Input paper: [[1]](#footnote-1) DTEC 1-5.1.3.1

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

**□** ARM **□** ENG **□** PAP X Input

X DTEC **□** VTS **□** Information

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

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

Author(s) / Submitter(s) China MSA…………………………………

Working draft of guideline on VDES VDL integrity monitoring

# Summary

Based on the discussion at ENAV31 hybrid meeting and the feedback from the offline communication group, China MSA has revised the working draft of Guideline on VDES VDL integrity monitoring (EM1-5.1.3.2 ) for further consideration at DTEC1.

The purpose of this document is to propose a working draft of Guideline on VDES VDL integrity monitoring. It provides an overview of the source of VDES VDL vulnerability, proposes methods for IALA members to detect and mitigate the effects of abnormal VDL transmissions, and gives suggestions on implementation and enforcement.

# Background

At ENAV28, China MSA proposed a new work item of developing Guideline on VDES VDL integrity monitoring and the Council 74 approved to add this new work item for work programme 2018-2023. At ENAV29, Chapter 1 to 4 of the input draft guideline were discussed and revised. At ENAV30, Chapter 4 to 6 were discussed. Section 5.5 and other technique details were added and improved during the meeting. At ENAV31, the draft guideline underwent a comprehensive review, with relevant technical details further clear and refined. This work has been incorporated into the 2023-2027 work plan of the IALA DTEC Committee. It will be finalized and submitted for silent approval during DTEC1.

# Discussion

At DTEC1, final refinements will be made to the draft guideline and it will be submitted for silent approval. During previous meetings, the progress in the development of this guideline has been as follows:

* discuss and revise Chapter 1 to 4 based on the feedback from ENAV29;
* revise and improve Chapter 4 to 6 and add the new section 5.5 titled ‘Resource coordination’ based on the suggestions at ENAV30;
* conduct a comprehensive review of the entire draft guideline and refine relevant technical details.

# References

1. IALA R0124, *The AIS Service, December 2012*
2. IALA G1117, *VHF Data Exchange System(VDES) Overview, December 2022*
3. ITU-R M.2092-1, *Technical characteristics for a VHF data exchange system in the VHF maritime mobile band, February 2022*

# Action requested of the Committee

The Committee is requested to confirm the content of the 'Guideline on VDES VDL integrity monitoring' and submit it for silent [approval](javascript:;).

|  |
| --- |
| IALA Guideline |

Gnnnn

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** 5

1.1 Purpose 5

1.2 Scope 5

1.3 Text structure 5

**2 Background** 5

**3 Sources of VDES VDL vulnerability** 5

3.1 Unauthorized signaling 5

3.2 Sub-standard devices 6

3.3 Incorrect device configuration and installation 6

3.4 Unauthorized VDES messages 6

3.5 Spoofing messages 6

3.6 DOS attack 6

3.7 Protocol attack 6

3.8 Radio interference 6

**4 Detection** 7

4.1 Air interface status 7

4.2 Signaling detection 7

4.3 Standard compliance detection 7

4.4 Dynamic/static/voyage AIS information detection 8

4.5 VDES messages authorization status detection 8

4.6 Protocol vulnerability detection 9

**5 Mitigation** 9

5.1 Identifying abnormal VDES station 9

5.2 Easing unauthorized signaling influence 9

5.3 Shore-based data modification function 9

5.4 Protocol revision 9

5.5 Resource coordination 10

5.6 Ship terminal 10

**6 Implementation and enforcement** 10

6.1 Risk analysis 10

6.2 Service architecture 11

6.3 Enforcement 13

**7 Terms and abbreviations** 13

**8 References** 14

**List of Tables**

*Table 1 Risk Analysis 10*

**List of Figures**

*Figure 1 VDL Integrity Monitoring Service 12*

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

VDES VDL integrity monitoring includes the AIS, the ASM, and the VDE, all of which is crucial to use VDES properly. VDES VDL integrity monitoring is the process of determining whether the 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 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 competent authorities in deploying and running VDES properly.

* 1. **Text structure**

Chapter 2 provides background on the VDES VDL integrity monitoring.

Chapter 3 lists the sources of VDES VDL vulnerability.

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

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

Chapter 6 outlines the implementation and enforcement of VDES VDL integrity monitoring.

1. **Background**

VDES services are based on 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 competent authorities take the necessary steps. IALA also strongly recommends that a national competent authority be appointed to manage the AIS VDL in R0124. The users and the types of AIS messages, services, 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-R M.2092-1, 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 VDES services.

1. **Sources of VDES VDL vulnerability**

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

* 1. **Unauthorized signaling**

AIS base stations manage the AIS VDL with messages 16, 20, 22 and 23. The VDES base stations and satellites manage the VDE VDL by bulletin boards and other signaling. The bulletin board should apply PKI for signature authentication, but the terminals also accept the ones of authentication failure. Signaling should be transmitted under the authorization of the competent authorities. Unauthorized signaling can cause chaos in 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, reporting interval, and incorrect communication state, etc. It may cause slot conflicts, message errors, or congestion in VDL. In addition, frequency offset or output power which is not compliant with standards should also be considered. Sub-standard devices may also cause incorrect reaction, even no response to specific messages (such as signaling, addressing messages, DGNSS broadcast binary messages, and interrogation messages, etc.). 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 the GNSS antenna of the mobile station is installed incorrectly. These errors and invalid information will reduce the efficiency of data exchange.

* 1. **Unauthorized** **VDES messages**

VDES can send some specific messages, such as safety related messages, hydro-meteorological messages, DGNSS broadcast binary messages, VDE-SAT Network Orbit Data, etc. The transmission of these messages must be authorized to ensure that reliable information is provided. However, VDES lacks verification mechanism for these messages, and unauthorized VDES messages will lead to information confusion.

* 1. **Spoofing messages**

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 competent authorities in tracking targets.

* 1. **Denial of service attack**

Some altered VDES devices can broadcast a large number of messages over the VDL as malicious. The messages occupy or reserve a large number of 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. It 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. **Radio interference**

Radio interference will affect all communication systems. VDES channel will be interfered with by the radios, including co-channel interference from services other than VDES, adjacent channel interference of other maritime services, and spurious emission interference of other high-power equipment. Co-channel interference caused by slot conflicts among VDES stations should also be considered. It could cause error when demodulating VDES signals, so that the message cannot be received normally.

Radio interference from marine VHF radios is not likely because RR Appendix 18 designates these channels for VHF public channels in a duplex configuration. Thus, communications ship to ship is impossible, and ship to shore communications would not be possible without a shore station configured for VHF public correspondence. However, the VHF correspondence service, where it is allowed by an Administration may continue until 1 Jan, 2030.

1. **Detection**

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

* 1. **AIR INTERFACE STATUS detection**

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

* Number of VDES units received by each station;
* Number of slots occupied by VDES stations;
* VDL load;
* Channel loading balance;
* PSS transmissions and coverage;
* CRC error;
* Noise level;
* RSSI.
  1. **Signaling detection**

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

VDES signaling detection analyzes the received signaling to determine:

* Whether the signaling is transmitted by authorized stations;
* Whether the signaling contents and validity duration are authorized;
* Whether there are conflicts between signaling in the same area;
* Whether signaling is coordinated among VDE-TER and VDE-SAT stations.
  1. **Standard compliance detection**

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

* S Slot access compliance (SOTDMA, MITDMA, CSTDMA, etc.);
* Reporting interval (whether it matches the SOG and ROT);
* Transmitted power (approximately);
* Frequency error;
* Synchronization jitter;
* Reaction to some specific messages, such as addressing messages, DGNSS broadcast binary messages, and interrogation messages;
* Alternating between candidate channels;
* Signaling compliance, such as AIS VDL management messages, VDE bulletin board, acknowledgement, resource allocation, and resource de-allocation.
  1. **Dynamic/static/voyage AIS information detection**

Dynamic/static/voyage AIS information detection is used 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, time of arrival);
* Whether the receiving base station is reasonable;
* Whether the strength of the received signal is in consistence with the estimated strength based on dynamic data.
  + 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.

**Voyage related data**

* Whether the voyage related data (status, destination, ETA, etc.) is updated according to the actual voyage.

Big data analysis and ship behavior analysis may be helpful to identify abnormal dynamic/static/voyage AIS information.

* 1. **VDES messages authorization status detection**

Some VDES messages, such as navigational warning, hydro-meteorological messages, DGNSS broadcast binary messages, VDE-SAT Network Orbit Data, etc., should be transmitted under the authorization of the competent authorities. To detect VDES messages authorization status, the following aspects need to be determined by analyzing received related messages:

* Whether the transmission of the specific VDES message is authorized;
* Whether the contents of specific VDES messages are authorized;
* Whether the occupied VDL resource 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 behaviors on protocol vulnerability according to the attack characteristics;
* Monitoring and analyzing of abnormal VDES stations.

1. **Mitigation**

According to the detection results, some measures could be taken to mitigate the VDL integrity anomalies. Potential mitigation solutions are described as follows.

* 1. **Identifying abnormal VDES station**

For the VDES station with anomalies caused by sub-standard devices, incorrect device configuration and installation, unauthorized VDES messages, etc., they can be identified based on the information of messages. And the authority could take corresponding actions.

For the VDES station with anomalies caused by DOS attack, spoofing messages, etc., the position information may not be carried in the messages, or the position information may be invalid. The tag block of messages can identify the receiving station's location to identify the attack source's approximate location. Under certain conditions, the abnormal VDES station can be localized by performing direction-finding on its signals. And then, the authority could take corresponding actions.

* 1. **Easing unauthorized signaling influence**

In some cases, the shore station may transmit new appropriate signaling to eliminate the influence of abnormal signaling.

For the unauthorized Message 16, Message 20, Message 22, and Message 23, the authorized station can transmit the new signaling message to the corresponding area to reset the default settings.

For the unauthorized bulletin board, the authorized station can also transmit the new bulletin board to refresh the physical layer settings within the influenced area.

* 1. **Shore-based data modification function**

By matching with the relevant information according to the official database, the shore-based service can take corresponding measures to mitigate the effects of missing fields, information conflicts, and incorrect data caused by incorrect device configuration and installation.

* Identifying the incorrect messages and fields;
* Providing users with the modified AIS data and the original messages to mitigate these effects.
  1. **Protocol revision**

Due to the complexity of VDES protocol and uncertainty of the attack mode, corresponding countermeasures should be taken.

* T Taking provisional measures according to the detected attack;
* Standard revision.

## Resource coordination

VDE-TER and VDE-SAT share VDE channels and the resources need to be coordinated to avoid signaling conflicts and improve the reliability and throughput of VDES. The corresponding countermeasures should be taken:

* VDES channel and slot resource coordination among VDE-TER stations should be managed by the competent authority;
* VDES resource allocation between VDE-TER and VDE-SAT should be coordinated by the competent authorities in accordance with IALA Guidelines;
* Resource coordination should be performed among satellite service providers in accordance with IALA Guidelines

## Ship terminal

Besides the internal integrity monitoring function, the ship terminal should have the ability to identify the apparent anomalies and filter data to mitigate the confusion to seafarers.

* BIIT: It is recommended to supplement comprehensive integrity requirements for equipment BIIT;
* Garbage filter: Filtering some obvious invalid information to avoid or tag these information outputs to PI.
* Supporting integrity services from shore side: The ship terminal could benefit from encapsulated integrity monitoring services by the shore side.

# Implementation and enforcement

## Risk analysis

Table 1 gives risk assessments of the different vulnerability sources in terms of their perceived probability of occurrence, consequences, and mitigation difficulty. This risk analysis helps to identify the threats that should be addressed by the authority, particularly those with high probability and high consequences. For those issues with highly difficult mitigation, the authority should prepare some response plans in advance and take timely reaction.

1. Risk Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Source | Probability | Consequence | Mitigation difficulty |
| Unauthorized signaling | L | H | M |
| Sub-standard devices | M | L | L |
| Incorrect device configuration and installation | M | L | L |
| Unauthorized VDES messages | L | L/M/Ha | L |
| Spoofing messages | L | M | H |
| DOS attack | L | H | H |
| Protocol attack | L | H | L/M/Hb |
| Radio interference | M | M | M |

a: The level of the consequences is decided based on the attribution of the VDES messages.

b: Mitigation difficulty needs to be further assessed based on the specific protocol vulnerabilities and types of attack.

* 1. **Service architecture**

The architecture comprises two aspects, the ship terminal and the shore-based system. An example of the architecture is shown in Figure 1. The shore-based VDL integrity monitoring service is an application of shore-based VDES services. VDL integrity detection is performed according to the VDL raw data from the VDES base station, other data from the ship database, signal analyzer, etc. Potential risks are detected in time, and corresponding mitigation measures can be taken.

In the ship terminal, VDL integrity monitoring relies on BIIT, message filtering, and shore-based VDL integrity services. It reduces the impact of abnormal messages on bridge equipment.



1. VDL Integrity Monitoring Service

The following processes to realize the shore-based VDES integrity monitoring should be included:

* Data access
* Pre-processing
* Detection
* Mitigation
* Human Machine Interfaces (HMI) / Application programming interface (API)

## Enforcement

For some scenarios, the authority should take necessary enforcement as timely reactions according to the detection and mitigation results. Enforcement should be by the competent authorities resulting in equipment inspection and appropriate corrective actions.

* VDL integrity anomalies output from API;
* Analysis of VDL integrity abnormal issues;
* The formulation of a specific realistic program;
* The action of enforcement with modification in the process;
* The evaluation and summary.

# Terms and abbreviations

ADM ASM VHF Data-Link Message

ADO ASM VHF Data-Link Own-Vessel Report

AIS Automatic Identification System

API Application Programming Interface

ASM Application Specific Messages

BAS Basic AIS Service

BIIT Built-In Integrity Test

CRC Cyclic Redundancy Check

CSTDMA Carrier Sense Time Division Multiple Access

DGNSS Differential Global Navigation Satellite Systems

DOS Denial of Service

ECDIS Electronic Charts Display Information System

EDM VDE Broadcast Message

EDO VDE Data Message Sentence own Report ...

ETA Estimated Time of Arrival

FSR Frame Summary of AIS Reception

GNSS Global Navigation Satellite Systems

HMI……………… Human Machine Interfaces

IALA International Association of Marine Aids to Navigation and Lighthouse Au­thorities

IMO International Maritime Organization

MITDMA Multiple Incremental Time Division Multiple Access

MMSI Maritime mobile service identity

PI Presentation Interface

PKI Public Key Infrastructure

PSS Physical Shore Station

ROT Rate of Turn

RSSI Received Signal Strength Indicator

SOG Speed over Ground

SOTDMA Self Organized Time Division Multiple Access

VDE VHF Data Exchange

VDES VHF Data Exchange System

VDE-SAT VHF Data Exchange-Satellite

VDE-TER VHF Data Exchange-Terrestrial

VDL VHF Data Link

VDM VHF Data Link Message

VDO VHF Data Link message Own

VHF Very High Frequency

VSI VDL Signal Information

# References

1. IMO Resolution MSC.140 (76), Recommendation for the protection of the AIS VHF data link, December 2002
2. IALA R0124, The AIS Service, December 2012
3. ITU-R Recommendation M.1371-5, Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile band, February 2014
4. ITU-R M.2092-1, Technical characteristics for a VHF data exchange system in the VHF maritime mobile band, February 2022
5. IALA G1117, VHF Data Exchange System (VDES) Overview, December 2022
6. NMEA 0183, Standard for Interfacing Marine Electronic Devices, November 2018

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)