CASE STUDY 1004 v1.2
Detection of Maritime AIS Denial & Deception

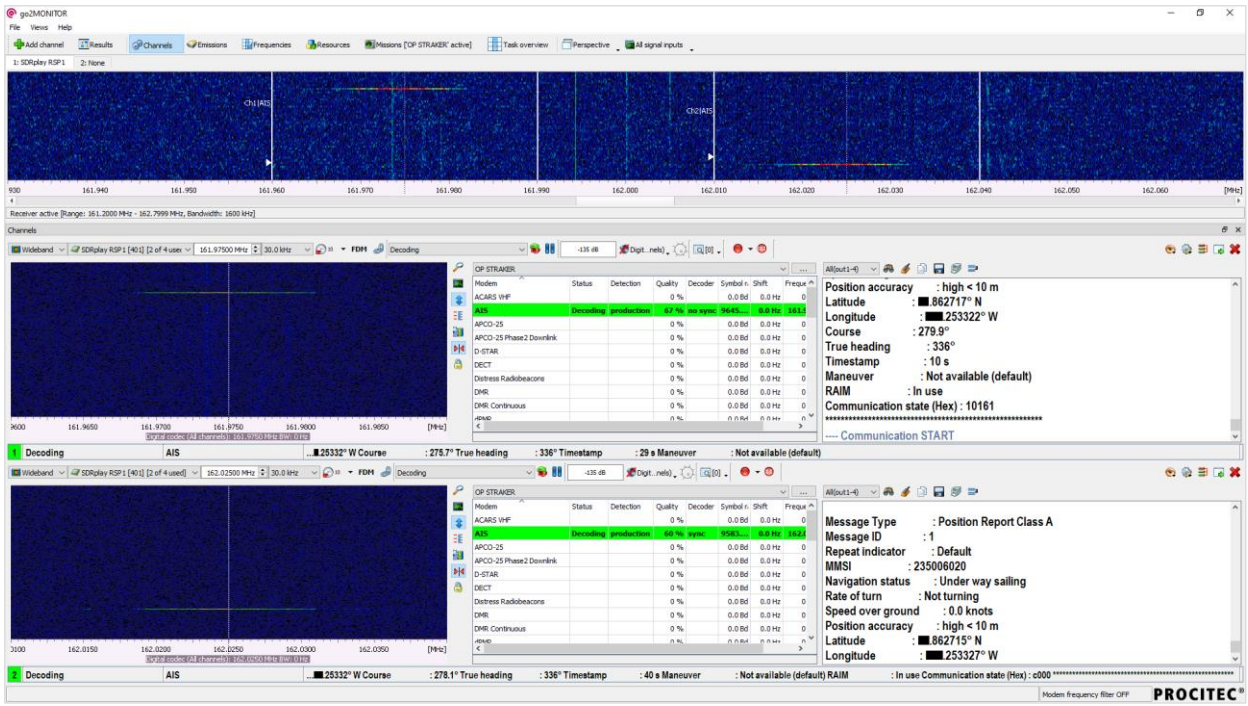
INTRODUCTION

Recent **go2signals** ops-workshops focusing upon specific theatres with our CEMA End-User units have emphasized renewed interest in the ability of **go2signals** & host Direction-Finding (DF) sensor systems to detect & report 3rd-party attempts to use Electronic Attack (Denial & Deception ['spoofing']) techniques against the VHF Automatic Identification System (AIS) used by maritime platforms whilst at sea & in harbor.

Merchant Vessels transiting toward a potentially hostile maritime choke-point (sub-tropical location) – AIS active

BACKGROUND – WHAT IS AIS..?

AIS is an automated tracking system using ship-borne (& land-based) transceivers ('transponders').The principal use of AIS is collision avoidance, but AIS is also used for fishing fleet monitoring & control, maritime security, navigational aids, search & rescue, fleet & cargo tracking, & a variety of other uses.



CEMA Team using **go2signals** at a littoral location to detect & decode vessels' in-range AIS emissions

Employing 'Self-Organized Time Division Multiple Access' (SOTDMA) techniques, AIS emissions are 'burst' signals which broadcast, in real-time, a maritime platform's unique ID, Position, Course & Speed ('PC&S'), & other data. Each maritime platform is allocated with a unique 9-digit 'Maritime Mobile Service Identity' (MMSI) which forms part of each AIS 'burst' from the vessel.

Terrestrial AIS uses VHF maritime channel 87B (161.975 MHz) & 88B (162.025 MHz). Each AIS burst employs FM/GMSK digital modulation at 9600 Bauds. The maximum nominal range for terrestrial AIS is 40 Nautical Miles, but this range can vary drastically depending upon a number of propagation factors.

AIS TRANSPONDERS

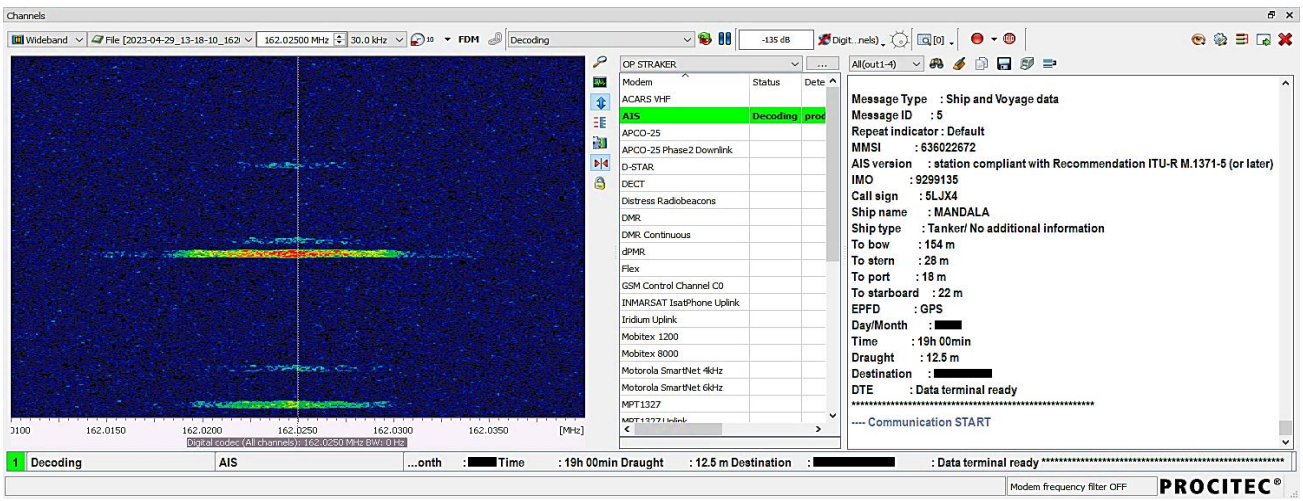
A wide variety of commercially available AIS Transponders are available on the global marketplace.

With numerous variations in shape, size & cost-versus-capability, these Transponders use Global Navigation Satellite System (GNSS) to compute & report their host vessel's PC&S, & are usually located on the vessel's bridge or control-room, whether standalone or fully integrated into the vessel's control infrastructure.

Ocean Signal ATA100 AIS Transponder
Image © courtesy of Ocean Signal [UK] Ltd

DECODING VESSELS' AIS EMISSIONS

The screenshot below shows a **go2signals** Production-Channel decoding consecutive AIS emissions on VHF Maritime Channel 88B (162.025 MHz). In this example, the emission of a vessel broadcasting the AIS message type 'Ship & Voyage data' is successfully decoded; the vessel is found to be the Merchant Vessel (MV) 'MANDALA' sending PC&S & other data including its registered MMSI of 636022672.



CEMA Team at range >20 Nautical Miles from the "Vessel Of Interest" MV MANDALA

OPERATIONAL EXAMPLE – MERCHANT VESSEL 'MANDALA'

The following vessel-specific operational example relates to the Liberian-registered 'Oil-Chemical Tanker' ('OCT') MV MANDALA, & is purely arbitrary, being used in this Study for illustrative purposes only.

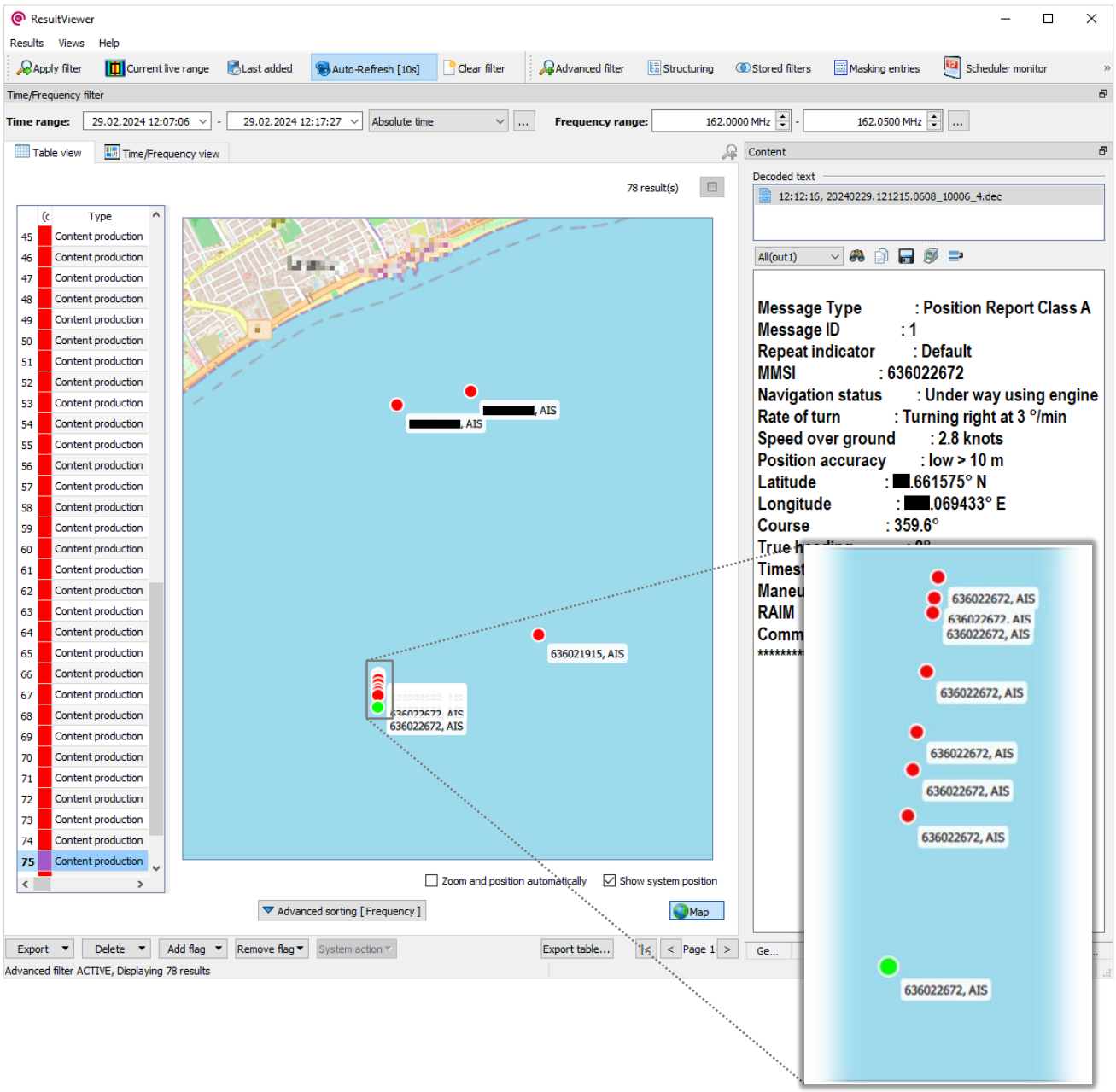
Representative OCT at-anchor

At the time of development of this Case-Study, MV MANDALA is owned by Minsheng Qihang (Tianjin) Shipping Lease Company Limited. This vessel (IMO 9299135) must not be confused with the South Korean registered OCT of the same name (IMO 9200598 / MMSI 440150000).

AIS TRACKING USING GEOSPATIAL INFORMATION SYSTEMS

Each **go2signals** Production-Channel's consecutively decoded AIS 'hits' are populated in the CEMA Team's 'ResultViewer' database & can be exported in real-time to 3rd-party Geospatial/Mission Information Systems (G/MIS) such as a host DF-Sensor's e-mapping subsystem.

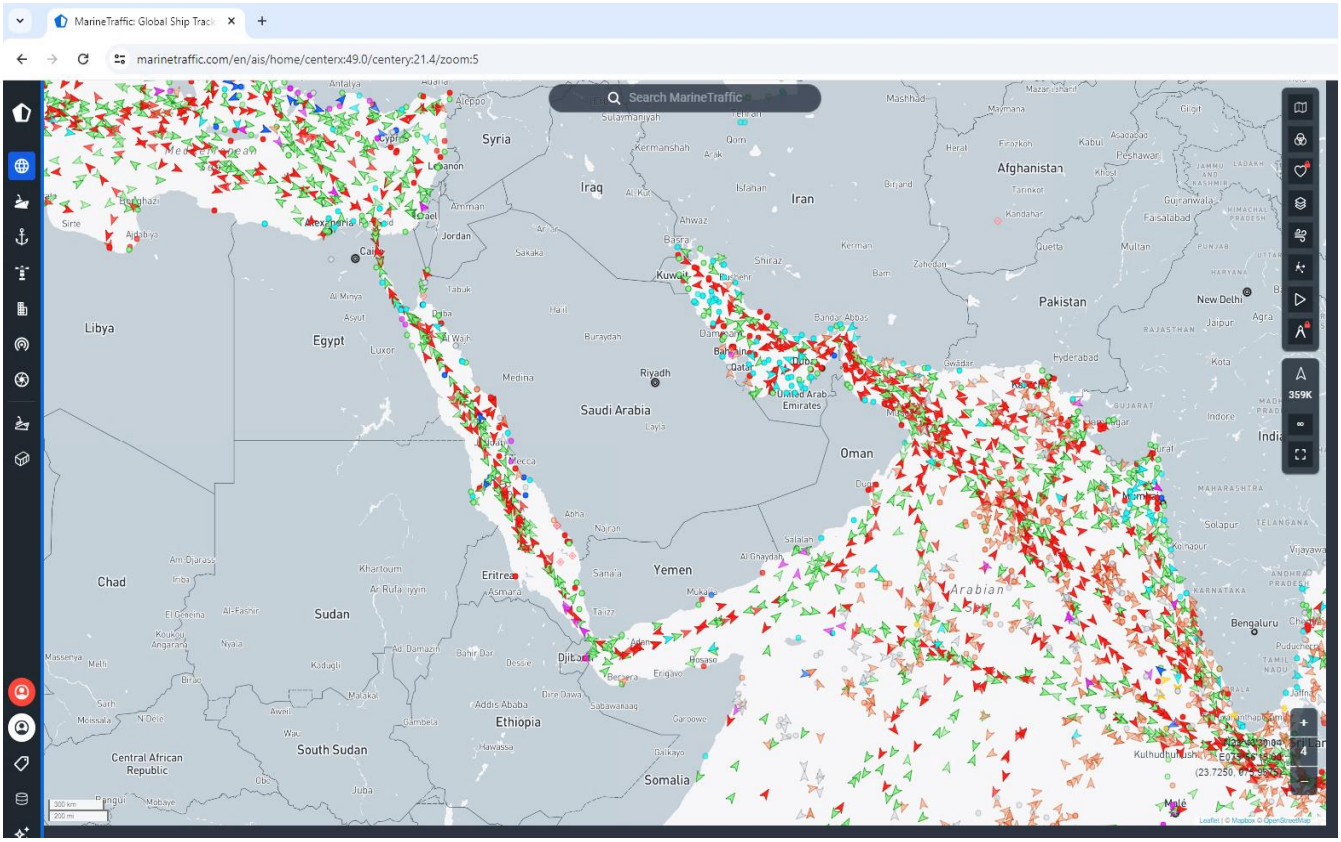
The 'real-world' **go2signals** ResultViewer screenshot below shows the AIS-derived tracking by a deployed CEMA Team of MV MANDALA on a course of 359.6 degrees (true) as the vessel slowly approaches a selected anchorage location.



Note the proximity to MV MANDALA of MV CORN (MMSI 636021915), a Liberian registered Bulk Carrier (BLK) broadcasting AIS at range 1000 Yards & bearing 065 degrees (true) from the MANDALA. The 2x vessels with obscured MMSIs in the screenshot were Minor War Vessels (MWVs) at anchor.

AIS ‘LIVE’ TRACKING ONLINE

A wide range of online portals & websites are available which track & plot global AIS emissions in real-time (the example screenshot below is courtesy of the *marinetraffic.com* website).



marinetraffic.com portal showing live AIS-derived regional shipping activity

However, there are a range of deployment configurations when, for example, CEMA Teams may not have access to these online resources, & are instead directed to detect & track in-theatre/close-proximity vessels’ AIS emissions without the benefit of internet connectivity or access to these online portals.

Additionally, there is growing speculation that the majority of recent ‘spoofing’ data is not being introduced by deceptive AIS emissions at the maritime or littoral VHF air-interface, but injected by potentially adversarial 3rd-parties into the AIS data-streams used by these AIS live-tracking websites.

…THE ‘GROUND TRUTH’

In these cases, the deployed CEMA Teams are able to prosecute the ‘ground-truth’ (i.e. the reality) rather than falling victim to these 3rd-party online spoofing attempts.

Employing techniques captured in this Study, the deployed CEMA Teams can develop & deliver confirmatory evidence to C2 entities that a Vessel-Of-Interest really is (or is not!) at the vessel’s AIS-reported & plotted location…

DETECTION & REPORTING OF AIS DECEPTION ('SPOOFING') ATTEMPTS

AIS SPOOFING – A QUICK OVERVIEW

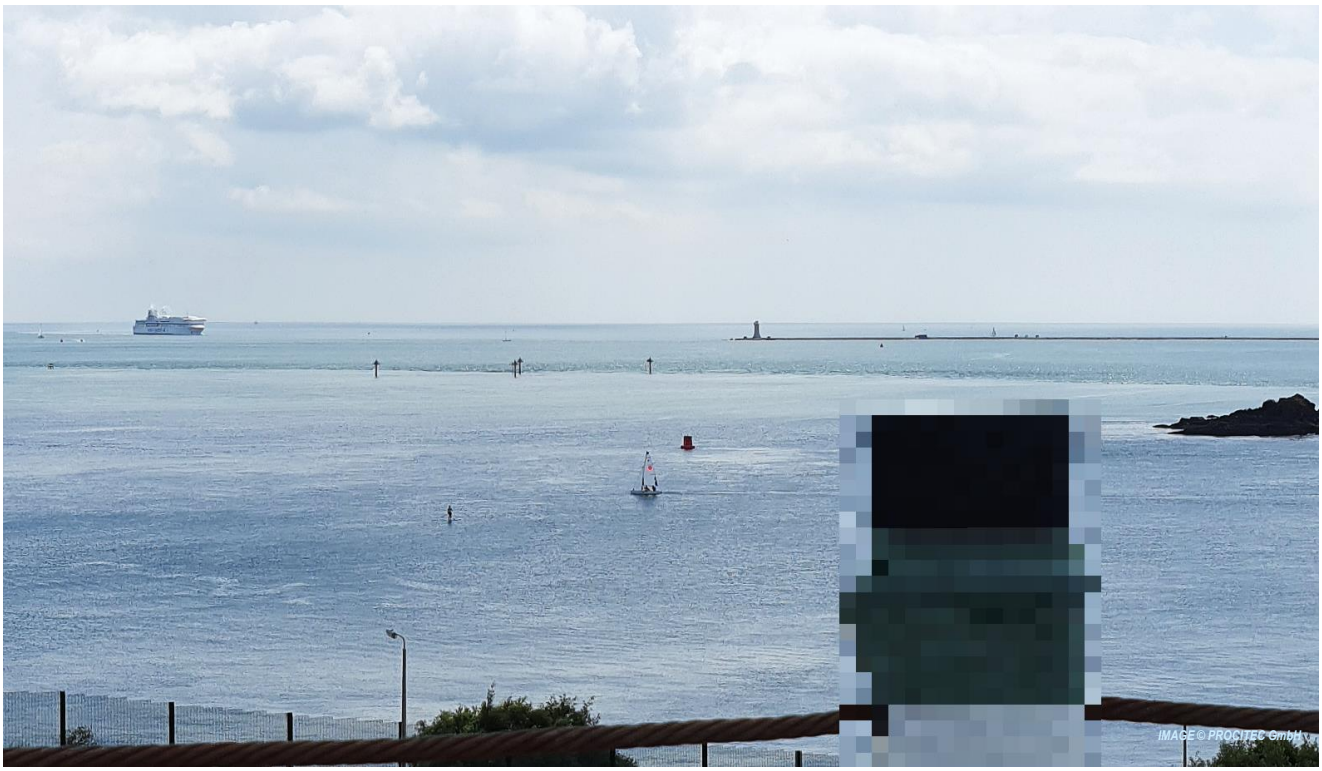
AIS deception (more commonly known as 'spoofing') is a complex & wide-ranging subject. As an introduction, the reader is encouraged to refer to the insightful publication at Principal Reference 5 (page 8) authored by Pole Star Defense of St Petersburg, Florida USA.

Additionally, an independent 3rd-party observes "the use of AIS spoofing is not limited to military purposes. Maritime data showed more than 500 cases of ships manipulating their navigation systems to hide their locations. Its use ranged from Chinese fishing fleets hiding operations in protected waters, tankers concealing stops in Iranian oil ports, container ships obfuscating journeys in the Middle East, and reportedly also weapons and drug smuggling."

To summarize, ship operators & other entities do face fines & sanctions for tampering with AIS tracking technology, but some are clearly willing to accept the risk!

CEMA TEAMS' DETECTION & REPORTING OF AIS SPOOFING

Using **go2signals** & host DF/Intercept-Sensor systems, various techniques can be employed to detect & report AIS spoofing attempts.



CEMA Team deployed at sub-tropical littoral 'overwatch' location (DF-Sensor head intentionally pixelated/obscured)

The following sub-section highlights a range of these techniques, some of which are currently being tailored & exercised by our **go2signals** End-User units in preparation for forthcoming deployed operations.

OPERATIONAL EXAMPLE – 'DF & DECODE'

In this operational example, a high-priority Vessel-Of-Interest transiting in a country's territorial waters after its embarkation of controlled military goods is reporting its *apparent* Position, Course & Speed via its AIS Transponder (**red**).

However, 2x CEMA Teams' DF-sensors (**blue**) running **go2signals** & deployed at the littoral are automatically decoding the Vessel-Of-Interest's MMSI for platform-discrimination purposes & tracking the vessel's SOTDMA AIS bursts using collaborative Position-Fixing techniques via their wireless communications bearer to derive the vessel's *real* Position, Course & Speed (**green**).

The CEMA Teams report to C2 an apparent vessel-specific AIS spoofing event for cross-cue to 3rd-parties including Visit, Board, Search & Seizure (VBSS) Teams & other agencies to action further as appropriate.

CAPABILITY DEVELOPMENT

In collaboration with our System Integrator customers & End-User groups, our R&D Team continues to explore & develop both **go2signals**-centric & collaborative techniques to detect & prosecute AIS spoofing attempts.

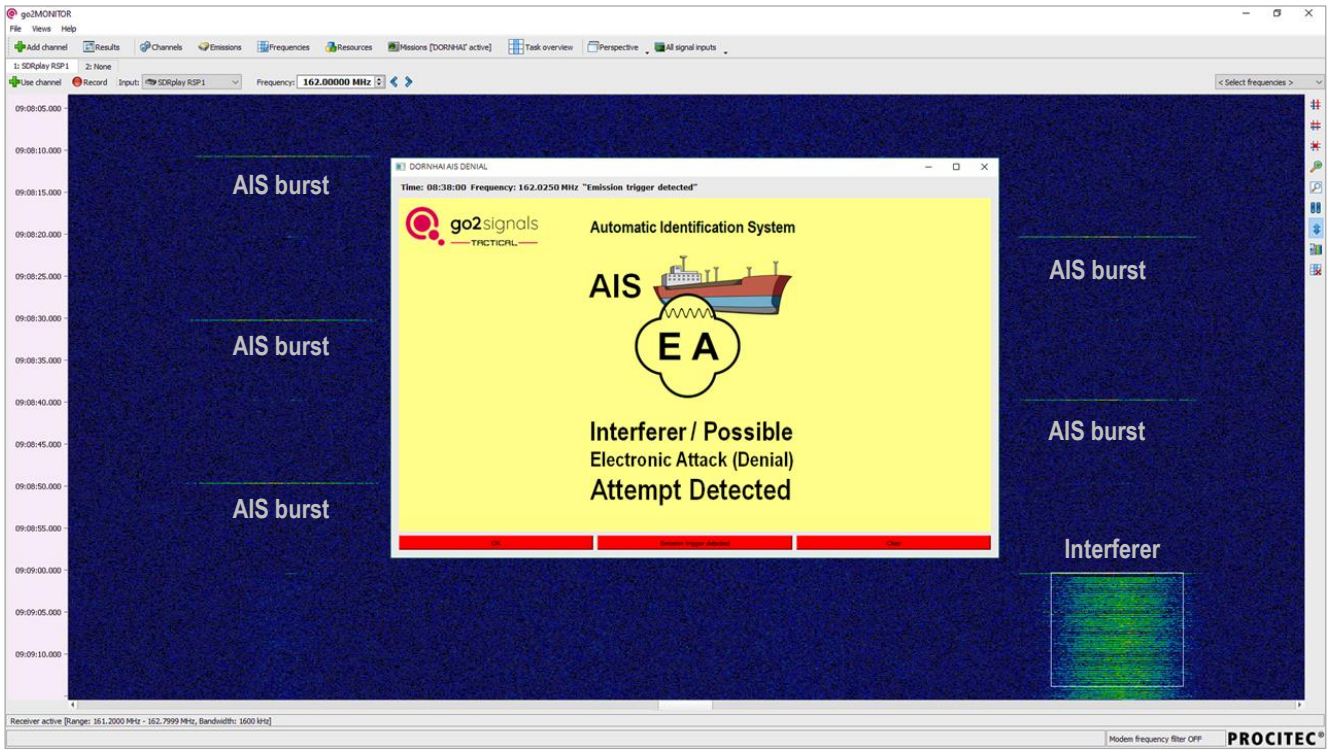
Some of these techniques require DF-sensor derived locational information for computation by **go2signals**, whilst other methods, provisionally including those using Machine Learning Algorithm techniques, can run exclusively within the **go2signals** environment then reported externally to a 3rd-party Geospatial/Mission Information System (G/MIS) in real-time or at scheduled intervals.

For example, if, according to its organic AIS report, a vessel is apparently changing position irregularly or is seemingly in-transit at a rate beyond its maximum possible speed, then user-defined filters can be created in the **go2signals** environment to identify & report these 'clues' for further analysis.

DETECTION & REPORTING OF AIS DENIAL ATTEMPTS

An 'inelegant' but effective 'Denial-Of-Service' technique employed by potentially adversarial entities is to simply transmit an intentional interferer ('jamming') waveform on the VHF AIS frequencies in an attempt to deny & confuse local shipping & agencies, or to prevent neutral 3rd-party authorities from tracking the potential adversary's own or protected vessels without the knowledge of the vessels themselves.

Employing legacy 'spot jamming' (rather than even less elegant 'barrage jamming' techniques!), activation of these 'interferers' can be detected & reported in real-time using specific **go2signals** mission-planning techniques.



go2signals WB spectrogram display - User-defined Mission Task activates alert/trigger upon detection of interferer

In the above example, a specific **go2signals** user-defined Task within a 'parent' Mission Plan has triggered a factory-example/user-modified python-script to generate an audio-visual 'splash' alert upon the detection of an 'interferer' on either (or both) of the 2x VHF AIS frequencies.

In this example, an attempted 'spot-jam' Denial-Of-Service using a Narrowband digital waveform has been detected on 162.025 MHz & a user-created audio-visual alert automatically triggered.

This automatic **go2signals**-derived alert/trigger can also be used to cross-cue other collocated or deployed assets, such as DF-Sensors to compute the source of this inelegant but effective Denial-Of-Service attempt by potential adversaries.

PRINCIPAL REFERENCES

1. International Telecommunications Union Recommendation ITU-R M.1371-5
Technical characteristics for an automatic identification system…

2. NATO Shipping Centre, Northwood HQ, UK
AIS Overview

3. US Department of Transportation - Maritime Administration
Various GPS Interference & AIS Spoofing

4. French General Directorate for Armament (DGA) (.pdf document)
Multi-Domain Assessments in AIS Falsification Cases

5. Pole Star Defense
What Is Spoofing? Your Complete Guide (+4 Key AIS Spoofing Typologies)

6. Riviera News Content Hub
Ship operators face sanctions for tampering with tracking technology

MMSI LOOKUPS

All MMSI lookups used in this Study are sourced from the ITU MMSI search-engine at:
https://www.itu.int/mmsapp/ShipStation/list

ONLINE OPERATIONS WORKSHOPS

Ops Workshops & Training Modules are available for those **go2signals** user-groups who may wish to further explore the detection & reporting of AIS denial & deception attempts. Please contact us for further information & scheduling.

FURTHER INFORMATION

For further information relating to the Detection of AIS denial & deception attempts, please contact *sales@procitec.com*

PROCITEC®
HOUSE OF SIGNALS

PROCITEC GmbH
Rastatter Straße 41
75179 Pforzheim
Phone +49 7231 155 61 0
Fax +49 7231 155 61 11

go2signals