Radiflow
CAPULA

CASE STUDY

How a Large Offshore Wind Farm Manages its OT Assets to Avoid Cyber Attacks

Wind farms, which currently supply over 14% of Europe's electricity demand, have in recent years joined the ranks of critical national infrastructures in many countries. A debilitating cyberattack on a large wind farm can disrupt economic activity and civilian life far beyond its vicinity. It's no surprise that wind farms, as well as other renewable energy facilities, have become the target of cyber-attackers, including state-funded hacker groups.

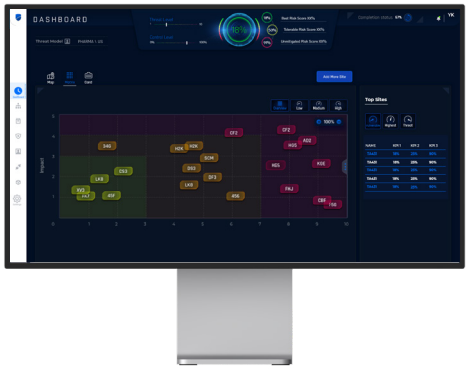
While many of the challenges involved in securing an offshore wind farm's OT network are due to its wide-area distribution, in this case - securing one of the world's largest offshore wind farms, with over 150 turbines off the coast of the United Kingdom (UK) - the customer had to content with limited OT expertise, a lack of visibility of its OT network and compliance certification.

The wind farm project was a joint operation between Radiflow and Capula, a leading OT systems integrator and managed security services provider for the Nuclear and Energy sectors in the UK.

Objectives of the project

The main objectives of the project were:

- Lack of visibility into the OT network: while the customer had a system in place for monitoring their IT network, there was a need to have visibility into their OT estate with current limited ability to detect anomalies that may indicate a breach attempt
- Ensure compliance with NIS-D, the EU-wide cyber security legislation aimed at improving system security across the critical infrastructure.



Radiflow's CIARA OT risk assessment and management solution was selected as a way of optimising IT-OT security expenditure through the assessment of the customers' overall exposure to cyber-risk (accounting for the actual impact of an attack on different business units) and prioritising threat mitigation measures by their ability to reduce risk

Reasons for selecting Capula/Radiflow

- Having worked with the customer on previous projects, Capula was seen as a trusted advisor having previously demonstrated their OT-specific knowledge and experience
- Understanding the customer requirement, Capula recommended Radiflow's managed monitoring service as it solved the availability issue of OT-security specific personnel which are in very high demand and typically expensive to secure
- With a live demonstrator of the Radiflow platform, Capula was able to present the solution more easily to the customer in particular showcasing the technical capability and overall business benefits
- Radilfow's CIARA OT risk assessment and management solution was also offered as part of the project as a tool for optimizing IT-OT security expenditure through assessing the customer's exposure to cyber-risk (accounting for the actual impact of an attack on different business units) and prioritizing threat mitigation measures by their ability to reduce risk
- Thanks to efficiencies built in to the proposed solutions, including Radiflow's iSAP smart collectors, iSID's centralized operation and the iCEN MSSP-friendly distributed systems management, Capula and Radiflow were able to design a solution that delivered the right business benefit at a cost effective (or attractive if prefer) price

Solution and process

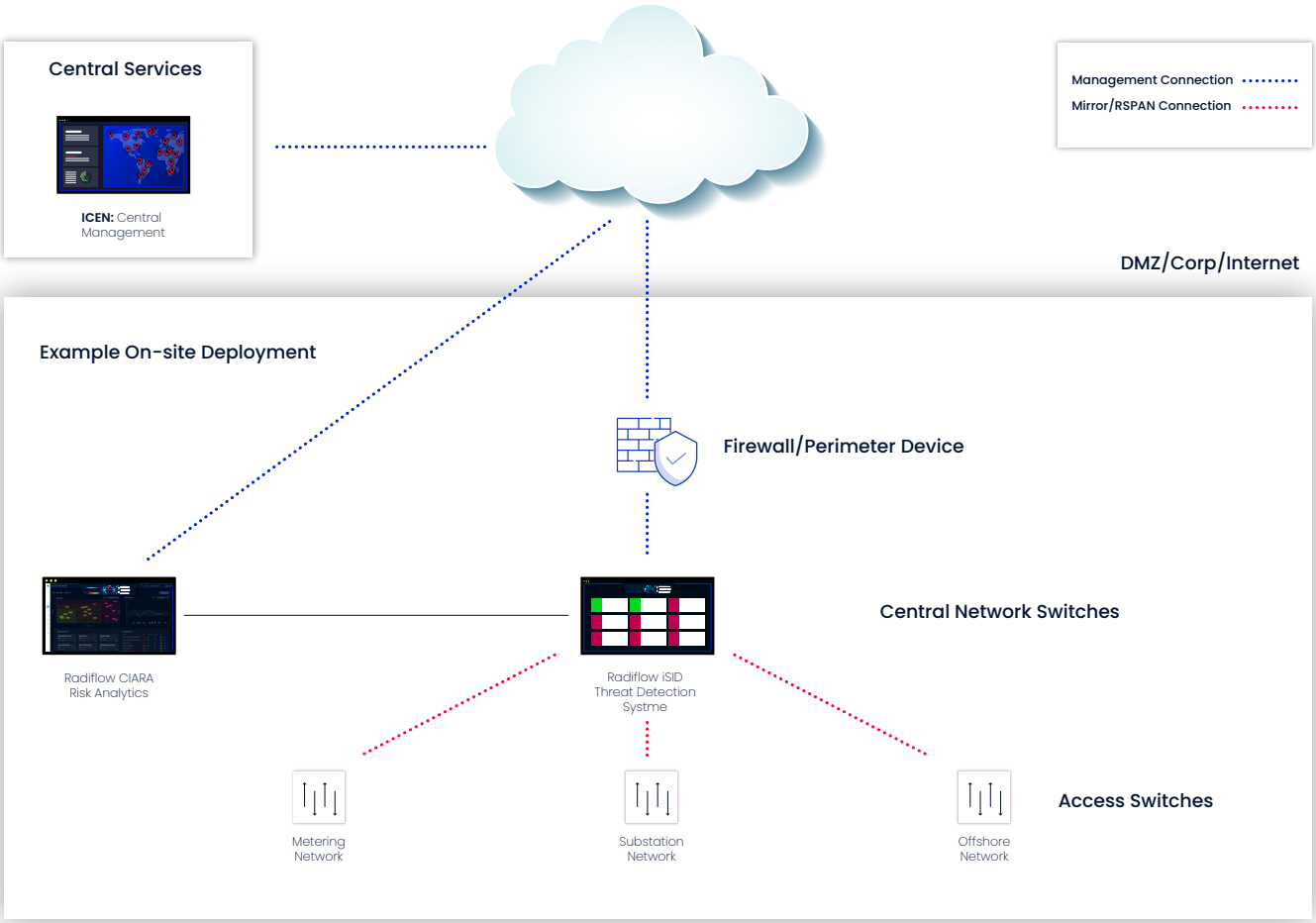
The joint Radiflow/Capula project included deploying Radiflow's iSID OT cyber security platform on the customer network within the IT-OT DMZ. From there, the iSID connected to the OT network via multiple network interfaces as the requirement was for onshore and offshore legs of the network to be monitored by a single, central instance of iSID.

Radiflow's CIARA OT risk assessment and management platform was also deployed at the site in order to provide risk assessment, management and reporting. Now a centrepiece of the project, it is planned that the monitoring system is expanded to monitor additional parts of the customer network.

The central on-site instance of iSID is monitored remotely by Capula using the iCEN central management platform. This allows for remote maintenance checks and updates, as well as real-time response to incidents while saving the needed for dedicated onsite cybersecurity engineers.

What our Partner say

Jim Allen, Capula's Strategy Manager, Future Energy Systems: As an independent OT systems integrator, we are continually building and developing strong working relationships with some of the world's leading security organisations, helping us to design the best solutions for our customers. These relationships are vital to us being able to deploy the most sophisticated and proven technologies on the market, building a comprehensive portfolio of cyber security solutions that can be delivered and supported by our team of OT industrial security experts.



(C) 2021 Radiflow LTD. All Rights Reserved. Radiflow reserves the right to change product specifications without prior notice.