Input paper: [[1]](#footnote-1) ENAV29-5.1.3.2

Input paper for the following Committee(s): check as appropriate Purpose of paper:

**□** ARM **□** ENG **□** PAP X Input

X ENAV **□** VTS **□** Information

Agenda item [[2]](#footnote-2) n.n

Technical Domain / Task Number 2 …………………………………

Author(s) / Submitter(s) …………………………………

Working Draft of Guideline on AIS/VDES VDL integrity monitoring

# Summary

As AIS/VDES VHF Data link (VDL) is very complex, AIS/VDES VDL integrity is crucial to use AIS/VDES properly. At ENAV28, China MSA proposed a new work item of development of guideline on AIS/VDES VDL integrity monitoring by document ENAV28-5.1.3.4, and the IALA Council in mid-December 2021 approved to add this new work item for work programme 2018-2023.

# Purpose of the document

The purpose of this document is to propose a working draft of guideline on AIS/VDES VDL integrity monitoring. It provides an overview of the source of AIS/VDES VDL vulnerability, and proposes methods for IALA members to detect and mitigate the effects of invalid VDL transmissions.

1. **Action requested of the Committee**

The Committee is requested to consider the draft guideline in the annex ENAV29-5.1.3.2.1, and jointly supplement the contents of the guideline.

Gxxxx

AIS/VDes vdl integrity monitoring

Edition x.x

Date (of approval by Council)

**urn:mrn:iala:pub:gnnnn**

Revisions to this document are to be noted in the table prior to the issue of a revised document.

|  |  |  |
| --- | --- | --- |
| Date | Details | Approval |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**1 Introduction 4**

1.1 Purpose 4

1.2 Scope 4

1.3 Text structure 4

**2 Background 4**

**3 Sources of AIS/VDES VDL vulnerability 4**

3.1 Unauthorized VDL signalling 4

3.2 Sub-standard devices 5

3.3 Incorrect device configuration and installation 5

3.4 Unauthorized AIS/VDES messages 5

3.5 Spoofing message 5

3.6 DOS attack 5

3.7 Protocol Attack 5

**4 Detection 6**

4.1 Air interface status detection 6

4.2 VDL signalling detection 6

4.3 Standard compliance detection 6

4.4 Dynamic/static/voyage related AIS information detection. 6

4.4.1 Dynamic data 7

4.4.2 Static data 7

4.4.3 Voyage related data 7

4.5 AIS/VDES messages authorization status detection. 7

4.6 Protocol vulnerability detection 7

**5 Mitigation 7**

5.1 Identifying abnormal node 7

5.2 Easing unauthorized VDL signalling influence 7

5.3 Data modification function 7

5.4 Protocol revision 8

5.5 Ship terminal 8

**6 Implementation 8**

6.1 Risk analysis 8

6.2 Service architecture 8

6.3 Implementation process 8

**7 Terms and abbreviations 8**

**8 References 8**

1. **Introduction**
   1. **Purpose**

As AIS/VDES VHF Data link (VDL) is very complex, AIS/VDES VDL Integrity is crucial to use AIS/VDES properly. AIS/VDES VDL integrity monitoring is the process of determining whether the AIS/VDES VDL is abused for other purposes or due to faults. The purpose of this document is to provide an overview of the source of AIS/VDES VDL vulnerability, and propose methods for IALA members to detect and mitigate the effects of invalid VDL transmissions.

* 1. **Scope**

This document provides guidance for stakeholders, ship and shore, and authorities in deploying and running AIS/VDES properly.

* 1. **Text structure**

Chapter 2 provides background on the AIS/VDES VDL integrity monitoring.

Chapter 3 lists the sources of AIS/VDES VDL vulnerability.

Chapter 4 describes AIS/VDES VDL integrity detection and proposes corresponding methods.

Chapter 5 gives potential solutions to mitigate the effects on shore and ships.

Chapter 6 outlines the implementation of AIS/VDES VDL integrity monitoring.

1. **Background**

AIS/VDES services are based on AIS/VDES VDL, which involves 2 AIS channels (AIS 1 and AIS 2), 2 ASM channels (ASM 1 and ASM 2), 2 Long range AIS channels (75 and 76), and 12 VDE channels (1024, 1084, 1025, 1085, 1026, 1086, 2024, 2084, 2025, 2085, 2026 and 2086).

In resolution MSC.140 (76) the IMO recognizes a compelling need to ensure the integrity of the AIS VDL and recommends that authorities take the necessary steps to do so. IALA also strongly recommends a national competent authority is appointed with the responsibility of managing the AIS VDL in R0124. The users and the types of AIS message, service, and equipment are increasing with the development of AIS. The risk of AIS VDL overloading has emerged and shown the vulnerability of AIS. It led to the development of VDES. According to ITU standards, VDES has a larger data transfer rate and more complex protocols. Its VDL is more vulnerable. Therefore, it is necessary to detect the VDL integrity and mitigate the effects to ensure the validity of the AIS/VDES services.

1. **Sources of AIS/VDES VDL vulnerability**

Since AIS/VDES is a wireless communication system with transparent air interface, the VDL has inherent vulnerability that comes from the following aspects:

* 1. **Unauthorized VDL signalling**

AIS base stations manage the VDL using AIS messages 16, 20, 22 and 23. The VDES base stations and satellites control the terminals transmitting by bulletin boards and other signallings. The bulletin board should use PKI for signature authentication, but the terminals also accept the ones of authentication failure. VDL signalling should be broadcast under the authorization of the competent authorities. Unauthorized VDL signalling can cause chaos in AIS/VDES resource allocation and slot access.

* 1. **Sub-standard devices**

If the device is not designed in strict accordance with standards, or the device itself is defective, it will lead to abnormal slot access, channel selection, transmission interval, etc. It may cause slot conflicts, message errors, or congestion in VDL. Compared with AIS, VDE VDL is more susceptible to the influence of substandard devices due to the requirement of reliable data transmission.

* 1. **Incorrect device configuration and installation**

Incorrectly configured and installed devices may send messages with incorrect or incomplete information. For example, incorrect static and voyage related information is transmitted due to incorrect configuration of a mobile station, or the dynamic information is partly filled with default if GNSS antenna of the mobile station is installed incorrectly. These errors and invalid information will reduce the efficiency of data exchange.

* 1. **Unauthorized AIS/VDES messages**

AIS/VDES can send some specific information, such as safety related messages, hydro meteorological messages, DGNSS broadcast binary messages, etc. The transmission of these messages must be authorized to ensure that reliable information is provided to seafarers. However, AIS/VDES lacks verification mechanism for these messages, and unauthorized AIS/VDES messages will lead to confusion or even misleading.

* 1. **Spoofing message**

AIS/VDES messages should carry valid information. For instance, AIS dynamic and static spoofing messages carrying fake information may significantly reduce the VDL reliability to mislead the crew in making decisions and affect the authorities in tracking targets.

* 1. **DOS attack**

Some altered AIS/VDES devices can broadcast a large number of messages over the VDL as malicious. The messages occupy or reserve a large number of time slots, causing other devices to fail to work. Such an attack may cause overloading of the VDL.

* 1. **Protocol Attack**

VDES has complex protocols, transparent air interface, and diversified applications. This also means that its protocol is more vulnerable. Attacks against the vulnerabilities of VDES protocol may cause system overload, message errors, and information leakage.

1. **Detection**

AIS/VDES VDL integrity monitoring is to assure proper usage of the VDL. Detection is the essential function of AIS/VDES VDL integrity monitoring and the prerequisite for mitigation effects. The following aspects should be detected:

* 1. **Air interface status detection**

AIS/VDES air interface status detection ensures the availability of the VDL and normal function of the AIS/VDES. The following items are recommended to detect:

* Number of AIS/VDES units received by each station;
* VDL load;
* Channel loading balance;
* PSS transmissions and coverage;
* CRC error.
  1. **VDL signalling detection**

VDL signalling should be transmitted under the authorization of the competent authorities. AIS/VDES VDL signalling detection mainly identifies whether the AIS VDL management messages, such as 16,20, 22 and 23, and the VDE bulletin boards and other signallings are authorized.

AIS/VDES VDL signalling detection analyzes the received VDL signallings to determine:

* Whether the signalling is issued by authorized stations;
* Whether the signalling contents and validity duration are authorized;
* Whether there are conflicts between signallings in the same area.
  1. **Standard compliance detection**

AIS/VDES standard compliance is the key factor in ensuring VDL integrity. The judgment of AIS/VDES standard compliance is based on the detection of message information and signal characteristics (signal strength, transmission time slot, etc.) of the AIS/VDES unit. The contents of detection include:

* Slot access compliance (SOTDMA, MITDMA, CSTDMA, etc.);
* Reporting interval (whether it matches the SOG and ROT);
* Transmitted power;
* Frequency error;
* Synchronization jitter;
* Responses to some specific messages, such as signalling, addressing messages and DGNSS broadcast binary messages;
* Alternating between candidate channels;
* Link ID selection.
  1. **Dynamic/static/voyage related AIS information detection**

Dynamic/static/voyage related AIS information detection refers to determine whether the data transmitted by AIS units is valid. The data to be detected includes:

* + 1. Dynamic data
* Whether dynamic data is available;
* Whether the ship's position is reasonable (on land, switch back and forth);
* Whether the receiving base station is reasonable;
* Whether the strength of received signals is in consistence with estimated strength based on dynamic data;
* Whether the estimated position by passive R-mode is in consistence with its reported position.
  + 1. Static data
* Whether static data (MMSI, IMO number, name, etc.) is available;
* Whether static data matches the official database of ship registration information;
* Whether there are conflicts between static data.
  + 1. Voyage related data
* Whether the voyage related data (status, destination, ETA, etc.) is updated according to the actual voyage.
  1. **AIS/VDES messages authorization status detection**

Some AIS/VDES messages, such as safety related messages, hydro meteorological messages, DGNSS broadcast binary messages, should be transmitted under the authorization of the competent authorities. To detect AIS/VDES messages authorization status, the following aspects need to be determined by analyzing received related messages:

* Whether the transmission of the specific AIS/VDES message is authorized;
* Whether the contents of specific AIS/VDES messages are authorized;
* Whether the occupied time slots number of messages is reasonable.
  1. **Protocol vulnerability detection**

The following effective measures are recommended considering the potential attack on VDES protocols:

* Analyzing and sharing of VDES Protocol Vulnerability Catalog;
* Monitoring attack on protocol vulnerability according to the characteristics;
* Monitoring and analyzing of abnormal VDES nodes.

1. **Mitigation**
   1. **Identifying abnormal node**
   2. **Easing unauthorized VDL signalling influence**
   3. **Data modification function**
   4. **Protocol revision**
   5. **Ship terminal**
2. **Implementation**
   1. **Risk analysis**
   2. **Service architecture**
   3. **Implementation process**
3. **Terms and abbreviations**

AIS Automatic identification System

ASM Application Specific Messages

BAS Basic AIS Service

BIIT Built- In Integrity Test

CRC Cyclic redundancy check

DOS Denial of Service

IALA International Association of Marine Aids to Navigation and Lighthouse Au­thorities

IMO International Maritime Organization

PI Presentation Interface

PKI Public Key Infrastructure

PSS Physical Shore Station

VDES VHF Data Exchange System

VDL VHF Data Link

VHF Very High Frequency

1. **References**
2. IMO Resolution MSC.140 (76), Recommendation for the protection of the AIS VHF data link
3. IALA Recommendation A-124 ,The AIS Service
4. ITU-R Recommendation M.1371,Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile band
5. ITU-R Recommendation M.2092, Technical characteristics for a VHF data exchange system  
    in the VHF maritime band

……

Reference documents are the latest from the date of issuance of these guidelines. Readers have to consider that some will be amended or revoked and care should be taken to follow up with the most up to date information.

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)
2. Leave open if uncertain [↑](#footnote-ref-2)