OCEANSTAR™
GNSS SPOOFING DETECTION

Fugro OCEANSTAR detects when a vessel’s position is being manipulated. In the case of a cyber-attack, Oceanstar’s spoofing alarm will be triggered to alert the crew.

THE RISK
Today, man-made technology is available at moderate cost which can be used to deliberately disturb the normal operation of GNSS equipment. GNSS signals coming from satellites are weak and even a low-power transmitter can easily affect GNSS receivers within a radius of several nautical miles.

It is common to talk about two different forms of interference: spoofing and jamming.

SPOOFING
A GNSS spoofing attack attempts to deceive a GNSS receiver by broadcasting incorrect GNSS signals, or by rebroadcasting genuine signals captured elsewhere.

The effect is that the vessel appears to be in the wrong position. The attacker can further manipulate the fake signal in such a way that he in effect gains full control of the vessel.

JAMMING
Jamming is the blocking of GNSS Signals by local transmissions, which may come from own ship or from nearby vessels and installations, or ashore. GNSS frequency bands are reserved but malfunctioning or incorrectly configured equipment can produce noise in these bands. Intentional interference should also not be overlooked.

The symptoms of such interference can vary from position instability if only some satellites or frequencies are affected, to a complete positioning black-out under severe conditions.
SPOOFING DETECTION

Oceanstar™ spoofing detection consists of two methods.

- The first is the use of the most powerful anti-spoofing technique, Spatial Integrity Analysis (SIA). SIA is a multi receiver design concept.

  Oceanstar™ is constantly comparing GNSS antenna geometry with known offsets. If one or more antennas depart from the expected location the system will trigger a spoofing alert.

- The second is the unique Fugro developed technique for GNSS Navigation Message Authentication, Satguard™. This method applies the Fugro network of more than 100 reference stations world-wide.

  Satguard™ monitors the status of and data received from each individual GNSS satellite. A unique signature for each satellite is transmitted to the vessel as part of the Fugro G2/G4 correction service.

  By comparing the satellite data seen by the vessel with the Fugro data, fake satellites can be identified and discarded. Vessel crew will be alerted of an ongoing spoofing attack.

JAMMING MITIGATION

To effectively mitigate jamming and other types of interference, local transmissions need to be neutralised with specialised hardware. Oceanstar™ applies two techniques to prevent jamming.

- The Fugro G4 correction solution utilising GPS, GLONASS, Beidou and Galileo. These GNSS systems operate on different (multiple) frequencies and multi constellation receivers are therefore less prone to interference.

- A specialised high-performance antenna with optimised filters which reduce interference in the applicable frequency bands.