

From: e-NAV Committee
To: Legal Advisory Panel

e-NAV13/output/17
22 March 2013

LIAISON NOTE

RELIABILITY OF AIS DATA

1 SUMMARY

This paper contains a preliminary technical analysis of the reliability of AIS data, drawing on work already carried out on failure modes of AIS aids to navigation. It is provided in response to a question posed by the IALA Legal Advisory Panel (LAP).

It was recognized that juridical organization and systems for the acceptance of specific data or information as evidence or subsidiary evidence will differ in each individual country and/or region.

However, it was also concluded that other causes could constrain the use of AIS data and information for the mentioned juridical purposes. On the other hand a variety of measures were identified that could be put in place by competent administrations or organizations to assure that AIS properly operates in a technical and functional sense and therefore potential risks for the use of AIS data or information can be limited or could be avoided.

1.1 Purpose of the document

The Committee is invited to consider the contents of this paper when preparing an answer to the question from the LAP on the reliability of AIS data.

1.2 Related documents

References given in this paper.

2 BACKGROUND

This technical analysis on the reliability of AIS data arises from a request by the IALA Legal Advisory Panel to the e-Navigation Committee. This in turn arose from the increasing use of AIS data in court cases. The analysis draws on work already carried out on failure modes of AIS aids to navigation by the GLA in the UK.

It should be noted that AIS was originally provided for safety reasons, not for security purposes, so it was never designed to be resistant to malicious interference. However it can be stated that the AIS modulation scheme is a robust and proven method of communication.

3 DISCUSSION

It should be noted that there is certified and non-certified equipment. There is no way of determining from the AIS data whether equipment is certified or not. Statistics show that there are more problems with non-certified equipment.

3.1 Causes of failure

A Failure Mode and Effect Analysis was carried out by the GLA on certified AIS AtoN in 2011 (1) and this identified the following potential causes of failure:

- incorrect data input to AIS unit;
- failure of AIS unit;
- disruption to GNSS (GPS);
- degradation of VHF propagation;
- loss of VHF reception;

- control system malfunction.

These overall headings can be used in a general way to analyse causes of AIS data loss or corruption and thereby to assess the reliability of AIS data.

When talking about AIS data the scope of data and the perception of causes of failure need to be clearly defined. Future analysis should include potential areas of failure, such as:

- physical installation:
 - placement and performance of the antennae;
 - co-site interference;
 - preventative maintenance.
- configuration:
 - not compliant with standards.
- environmental:
 - loading of the VHF Data Link;
 - sensor failure (including GNSS);
 - data transport (including VHF and network failures);
 - behaviour on the VDL.
- data input (during operation);
- equipment failure (AIS unit);
- causes affecting interpretation of data:
 - presentation configuration;
 - data portrayal;
 - data interpretation.
- method and location of data capture.

These general areas of failure should be further analysed and specific failures identified. The categories can be broken down further into sub-systems, as follows, with comments on the probabilities of each cause, where data is available.

3.2 Data Input

Data input to an AIS device is either manually configured or autonomously acquired. This data is usually categorized into Static, Dynamic and Voyage related.

Static information is input at installation, and should be updated when any change is made, such as during a refit. This information would generally be correct, subject to (deliberate/unintentional) user input error, or lack of updates due to inability to make those changes or neglect. Static data in the case of a ship will include MMSI, name and type (e.g. cargo, tanker, fishing, sailing vessel, other).

Dynamic information is derived from onboard sensors, such as a GNSS receiver or EPFS, compass or log. Dynamic data will include position, heading, COG, SOG. There are several ways in which this information can become erroneous, including sensor failure, deliberate manipulation (e.g. jamming), calibration errors, environmental effects and incorrect interfacing.

Voyage related information may be the commonest source of error, since the task of changing the information for each leg of a voyage can be overlooked. Destination information from ferries, for example, is often not changed for the return leg after completing the outward leg.

Most voyage related information is input at the masters discretion. Therefore, not all voyage related information may be available or updated. Voyage related information includes draft, destination and ETA.

3.3 Failure of AIS unit

Failure of the AIS unit, such that it is no longer transmitting, was calculated to be the most likely cause, at least in the case of an AIS AtoN – contributing roughly three-quarters of the overall probability of failure, based on manufacturer's MTBF figures. Reliability figures may have improved for newer units, with better design and components, but the original AtoN equipment is still installed so this figure is still appropriate. It should be noted that studies analysing this failure mode in other types of AIS stations have not been conducted and these figures may not accurately reflect the overall likelihood of failure.

3.4 Disruption to GNSS (GPS)

There are at least two components to this source of failure: the GPS receiver and the system itself. GPS receiver failure, again based on AtoN manufacturer's data, contributes about a quarter of the total, whereas the probability of an *undetected* satellite or ground station fault is relatively small. However, this assumes that Receiver Autonomous Integrity Monitoring or differential corrections are available, if not this becomes a much more significant contributor. It should be noted that studies analysing this failure mode in other types of AIS stations have not been conducted and these figures may not accurately reflect the overall likelihood of failure and further that there are many influencing factors for this failure mode.

3.5 Platform and Power Supply failure

This might be expected to be much more significant for an unattended floating platform such as a buoy than for a vessel, but the contribution is very small, even for a buoy and the causes (mooring breakage or dragging) would not apply to a vessel.

Power supplies on a buoy might be expected to be less reliable than on a ship, but the overall contribution is again quite small.

3.6 Effects of VHF propagation

Atmospheric noise is not a significant problem at VHF. Stratification causing anomalous propagation can extend ranges to as much as five times the normal 20-40 M. However, this phenomenon is related to particular weather conditions, mainly dependent on season and location, therefore it is difficult to apply a realistic probability to it. The VHF propagation may cause interference, which results in a partial loss of data, more studies in this area are needed.

3.7 Loss of VHF reception

The AIS system is designed to shrink cell size in high VDL loading conditions and therefore loss of reception of distant stations is likely but not problematic to the vessel. Further, the different power levels of the different types of AIS stations ensure a prioritization of Class A over other stations. The likelihood of interference to VHF is significant, either from other authorised stations, or from faulty equipment. However, it is again dependent on location, seasonal and diurnal factors, so that the confidence of any prediction of probability would be very low.

3.8 Control and Monitoring system malfunction

National AIS networks may have redundant systems. Communication links in remote areas could be a single point of failure, but would only affect very limited areas.

3.9 Malicious interference

In general it is recognized that manipulation of data in AIS messages (e.g. overwriting of the substance) is difficult to realize. Adding false data to AIS data (e.g. spoofing) is possible, the deliberate interference of AIS data with the objective to incompleteness is also possible (jamming).

AIS was introduced as a safety system and has no inherent protection against malicious interference. False transmissions or transmission containing false information can often be detected by suitably aware and trained operations personnel. However, procedures for this purpose are not generally publicised or standardised, partly because that would alert the perpetrators and make it easier for them to circumvent these measures.

Jamming and spoofing of GPS have been demonstrated on many occasions (3) and false AIS data can certainly result. It would be technically possible to create false AIS transmissions by setting up

a base station and programming it appropriately. Corroboration of AIS information, by radar for example, would be needed to ensure that it is correct. It is recommended that measures have to be further identified in order to facilitate future corroboration of AIS information to avoid manipulation of data, spoofing and jamming.

3.10 Substantial comments

- 1 In general the conclusions in this document may be true for AIS AtoN but may not reflect the overall reliability of AIS data in its full scope
- 2 Other causes, as reflected in the comments provided on paragraph 3.1 however may be significant for other types of AIS data.
- 3 Further work would be required to establish an overall probability of erroneous data, probably drawing on records collected over long periods.
- 4 Further measures and the development of the proper tools may detect and mitigate this disruption to some extent, but cannot eliminate it.
- 5 The correctness of AIS data in its own right could be relied upon in conjunction with competent monitoring, corroborative information and proper interpretation of the data. The reliability of the AIS data is high, but the accuracy of data is not guaranteed.

3.11 Checklist of measures providing guidance to competent administrations and organizations

In general competent authorities and administrations already put various necessary measures in place in order to secure the proper technical and functional operation of AIS both aboard and ashore. These measures, eventually complemented with other measures or issues to be considered, may be reflected in a list that could be used as guidance for juridical parties involved in court cases in order to identify the juridical acceptance of AIS data and information as (subsidiary) evidence.

It is recommended that a survey will be done with the aim to categorize measures to secure the proper technical and functional operation of AIS both aboard and ashore, resulting in a Guideline for competent authorities and administrations. This survey and the development of the Guideline can be done by the e-NAV Committee in conjunction with the Legal Advisory Panel where appropriate.

4 CONCLUSIONS

It was recognized that:

- legal organization and systems for the acceptance of specific data or information as evidence or subsidiary evidence will differ in each individual country and/or region;
- there is a difference between operational/technical processes and the proper interpretation of data afterwards (e.g. in court).

It was concluded that:

- the correctness of AIS data in its own right could be relied upon in conjunction with competent monitoring, corroborative information and proper interpretation of the data.
The probability of reception of the AIS data is high, but the validity of data is not guaranteed.
- the used methodology (Failure Mode and Effect Analysis carried out on AIS AtoN in 2011) may not fully cover all issues for identification of potential causes of failure.
The term “Causes of Failure” does not properly reflect the scope of the problem, which includes many aspects;
- the perspective of the conclusions as reflected in this document, being a technical analysis, in general focuses on the technical vulnerabilities of GNSS and communication networks; also

- other causes, as reflected in paragraph 3 (comments on paragraph 3.1 of this document) could constrain the use of AIS data and information for the mentioned legal purposes.

It is recommended that:

- general areas of failure (see comments on paragraph 3.1 of this document) should be further analysed and specific failures identified;
- measures have to be further identified in order to facilitate future corroboration of AIS information to avoid manipulation of data, spoofing and jamming;
- a survey be done with the aim to categorize measures to secure the proper technical and functional operation of AIS both aboard and ashore, resulting in a Guideline for competent authorities and administrations.

This survey and the development of the Guideline can be done by e-NAV Committee in conjunction with the Legal Advisory Panel where appropriate.

5 REFERENCES

- [1] GLA 2011. AIS AtoN FMEA, Report No: RPT-49-NW-11.
- [2] Reuters 2012. www.reuters.com/article/2012.
- [3] GLA 2010. GPS Jamming Demonstrations, Report No: RPT-AJG-10.

6 ACTION REQUESTED

The LAP is requested to consider the information provided and decide accordingly.