Innovative navigation capabilities to safeguard against GNSS positioning cyber security threats as part of the onboard cyber risk management approach

The reality of the problem
For more than a decade, attacks on satellite navigation systems have become a common occurrence. The maritime and aerial navigation sectors are constantly affected by such aggressions as they strongly rely on the GNSS signal. Many ships have already been victims of several cases of attacks. For example, between June 22 and 24, 2017 many ships operating in the Black Sea were reported to be in Russian airports following interferences identified in GPS signals. At least 20 vessels reported that their AIS systems erroneously indicated their position as being at Gelendzhik Airport in Russia. In July 2019, a British oil tanker, the Stena Impero, was seized by Iranian authorities after being diverted from its route, through manipulation of GPS signals, to end up in Iranian waters. The US House of Representatives Committee on Transportation and Infrastructure reports that the same year, an airliner nearly crashed into a mountain after a case of GPS jamming. There are many other examples of such aggressions.

These different cases of attacks characterize two types of phenomenon: radio frequency jamming and spoofing.

Jamming GNSS signals (GPS, Galileo, Beidou, Glonass ...) from satellite systems can happen accidentally by radio interference but the frequent cases that are continuously reported have been committed with malicious intent. The main consequence of this aggression is the loss of the position providing by this service.

Spoofing is more dangerous. It consists of transmitting, from various sources, fake GPS signals which replace those coming from the satellites. User receivers then pick up these fake signals which are then transmitted to onboard systems for vessel navigation. The danger of spoofing is primarily due to the fact that users are totally unaware that they are being guided by fake signals. Second, it is an effective way for the cyber pirates to take control of user systems.

All these threats on the primary source of vessel navigation information, whether accidental or deliberate, are classified as a cyber-aggression, in the sense that their targets are electronic receivers, integrated into IT/OT systems of users.

Impacts of signal interference on maritime navigation.
It is not necessary to recall that the aviation and maritime activities are among the sectors which depend the most on satellite navigation systems. Currently, most of the legacy navigation solutions such as offshore positioning and radio navigation are disappearing, thanks to SOLAS which requires all ships to be equipped with GNSS receivers.

This increased GPS dependency gives an idea of the impacts that attacks could have on the maritime activities. As cyber threats, these attacks can have the same consequences as classic cyber-attacks over Ethernet that put the whole planet on alert.

The magnitude of the problem is now such that on March 1, 2021, the US House of representatives Committee on Transportation and infrastructure drew the attention of the US federal government to the need for a back-up system in the event of GPS signal
breaches. Such an alternative would avoid catastrophic accidents and improve transport safety, at a time when new technologies in this field are rapidly evolving.

A year earlier, precisely March 10, 2020, the United States had already submitted a request to the IMO, expressing their serious concerns about the increase in attacks on GPS signals. They asked the IMO to "rule urgently on cases of jamming and spoofing which endanger the safety of ships and sailors at sea, after recalling the known intentional cases in the Black Sea and in Eastern Mediterranean from 2016 to 2018 having impacted navigation in international waters and in areas of high maritime transit".

Looking forward, we can anticipate a greater impact of these threats on future generations of ships which will have a higher level of automation or potentially even be fully autonomous. These ships will therefore entirely rely on their navigation systems, and will consequently be more vulnerable than current ships. Their effective deployment, probably within a few years, will require the rigorous consideration of multiple risk factors, including interference with satellite navigation system signals, which continue to threaten maritime safety.

**A risk to be managed in the framework of cyber security**

The inclusion of the risks of attacks on the signals emitted by GNSS among cyber risks is confirmed by the maritime community. In their "Guidelines on cyber security onboard ships" published by BIMCO and several players in the maritime community (including Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Ship owners (INTERCARGO), Inter Manager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), and the World Shipping Council (WSC)), these actors identify the various cases of interference with the GNSS signals used by ships, in particular jamming and spoofing, like cyber risks, forming part of the risk of loss or manipulation of data from external sensors essential for vessel operations. As a result, they recommend to ship owners to take them into account in the emergency plans in cyber security on board ships.

The inclusion of the risks of interference with GNSS signals implies that the fight against these types of threat is part of the general maritime cyber security framework. Thus, in accordance with IMO Resolution MSC.428 (98), adopted on 16 June 2017, considering the cyber risk management as part of safety management systems onboard ships, prescribed by the ISM Code, attacks on signals originating from GNSS are subject to the same requirement. Therefore, shipowners should not be limited to prevent conventional cyber risks.

In the process of preventing impacts linked to jamming and spoofing of GNSS signals, Thales Group has recently developed an innovative solution focused on the detection of cases of breaches, and provides a safe backup solution to pursue ship navigation.

**Innovative solution to detect and recover from cyber aggression toward GNSS signal**

IMO resolution A.915(22) adopted on 29 November 2001 - REVISED MARITIME POLICY AND REQUIREMENTS FOR A FUTURE GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS) - defined the minimum navigation performance GNSS usage for navigation.

For general navigation, the performance required is summarized below:

---

1 BIMCO, OCIMF, et al., The Guidelines on cyber security onboard ships, version 4,
### System level parameters

<table>
<thead>
<tr>
<th></th>
<th>Absolutes Accuracy</th>
<th>Integrity</th>
<th>Availability% per 30 days</th>
<th>Continuity% over 3 hours</th>
<th>Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Horizental (metres)</td>
<td>Alert limit (metres)</td>
<td>Time to alarm (seconds)</td>
<td>Integrity risk (per 3 hours)</td>
<td></td>
</tr>
<tr>
<td>Ocean</td>
<td>10</td>
<td>25</td>
<td>10</td>
<td>$10^{-5}$</td>
<td>99.8</td>
</tr>
<tr>
<td>Coastal</td>
<td>10</td>
<td>25</td>
<td>10</td>
<td>$10^{-5}$</td>
<td>99.8</td>
</tr>
<tr>
<td>Port approach and restricted waters</td>
<td>10</td>
<td>25</td>
<td>10</td>
<td>$10^{-5}$</td>
<td>99.8</td>
</tr>
<tr>
<td>Port</td>
<td>1</td>
<td>2.5</td>
<td>10</td>
<td>$10^{-5}$</td>
<td>99.8</td>
</tr>
<tr>
<td>Inland waterways</td>
<td>10</td>
<td>25</td>
<td>10</td>
<td>$10^{-5}$</td>
<td>99.8</td>
</tr>
</tbody>
</table>

A.915(22) : Appendix 2 Table of the minimum maritime user requirements for general navigation

For each type of navigation, a level of integrity is required to ensure safe maritime operations. At the time the resolution was adopted, GNSS navigation and receivers were emerging solutions restricted to a few domains of application mainly due to their price. More than 20 years have passed since this resolution and today, every mobile object on earth relies on GNSS navigation from either a single or multiple constellation. Parallel to the expansion of GNSS navigation, jammer and spoofer techniques have emerged from military uses, and today are widely used by civilians due to their simplicity and low cost regarding the benefits they can bring.

At the time the IMO resolution A.915(22) was written, GNSS aggression via radio frequency signals was an inconceivable idea, therefore none of today’s reported cyber aggression events were taken into account in the integrity and availability requirements for safe navigation.

Based on its safety culture from its civil aviation heritage, Thales has developed a new approach to naval navigation for military and maritime transport vessels providing the highest level of navigation integrity. For this, Thales has developed an innovative solution, which monitors the GNSS position provided by the receiver in order to detect any type of spoofing, even the most sophisticated. Once detected, the Thales solution is able to provide a safe recovery position and therefore ensure mission continuity without any compromise toward vessel and crew safety.

**Thales solution key characteristics**

**Guaranteed integrity within the mandatory performance**: Provide alarms when the position provided by the onboard GNSS equipment data is incoherent with the position safely and autonomously computed. This independent and safe monitoring capability will ensure the navigation required integrity (i.e. $10^{-5}$) in any condition and for any type of GNSS cyber aggression like spoofing.

**Ensure continuity during Cyber aggression**: Provide safe navigation backup solution when GNSS environment is jammed therefore contributing to cyber resilience and ensuring mission continuity.

**Immune from any cyber aggression**: Independent from any external information to check navigation integrity, the Thales solution has the highest cyber resilience level.
Cyber resilience can be reinforced by a direct physical connection to the GNSS receiver to prevent any onboard-corrupted data to be used. In addition, crew alerting can be done via a simple and independent warning system, reinforcing further the integrity resilience and awareness to any cyber aggression.

**Available worldwide:** Autonomous onboard system independent from any external infrastructure or information.

**Secure AIS position broadcasted:** With the same principal, uses the navigation AIS input data to ensure the same level of integrity for position broadcasted. The Thales system can be physically connected between the AIS and the onboard navigation to check the position integrity just before its usage by the AIS.

**Easy to install on existing and new vessels:** The Thales system can be installed anywhere in the vessel and requires limited space (8 litres) with only one cable to the GPS equipment, a second to the crew warning system, and a third cable to the AIS.

Typical onboard installation can be represented as follows:

![On board installation to alert on GNSS cyber aggression](image)

![On Board Installation to alert and provide backup solution during GNSS cyber aggression](image)

**Thales key enablers to secure navigation against GNSS cyber aggression**

Thales is applying a highly safety-critical airborne navigation approach to the naval domain to deliver trusted navigation performance for decisive moments and propose a
solution built around TopAxyz Naval Inertial Navigation System (INS) to prevent such cyber aggressions.

Inertial Navigation System are widely used across military vessels, however navigation integrity in GNSS-denied environment has never been achieved in current naval navigation systems.

TopAxyz Naval INS sensors and architecture were initially developed for critical safety airborne applications and brought them on the naval market to secure maritime vessels against GNSS cyber aggressions.

Patrice A. EDORH-KOMAHE
Chercheur
Adam Assurances
Le Lab - Recherches et innovations en assurances maritimes et transports
+33 556 007 980 | + 33 789 885 993 | ORIAS 07 002 980 | pedorh-komahe@adam-assu-mar.com
www.adam-assu-mar.com

En partenariat avec
le Centre de droit maritime et océanique, Nantes
et le Centre de recherche et de documentation européennes et internationales, Bordeaux

Emmanuel NGUYEN
Senior Navigation Expert, Flight Avionics

8 avril 2021