Orolia Maritime, as a global leader in resilient position navigation and timing solutions, offers navigational cyber security via our platform M-SecureSync, a suite of technologies that detect and mitigate cyber-attacks on navigation systems on vessels or ashore, that can be configured as either a standalone solution or integrated with bridge systems.

As the marine sector has become more aware of the vulnerabilities to cyber threats in vessel navigation systems, which renders the vessels GNSS position data unreliable; the industry has been forced to respond. By January 2021 countering cyber risks will be a mandated requirement for ship owners under IMO resolution MSC.428(98).

As GNSS (GPS) has become the foundation block of timing and positioning technology at the heart of business-critical systems for both IT and OT, increasingly fleet administrators are gaining awareness of the operational and financial impacts of unreliable and insecure GNSS sources and the need to include navigation in their cyber security risk plans.

M-SecureSync
Navigation Cyber Security
Solution Overview
M-SecureSync is a combination of hardware; based around a 19” mounted rack; with embedded analytics software that acts as a hub for layers of navigational cyber security resilience against threats to critical GNSS signals.

Precise Location
Our solution provides an ultra-precise platform for multi-constellation GNSS sources that offers a robust time and frequency reference system that can be used for comparison with existing navigation equipment. Our hardware platform is widely deployed in a number of industries because it offers the highest standards of extreme reliability, security and redundancy.

Spoofing & Jamming Detection
By incorporating our Interference Detection and Mitigation (IDM) Suite, including a complex radio frequency analysing algorithm software, M-SecureSync can detect interference, intentional jamming and advanced spoofing signals that could weaken, block or compromise critical navigation signals.

The platform can be integrated into the existing bridge navigation system or as a stand-alone solution by attaching an Alarm Display Unit that indicates the reliability of the signal, from normal to disruption. Allowing both ashore and onboard vessel management the ability to recognise threats to navigation and take corrective action.

Signal Augmentation
Additionally, M-SecureSync can be configured for additional signal resilience. Vessel owners can mitigate threats to navigation with the augmentation of the GNSS source by including the encrypted, spoofing resistant, alternative positioning signal STL. This subscription based component can be activated if vessel owners believe GNSS signals have been compromised.

Signal Protection
Additional navigation cyber security resilience can be achieved by including a specialist antenna to work alongside the M-SecureSync. The affordable passive Anti-Jam Antenna helps to prevent signal saturation by removing on the- horizon interference, both for ashore vessel management buildings, or ships near land. By rejecting signals from a lower elevation angle allowing only signals from satellites to be received.

Resilience
As we move towards the IMO mandate for maritime cyber security, it is important that the entire vessel management ecosystem, from port navigation and infrastructure to critical bridge systems, include protection of navigation by creating a resilient position and timing source detection and mitigation plan.