INTERTANKO

Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)

TWENTY 19

Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)

Contents

Introduction

A Global Navigation Satellite System (GNSS) refers to a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers. The receivers then use this data to determine location. By definition, GNSS provides global coverage.

High standards of navigation are fundamental to the safety of vessels, crews, cargoes and the protection of the environment. We are more and more reliant on types of GNSS such as Global Positioning Systems (GPS) for safe navigation. Growing threats to these systems have been identified that can affect how we use them for navigation and how we can mitigate against disruption to services provided by GNSS.

Scope

This document is aimed at owners, operators and Masters. It provides guidance on the various types of GNSS, an introduction to threats associated with these systems and guidance on how to mitigate against these threats. It is not intended to cover all of the technical aspects of these issues but it will aim to identify practical and pragmatic ways to mitigate disruptions.

Jamming and Spoofing

GNSS signals have low power, which means that a weak interference source can cause the receiver to fail or to produce hazardously misleading information. Until now, the biggest worry for GNSS has been that it can be jammed by masking the satellite signal with noise. Complete loss of GNSS is fairly easy to detect, but subtle movements due to the effect of jamming are not – and can appear similar to spoofing, which can be very hard to detect.

Spoofing is more insidious: a false signal from a ground station that simply confuses a satellite receiver.

To simplify, jamming causes the receiver to die, spoofing causes the receiver to lie. However, as explained below, this statement is not technically correct – but it does provide a broad overview of what the main difference is between jamming and spoofing.

Figure 1 Jamming

What is jamming?

Jamming is usually caused by interference to the signals at GNSS frequencies. However, jamming may also be caused by unintentional means, including space weather or faulty equipment that can radiate signals on the L1 frequency and jam GNSS signal reception.

Intentional jamming is designed to overpower the very weak GNSS signals receiver. Besides military jammers, strategies such as Personal Protection Devices (PPD) are frequently used. These are readily available and inexpensive but forbidden in the majority of countries.

Some GNSS bands are shared with certain radars, other satellite equipment as well as amateur radio. Other sources include Distance Measuring Equipment used for airplane navigation, TV harmonics, as well as malfunctioning electronic equipment. As an example, a 25W Inmarsat transmission near a poorly designed dual frequency receiver will at minimum "blank" all GNSS reception, and at worst "fry" the receiver front end.

Figure 2 Spoofing

What is spoofing?

GNSS spoofing is the provision of GNSS-like signals, transmitted locally and coded to fool the receiver to think it is somewhere it is not.

A GNSS spoofing attack attempts to deceive a GNSS receiver by broadcasting incorrect GNSS signals, structured to resemble a set of normal GNSS signals, or by rebroadcasting genuine signals captured elsewhere or at a different time. These spoofed signals may be modified in such a way as to cause the receiver to estimate its position to be somewhere other than where it actually is, or to be located where it is but at a different time, as determined by the attacker.

One common form of a GNSS spoofing attack, commonly termed a "carry-off attack", begins by broadcasting signals synchronised with the genuine signals observed by the target receiver. The power of the counterfeit signals is then gradually increased so that the vessel's GNSS receiver tracks the false signals which can then be manipulated to report a different location to the genuine signals. Spoofing GNSS signals with the aim of not being detected is a military grade technology, and currently unlikely to be seen in peacetime.

Meaconing

'Meaconing' is a type of spoofing where GNSS signals are re-transmitted. This requires simpler equipment than that required for a spoofing attack.

The source of a meaconing attack could also be a GPS/GNSS repeater such as those installed in airport hangars, allowing indoor reception of GPS signals for testing purposes. Should the power of such a repeater be increased intentionally or not, it would lead to a fake position being sent out.

Recent reports of spoofing attacks are believed by some experts to have been meaconing attacks.

Summary

A spoofing attack is considerably more complex than a jamming attack, especially if the attack is supposed to remain undetected.

Detection and mitigation against jamming and spoofing

In 2017, the IMO published MSC.1/Circ.1575, *Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing* to the Performance standards for multi-system shipborne radio navigation receivers.

The International Electrotechnical Commission (IEC) is developing test specifications for multi-system receivers, including SBAS as well as other radio-navigation systems, based on the IMO "Guidelines for shipborne PNT data processing" (MSC.1/Circ.1575).

If the equipment onboard meets the MSC.1/Circ.1575 specification and there are multiple types of GNSS as well as other inputs, the system should raise an alarm in case of a detected error to inform the navigator that the position has been lost. Modern equipment already exists that meets the MSC.1/Circ.1575 guidelines.

INTERTANKO recommends that navigation systems, equipment and software onboard are designed in line with these guidelines.

Guide for the Navigator

- Actions to detect GPS spoofing and jamming should include the use of radar and Electronic Chart Display and Information System (ECDIS) interlay (overlay or underlay), which are by far the best methods to identify jamming and spoofing when land is visible on the radar.
- Position verification at appropriate intervals as laid out in the *Guide to Safe Navigation, including ECDIS* (INTERTANKO 2017).
- Observing significant difference between DR position (position arrived with Gyro Course steered and distance by speed log) and GNSS fix.
- Observing and verifying by using an echo sounder to compare the depths when sailing in suitable depth areas.

<u>Actions if jamming and spoofing is detected</u>

Immediate actions:

- Manually select a secondary position sensor.
- Select other GNSS input if provided and use a "GNSS divergence" alarm to check any marginal difference between positioning sources.
- If a secondary sensor is unable to provide a vessel's position and no other means are available to input position fixing, the navigator should select the DR or EP mode.
- Start to manually plot ship's position if near enough to shore and seek greater sea room if possible.
- The Automatic Identification System (AIS) is likely be affected by a jamming or spoofing attack as well and should be used with extreme care (this refers to the other ships' positions that are likely to be affected by an attack, not the VHF AIS signal). Note: AIS virtual navigation aid position will be correct, since the position transmitted is a true static position and is not derived from GNSS signals.

- Use the parallel indexing method during coastal navigation to keep safe distances and determine turning waypoints.
- If unable to ascertain vessel position relative to navigational hazards then stop the vessel.

When the situation is somewhat stable:

- Check the vessel GNSS position frequently to detect when the service is available again.
- Report GNSS disruptions or anomalies to the authorities listed in 'Appendix A: Reporting of jamming and spoofing events'.
- Take note of critical information such as the actual location (latitude/longitude), date/time, and the duration of the outage or disruption.
- When possible, provide photos or screenshots of equipment failures during a disruption to assist analysts with identifying a potential cause.

For vessels using paper charts:

- Continue plotting with alternate position fixing or DR.

During normal operation:
Periodically check sensor input for position and source. The Officer should be familiar with changing the settings when operational limitations demand, see the section on Training below.

Guide for the ship owner/manager:
Your bridge navigation equipment should follow the MSC.1/Circ.1575 – Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing. A multi GNSS receiver will enhance such a system. Ensure that the ECDIS system chosen has an alarm management function commensurate with the above and that proper procedures are in place. Further protection may be gained by using GNSS open signals which have Navigation Message Authentication.

Consider using Loran/E-Loran receivers as a backup/part of the resilient system and a way to detect jamming and spoofing. (Note: these do not have worldwide coverage).

Training
It is recommended that regular GNSS failure drills are carried out to maintain the familiarity with handling jamming and spoofing events.

The drills could include situations like the GNSS sensor being lost or failed and the ECDIS needing to be operated with manually-inserted lines of positions (LOPS) (e.g. DR or EP mode or through LOP or echo reference. It is necessary for the Officer On Watch (OOW) to identify the other equipment affected by GNSS sensor failure (e.g. AIS, Digital selective calling-DSC, gyro and radar). When the GNSS signal is restored to normal, it is necessary to cross-check the position with manual fix or radar interlay when in coastal range and

it is available. On confirmation, select GNSS as the primary position sensor and closely monitor it. The aim of the drill is to develop competency in detection of GNSS jamming or spoofing and safe navigation practices that are independent of GNSS.

Countermeasures

Jamming countermeasures

Fortunately, there are multiple mitigation strategies to help overcome interference:

- Filtering in the receiver. This is especially effective for out-of-band signals, but unfortunately, if a signal falls directly in-band it may still overpower the receiver.
- Aid the receiver with an inertial measurement unit (IMU). Even a low cost IMU would be very effective for this purpose.
- Use of an adaptive antenna array. Controlled reception pattern antennas (CRPAs) are extremely effective at mitigating all types of interference, even if that interference falls within the GNSS frequency band.
- Development of advanced mitigation techniques using wideband GNSS signals like Galileo E5 or Galileo PRS could be seen in the future.
- Consider using E-Loran receivers as a backup.

With respect to jamming, various GNSS delivers different services at different frequencies. For the Open Service and for maritime receivers type-approved against IEC 61108-3, the frequencies are at E1 and E5 position. Using different frequencies will to some extent mitigate against an attack, but it does not necessarily mean the system will work through it.

Aiding the receiver/navigation equipment with an IMU and an appropriate alarm management plan would greatly improve the ability to detect an attack.

Spoofing countermeasures

Viable countermeasures against spoofing include the use of array antennas. However, against simple spoofing attacks, the monitoring of certain GNSS receiver Key Performance Indicators (KPI) can be successful, such as monitoring for clock jumps, unusual or implausible signal-to-noise density ratios, or differences between code and carrier measurements. Check with the equipment manufacturer how their equipment can solve these issues.

The use of array antennas, such as CRPA, can help mitigate the impact of jamming and spoofing incidents. However, when considering vessels with multiple GNSS antenna to support different functions, the question arises of which antennas to protect. Should all antennas be replaced with a CRPA, or is the data from one or two CRPA-protected GNSS receivers used to feed GNSS data to all ship systems? The answer is not straightforward and costs may become an issue.

Furthermore, cryptographic techniques can be effective. Some types of GNSS will soon provide Navigation Message Authentication (NMA), which involves a signal consisting of some parts that cannot be generated by a spoofer.

Other measures exist, but will require software and hardware to support them (for example, software: ECDIS systems, hardware: GNSS receiver). These measures include:

- Use of an adaptive antenna array.
- Fly wheel algorithms to prohibit the system from immediate jumps in location and time in the GNSS Receiver (ECDIS or external PNT software).
- Limit the jumps (location) – GNSS receiver.
- Aid the receiver with an IMU. Even a low cost IMU would be very effective for this purpose.
- Consider using Loran/E-Loran receivers as a backup/part of the resilient system, where available.

Meaconing countermeasures

Against meaconing, i.e. the use of repeaters, similar countermeasures apply as against spoofing. The only exception is that cryptographic techniques, i.e. encrypted navigation messages, spreading code generation by cryptographic means and NMA, do not always help against meaconing, depending on the receiver's architecture and anti-replay features. This is because unlike spoofing attacks, the repeater does not need to know the structure of the GNSS signal it re-transmits.

APPENDIX A: Reporting of jamming and spoofing events

There are several systems in place that allow ships and managers to report problems and suspected jamming and spoofing attacks. The international working group, IDM (Interference Detection and Mitigation Task Force), has been set up to coordinate international efforts in the area of detecting and reporting jamming and spoofing. It is yet to establish an international reporting mechanism, but such a system is likely to be set up in the future.

Reporting systems known to INTERTANKO at the time of print are detailed below.

GPS problem reporting

The US Coast Guard Navigation Center welcomes reports regarding service degradations, disruptions, or other incidents or anomalies. All personal data is kept private and will only be used in the event that more information is needed or if further clarification is required. It is requested that submissions are as complete as possible when reporting an incident.

NAVCEN (Navigation Center – US Coast Guard) recommends that the steps below are followed before a GPS problem is reported:

- Reset the device by cycling power to the unit.
- Confirm the settings for the GPS unit or GPS application.
- Refer to the equipment manual.
- Update the equipment software or firmware and GPS mapping software.
- Contact the equipment manufacturer for additional assistance.
- For more information, refer to the GPS Frequently Asked Questions page.

If the GPS unit is leading people to an incorrect address OR are otherwise leading people to an incorrect location, the problem is not likely a "GPS" problem, but rather, it is very likely a MAPPING problem.

To submit a report to NAVCEN, please fill in the form on the following link:

https://www.navcen.uscg.gov/?pageName=gpsUserInput

Galileo incidents report form

The European GNSS Service Centre (GSC) welcomes reports regarding Galileo SiS performance degradations, disruptions, interferences or any other incident. Inputs will be processed and the incident investigated.

Some fields are required for submission, but all personal data will be kept private and will only be used in the event that more information is needed or if further clarification is required. It is requested that submissions are as complete as possible when reporting an incident.

To submit a report to GSC, please fill in the form on the following link:
https://www.gsc-europa.eu/contact-us/galileo-incidents-report-form

Tracking of events: NATO

As peacetime GPS/GNSS disturbance must be regarded as a threat to navigation safety, the respective NAVAREA Coordinators are responsible for promulgating warnings and keeping track of incidents.

NATO is concerned about cyber security and requests assistance with reporting in order to construct a comprehensive picture of this activity and assess the impact in the maritime domain. The NATO Shipping Centre (NSC) remains the point of contact for merchant vessels and shipping companies.

Please report the following:

/1/DTG (DATA TIME GROUP)/UNIT LAT/ LONG POSITION AT REPORTING TIME//

/2/TRACK WHILE OBSERVING INTERFERENCES/FROM LAT/LONG-TO LAT/ LONG//

/3/DURATION WHILE OBSERVING INTERFERENCES – START AND END TIME//

/4/INTEFERENCE TYPE (SYSTEMS AFFECTED AND HOW)//

/5/ASSESED DIRECTION OR COVERAGE AREA OF INTERFERENCE//

/6/NAVIGATION – SECONDARY MODES OF NAVIGATION USAGE AND ACCURACY VS GPS SYSTEMS//

/7/COMMUNICATIONS SYSTEMS AFFECTED

/8/OVERALL ASSESSMENT OF OBSERVATIONS – PROVIDE FREE TEXT COMMENT ON THE EVENT AND ADDITIONAL INFORMATION THAT CAN BE CONSIDERED INTERESTING.

Please submit reports to NSC by email to: info@shipping.nato.int

or to

NATO Shipping Centre
Atlantic Building
Northwood Headquarters
UK
Telephone +44 (0) 1923-956574
Fax +44 (0) 1923-956575

APPENDIX B: Types of GNSS

A GNSS is a worldwide position, time and velocity radio determination system comprising space, ground and user segments (IMO A.915).

For maritime users, Class Societies will recognise a GNSS as a system which meets the carriage requirements for position-fixing equipment for a World Wide Radio Navigation System (WWRNS), IMO Resolution A.1046 (27) Worldwide Radio Navigation System (WWRNS).

Examples of types of GNSS include the USA's NAVSTAR Global Positioning System (GPS), Russia's Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS), Europe's Galileo, and China's BeiDou Navigation Satellite System.

The performance of GNSS is assessed using four criteria:

1. Accuracy: the difference between a receiver's measured and real position, speed or time;
2. Integrity: a system's capacity to provide a threshold of confidence and, in the event of an anomaly in the positioning data, an alarm;
3. Continuity: a system's ability to function without interruption;
4. Availability: the percentage of time a signal fulfils the above accuracy, integrity and continuity criteria.

USA's NAVSTAR Global Positioning System (GPS)
The Global Positioning System (GPS) is a US-owned utility that provides users with positioning, navigation, and timing (PNT) services and has global coverage. The US Air Force develops, maintains, and operates the space and control segments. There is an ongoing modernisation programme called IIIA with the first satellite planned to be launched and completed by 2023. This is important, because GPS III will broadcast L1C (signal in common with Galileo E1). The system is also expected to develop a Navigation Message Authentication (NMA) service (see later section on Navigation Message Authentication).

Russia's Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS)
GLONASS is a space-based satellite navigation system operating in the radionavigation-satellite service. It provides an alternative to GPS and is the second navigational system in operation with global coverage and of comparable precision.

The GLONASS satellite designs have undergone several upgrades, with the latest version, GLONASS-K2, scheduled to enter service in the near future.

GLONASS uses what is called a frequency division multiple access method (FDMA) whereas GPS and Galileo use a code division multiple access technique (CDMA). However, the modernisation plan in progress will also have CDMA included.

Galileo is the European global satellite-based navigation system
Galileo is Europe's GNSS, providing improved services relating to the use of dual frequency. Galileo has made significant progress in recent years and is in use now and will have full global coverage in 2020. The programme is designed to be compatible with all existing and planned GNSS. Further to this, Galileo will include NMA (see later section on NMA), which is expected to reach full service in 2020.

China's BeiDou Navigation Satellite System (BDS)
The second generation of the system, known as COMPASS or BeiDou-2, is in operation and has been offering services to customers in the Asia-Pacific region since December 2012.

The third generation BeiDou system (BeiDou-3) in the global coverage constellation will eventually consist of 35 satellites and is expected to provide global services with a planned completion in 2020.

The GNSS signals are based on the CDMA.

Augmentation systems
Augmentation systems use additional receivers to compare signals. These can check for consistency, offering error and failure warnings to users who require high-integrity solutions. They can also correct errors to provide improved accuracy, using the technique of differential GNSS.

GNSS performance can be improved by regional satellite-based augmentation systems (SBAS), such as the European Geostationary Navigation Overlay Service (EGNOS).

SBAS can currently only be used within an IMO RESOLUTION MSC.401 compatible multi-system receiver.

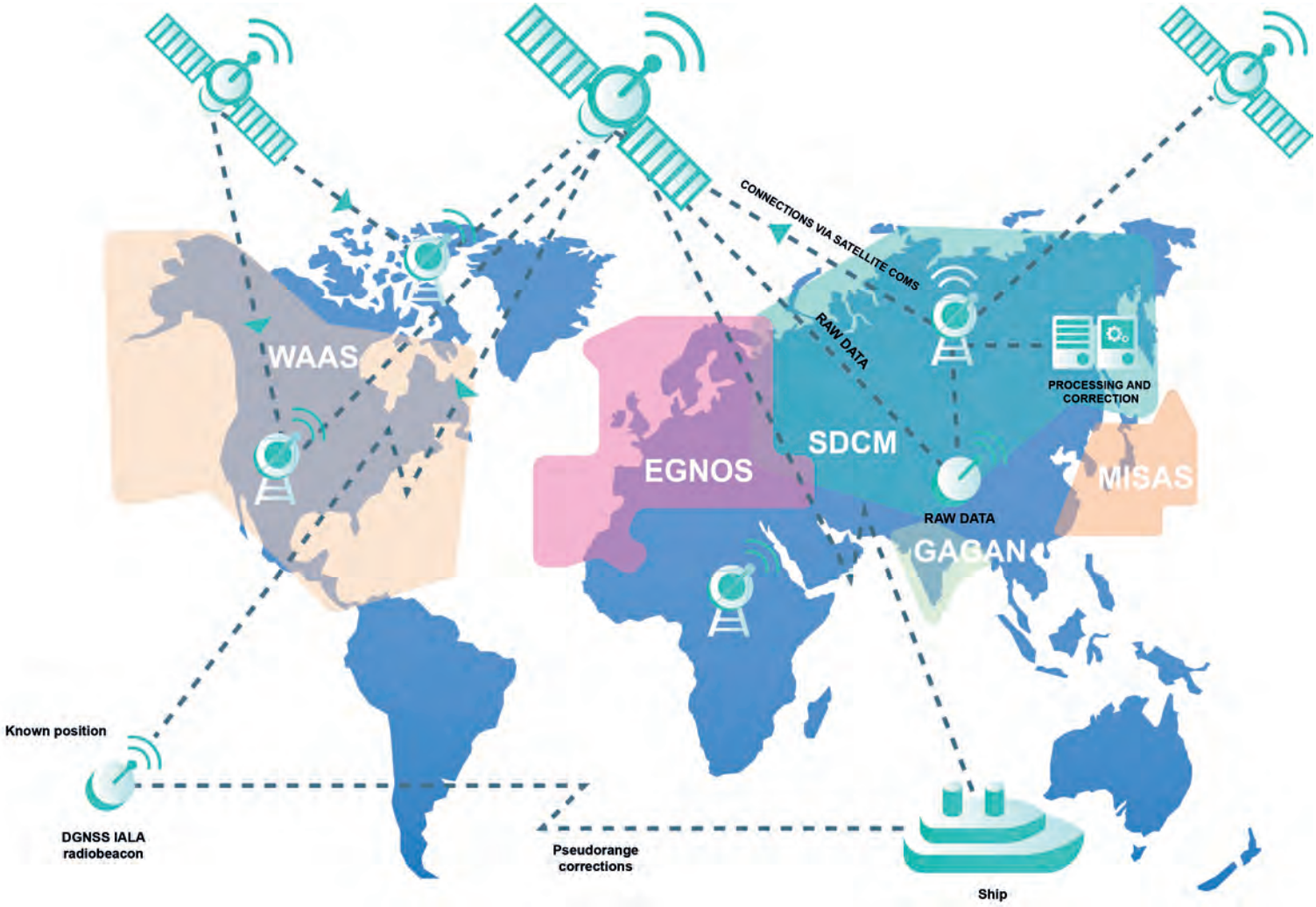

Figure 3 SBAS (Satellite Based Augmentation Systems)

Are there multi-constellation receivers capable of using GPS, Galileo, GLONASS and others?

Adding GNSS signals from more than one system to GNSS receivers will make more satellites available to them, meaning positions can be fixed more quickly and accurately, especially in built-up areas where the view to some GPS satellites is obscured. It is also more suitable for use in high latitudes (north or south). In this sense, with four global types of GNSS, receivers can now enhance the coverage currently available providing a more seamless and accurate experience for multi-constellation users around the world.

According to a recent study by the European GNSS Supervisory Authority (GSA), chipset and receiver manufacturers are already equipping their devices with multi-constellation capabilities, including Galileo, and taking advantage of the additional services that are available. In fact, more than 67% of all available receivers, chipset and modules support a minimum of two constellations and many of them offer BeiDou and Galileo functionality as well. The number of multi-constellation receivers able to receive all of the 'big four' is growing rapidly (recently reported as 30% of sold GNSS receivers).

Navigation Message Authentication (NMA)

Currently all open civil GNSS signals are transmitted in the open without any security measures, conforming to interface specifications that are fully available in the public domain. Message Authentication is based on the concept that the receiver of a message wants to ensure that the message they receive is:

- Identical to the message that was transmitted.
- By a trusted source.

NMA is one of many tools that can be used against spoofing. By itself it does not solve all of the spoofing problems, but it is certainly a step in the right direction.

Implementing NMA would in most cases require a new GNSS receiver. Several of the existing types of GNSS do now work on NMA applications. As an example, GPS is working on an Asymmetric NMA and Galileo intends to release a Hybrid Symmetric/Asymmetric NMA solution by 2020. It is up to the individual equipment manufacturers to take advantage of these services as they are made available.

References

- IMO. (2015). MSC.401(95) – *Performance Standards for Multi-System Shipborne Radionavigation Receivers.* London: IMO.
- IMO. (2017). MSC.1/Circ.1575 – *Guidelines for Shipborne Position, Navigation and Timing (PNT) Data Processing*. London: IMO.
- Lopez, M. (den 01 10 2018). GNSS Jamming and Spoofing. European Space Agency. (J. Gahnström, Interviewer)
- Sadlier, G., Flytkjær, R., Sabri, F., & Herr, D. (2017). *The economic impact on the UK of a GNSS disruption – full report.* London: London Economics.
- UK Goverment office for Science. (2018). *Satellite-derived time and position: a study of critical dependencies.* London: UK Goverment office for Science.

INTERTANKO London
St Clare House
30-33 Minories
London EC3N 1DD
United Kingdom
Tel: +44 20 7977 7010
Fax:+44 20 7977 7011
london@intertanko.com

INTERTANKO Oslo
Nedre Vollgate 4
5th floor
PO Box 761 Sentrum
N-0106 Oslo
Norway
Tel: +47 22 12 26 40
Fax:+47 22 12 26 41
oslo@intertanko.com

INTERTANKO Asia
70 Shenton Way
#20-04 Eon Shenton
079118
Singapore
Tel: +65 6333 4007
Fax: +65 6333 5004
singapore@intertanko.com

INTERTANKO North America
801 North Quincy Street – Suite 200
Arlington, VA 22203
USA
Tel: +1 703 373 2269
Fax:+1 703 841 0389
washington@intertanko.com

INTERTANKO Athens
Karagiorgi Servias 2
Syntagma
Athens 10 562
Greece
Tel: +30 210 373 1772/1775
Fax: +30 210 876 4877
athens@intertanko.com

INTERTANKO Brussels
Rue du Congrès 37-41
B-1000 Brussels
Belgium
Tel: +32 2 609 54 40
Fax: +32 2 609 54 49
brussels@intertanko.com

www.intertanko.com

INTERTANKO