile carries its own detection thresholds, alarm rules, and escalation protocols.

Focus on the Threat, Not the System

An offshore control room should not require sensor specialists. The people monitoring these facilities are security professionals, not radar engineers. They need a system that presents clear, actionable information and lets them focus on making security decisions.

T.react CIP is designed around that principle.

The platform operates the sensors autonomously, handling detection, tracking, classification, and correlation without manual intervention. When something requires attention, the system delivers a prioritized alert with the context the operator needs: what the object is, where it came from, how it is behaving, and why it matters.

Radar Doppler classification and advanced rule engine removing sea clutter keeps the false alarm rate low. This matters especially for offshore, where wind, waves, sea spray, and bird activity would overwhelm a conventional system with nuisance alerts. Automatic bird detection, critical at wind energy sites, filters out avian traffic without masking genuine threats.

Because of the system's comprehensive automation and intuitive interface onboarding new operators accelerate significantly, as they can focus on event mitigation rather than datahandling. Institutional knowledge lives in the platform's rules and profiles, not in the heads of individual staff members who might rotate, retire, or relocate.

Detect, Track, Classify, Report and Act

The principles behind a security concept for critical infrastructure follow a straightforward sequence: detect, track, 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 four steps, and on how they enable and support effective action when an incident occurs.

Built for Offshore and All Weather

Offshore energy installations face North Sea storms, Gulf humidity, Arctic ice, and persistent salt corrosion. Security systems that work reliably onshore can fail at sea, where extreme weather, limited power budgets, and remote and constrained locations are the baseline conditions.

T.react CIP is built for this reality.

The architecture is modular and scalable, perfectly adapted to accommodate offshore wind farms that span hundreds of square kilometers with dozens of turbines, transformer stations, and cable routes. T.react CIP scales across these distributed assets without requiring a dedicated system per structure.

Installation is designed to minimize operational disruption. A remote configuration capability and flexible framework ensure seamless deployment and maintenance. This architecture allows the system to adapt to varying security requirements through simple, high-level adjustments. And the entire system is cyber-hardened and built to the IEC 62443 security standards.

T.react CIP correlates data from radar, AIS, ADS-B, cameras, sonar, drone detection systems, and other surveillance sources into one unified operational picture

Early Warning, Deterrence & Documentation

Protection does not begin when an incident occurs. It begins long before.

T.react CIP detects, tracks and classifies threats at sufficient range to give the operator time to alert authorities, initiate response protocols, and, where mandated, activate countermeasures. Equipped with an Open API, the system ensures seamless integration with PSIM platforms and national security infrastructure.

Persistent, visible surveillance also changes the adversary's calculation. When a threat actor knows the facility is being continuously monitored across every domain, the operational risk for the attacker increases. The system deters before it detects.

And when incidents occur, the platform's scenario-based recording and replay- alongside an Enhanced Report and Evidence Manager - provide forensic-grade documentation of every detected event. This ensures total visibility into concurrent attacks, capturing every operator action and system alert in real time. Because post-incident analysis and regulatory reporting are native to the platform, legal evidence is integrated by design rather than added as an afterthought.

T.react CIP Unique Capabilities

Security teams operate in environments where threats rarely appear in isolation. A drone approaching restricted airspace, an unidentified vessel entering a security zone, or suspicious activity near critical assets may each seem routine when viewed separately. The challenge is understanding when they are connected.

Advanced Data Fusion

Security personnel cannot afford to make decisions based on fragmented information. T.react CIP correlates data from radar, AIS, ADS-B, cameras, sonar, drone detection systems, and other surveillance sources into one unified operational picture. Built on more than 20 years of multi-sensor fusion expertise, the platform presents a single validated track for each detected object, reducing uncertainty, improving situational awareness, and helping operators identify coordinated threats faster.

Enhanced Video Tracker

When an unidentified drone, vessel, or vehicle approaches a protected area, operators need visual confirmation quickly. T.react CIP automatically directs available long-range cameras to search, detect, classify, and track potential threats based on information received from radar and other sensors. By combining intelligent camera tasking with advanced video analytics, operators gain visual identification faster, providing valuable time to assess, escalate, and respond according to established security procedures.

Threat Level Engine

Security operations must adapt as the threat environment changes. T.react CIP allows organizations to define multiple threat levels, each with its own set of detection rules, alarms, and escalation procedures. When a threat level is activated, the system automatically applies the appropriate security posture, ensuring that operators work with the right level of surveillance and response without manual reconfiguration of the platform.

Features

Integrates with Your Existing Infrastructure

T.react CIP integrates seamlessly with existing radars, cameras, AIS, ADS-B, access control systems, and third-party technologies. Its open, sensor-agnostic architecture protects previous investments, minimizes deployment costs, and eliminates vendor lock-in.

One Operational Picture

T.react CIP combines data from multiple sensors into a single operational picture across air, surface, perimeter, and sub-surface domains. Operators gain a unified view of activity, enabling faster threat assessment and more informed decision-making.

Operational Continuity Through Fewer False Alarms

By combining intelligent sensor fusion, cooperative target identification, and advanced analytics, T.react CIP reduces nuisance alarms and unnecessary interventions. Security teams can focus on genuine threats while minimizing operational disruptions and maintaining continuity.

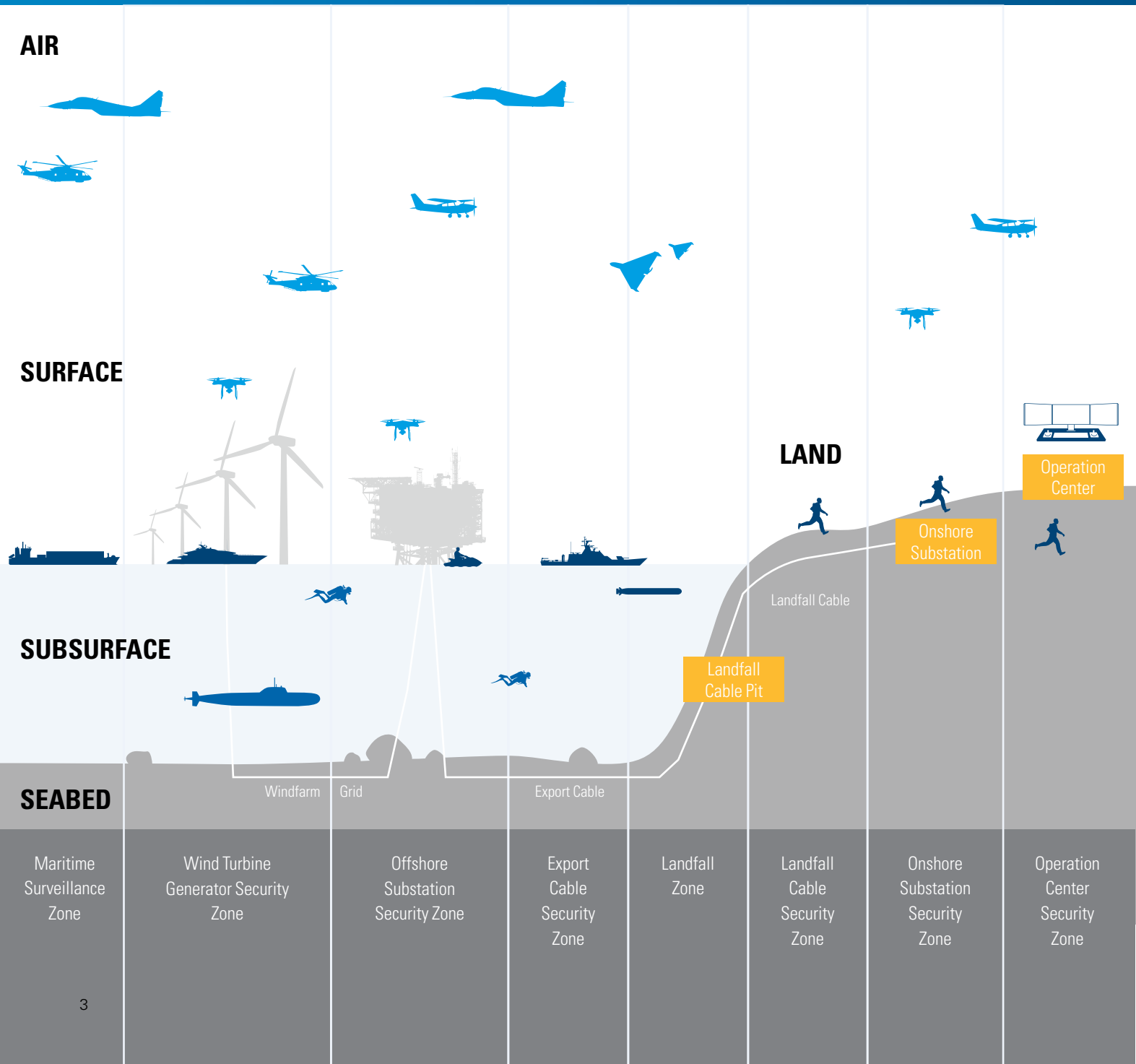
Key Benefits

- Unified surveillance across air, surface, subsea, and perimeter domains
- Sensor-agnostic, open architecture with no vendor lock-in
- Ultra-low false alarm rates via adaptive AI, intelligent sensor fusion, and an advanced rules engine
- Profile-based threat response that adapts without system reconfiguration
- Forensic-grade documentation with scenario-based recording and replay
- Cyber-hardened and IEC 62443 compliant
- Modular, scalable deployment across distributed offshore assets
- Fast installation with minimal operational disruption

Proven Terma Expertise

Terma's Command and Control solution leverages the operational experience and counter-drone expertise of both Terma and OSL, now part of the Terma Group, strengthening the combined platform's ability to detect, track, classify, and manage emerging threats also leveraging different effectors. Additionally Terma has been protecting critical infrastructure for more than 30 years. We know how a critical infrastructure protection system should be designed, integrated, and maintained, because we have already done it at scale, across continents and threat environments.

- 50+ critical infrastructure installations worldwide
- 30+ years of military-grade surveillance solutions
- 3,500+ Terma radar installations globally



Operating in the aerospace, defense, and security sector, Terma supports customers and partners all over the world. Our dedicated and talented global workforce develops and manufactures mission-critical products and solutions that meet rigorous customer requirements.

At Terma, we believe in the premise that creating customer value is not just about strong engineering and manufacturing skills. It is also about being able to apply these skills in the context of our customers' specific needs. Only through close collaboration and dialog can we deliver a level of partnership and integration unmatched in the industry.

Our business activities, products, and systems include: command and control systems; radar systems; self-protection systems for ships and aircraft; space technology; and advanced aerostructures for the aircraft industry.

Terma has decades of hands-on know-how in supporting and maintaining mission-critical systems in some of the world's most hostile areas. Terma Support & Services offers through-life support of all our products to maximize operational availability, enhance platform lifetime, and ensure the best possible cost of ownership.

Headquartered in Aarhus, Denmark, Terma has subsidiaries and operations across Europe, in the Middle East, in Asia Pacific as well as a wholly-owned U.S. subsidiary, Terma Inc., with offices in Washington D.C., Georgia, and Texas.