IALA GUIDELINE

GNNNN
VDES VDL INTEGRITY MONITORING

Edition 1.0
December 2023

urn:mrn:iala:pub:gnnnn

10, rue des Gaudines - 78100 Saint Germain en Laye, France
Tél. +33 (0)1 34 51 70 01- Fax +33 (0)1 34 51 82 05 - contact@iala-aism.org
www.iala-aism.org

International Association of Marine Aids to Navigation and Lighthouse Authorities
Association Internationale de Signalisation Maritime

DOCUMENT REVISION

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

Date	Details	Approval
December 2023	First issue.	Council 79

CONTENTS

CONTENTS

List of Tables

List of Figures

1. INTRODUCTION

VDES VDL integrity monitoring includes the AIS, the ASM, and the VDE, all of which are integrated in VDES. VDES VDL integrity monitoring is the process of determining whether the VDES VDL is subject to the injection of errors impacting the reliability and integrity of the data and/or the VDL itself. 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.

2. SCOPE

This Guideline deals ewith guidance for stakeholders, ship and shore, and competent authorities in protecting VDES from risks to its integrity. Among other things, it describes:

- Background on the VDES VDL integrity monitoring.
- Lists the sources of VDES VDL vulnerability.
- Describes VDES VDL integrity detection and proposes corresponding methods.
- Gives potential solutions to mitigate the negative effects on shore and ships.
- Outlines the implementation and enforcement of VDES VDL integrity monitoring.

3. 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 has a larger potential for integrity issues to arise. Therefore, it is necessary to monitor the VDL integrity and mitigate the effects to ensure the reliability and resiliency of the VDES services.

4. 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.

4.1. 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 (Public Key Infrastructure) for signature authentication, but the terminals are programmed to accept bulletin boards 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.

4.2. MISBEHAVING DEVICES

Misbehaving devices may lead to abnormal slot access, channel selection, reporting interval, and incorrect communication state, etc. They may cause slot conflicts, message errors, or congestion in VDL. In addition, frequency offset or output power which is not compliant with standards can also occur. Devices misbehaving 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 misbehaving devices due to the requirement of reliable data transmission.

4.3. 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. Incorrect configuration of VDES equipment may also be done maliciously by a ship wanting to mask its identity or other information such as cargo.

It may provide benefit to ensure that the latest compatible firmware for the VDES hardware is installed and correctly configured with the accurate and complete required information being entered into the VDES device.

4.4. 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 should be authorized and planned to ensure that reliable information is provided. However, VDES lacks verification mechanism for these messages, and unauthorized VDES messages will lead to information confusion.

4.5. 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.

4.6. SPOOFING AND JAMMING OF GNSS AND DGNSS DATA

Position data can be impacted by radio interface spoofing and/or jamming of the GNSS signals leading to inconsistent position data being transmitted by the VDES unit. The IALA Guidelines on Resilient PNT should be followed.

4.7. 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.

4.8. PROTOCOL ATTACK

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

4.9. 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. 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.

4.10. 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.

Table 1 Risk Analysis

Source	Probability[c]	Consequence[c]	Mitigation difficulty[c]
Unauthorized signalling	L	H	M
misbehaving devices	M	L	L
Incorrect device configuration and installation	M	L	L
Unauthorized VDES messages	L	L/M/H[a]	L
Spoofing messages	L	M	H
DOS attack	L	H	H
Protocol attack	L	H	L/M/H[b, c]
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.

c: L means “Low”, M means “Medium”, H means “High”.

5. IALA’S PROPOSED APPROACH

To mitigate the risks related to the VDES vulnerabilities identified above, IALA recommends that its members adopt a 5 steps approach to VDES integrity.

- Detect
- Investigate
- Report
- Inform and Defend
- Regulate and Enforce

The sections below will discuss each of these steps in detail.

6. 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.

6.1. 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; and
- RSSI (Received Signal Strength Indicator).

6.2. 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 4, 15, 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;
- the signaling contents and validity duration are authorized;
- there are conflicts between signaling in the same area; and
- signaling is coordinated among VDE-TER and VDE-SAT stations.

6.3. 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:

- slot access compliance (SOTDMA, MITDMA, CSTDMA, etc.);
- reporting interval (whether it matches the NAVSTATUS, 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;
- correct channel used; and
- correct message structure.

In addition to the elements above, it is recommended to monitor the Frequency and Time domain of each channel to detect any misbehaving device that could be a source of interference.

It is recommended that the conformance of all devices participating in VDES be assessed at a minimum against relevant standards.

6.4. 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:

6.4.1. 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; and
- Whether the strength of the received signal is in consistence with the estimated strength based on dynamic data.

6.4.2. STATIC DATA

- Whether static data (MMSI, IMO number, name, etc.) is available and consistent;
- Whether static data matches the official database of ship registration information; and
- Whether there are conflicts between static data.

6.4.3. 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.

6.5. 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; and
- Whether the occupied VDL resource is reasonable.

6.6. 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; and
- Monitoring and analyzing of abnormal VDES stations.

7. INVESTIGATION

The investigation aims at identifying the source of the anomaly detected and the reason for this anomaly. For example, an interfering signal may be caused by a specific manufacturer software issue.

8. REPORT

The integrity disturbance is recommended to be reported by the shore authority to the ship or ships involved, the competent regulatory authorities as well as the manufacturer when applicable.

9. INFORM AND DEFEND

As shore authorities consider action to stop the source of the integrity disturbance, it is recommended that the shore authority takes the time to educate participants on why the issue is problematic and it needs to be stopped and avoided in the future. According to the detection results, some measures could be taken to mitigate the VDL integrity anomalies. Potential mitigation solutions are described as follows.

9.1. ADDRESSING ABNORMAL VDES STATION

For the VDES station with anomalies caused by misbehaving 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 such as requesting that the situation be corrected and explaining why this is important and how the situation impacts the work of all channel participants.

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 such as requesting that the misbehaving unit be shut down and why.

9.2. 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.

9.3. 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.

9.4. PROTOCOL REVISION

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

- Taking provisional measures according to the detected attack; and
- Standard revision.

9.5. 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; and
- resource coordination should be performed among satellite service providers in accordance with IALA Guidelines

10. REGULATION AND ENFORCEMENT

For some scenarios, the authority should take necessary enforcement steps as timely reactions according to the detection and mitigation results. Enforcement steps should be taken by the competent regulatory authorities resulting in equipment inspection, appropriate corrective actions and in some instances interdiction to sail and/or even fines.

11. EXAMPLE SERVICE ARCHITECTURE

The example 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 (Built-In Integrity Test), message filtering, and shore-based VDL integrity services. It reduces the impact of abnormal messages on bridge equipment.

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

- Data access
- Pre-processing
- Detection
- Mitigation
- Human Machine Interfaces / Application programming interface

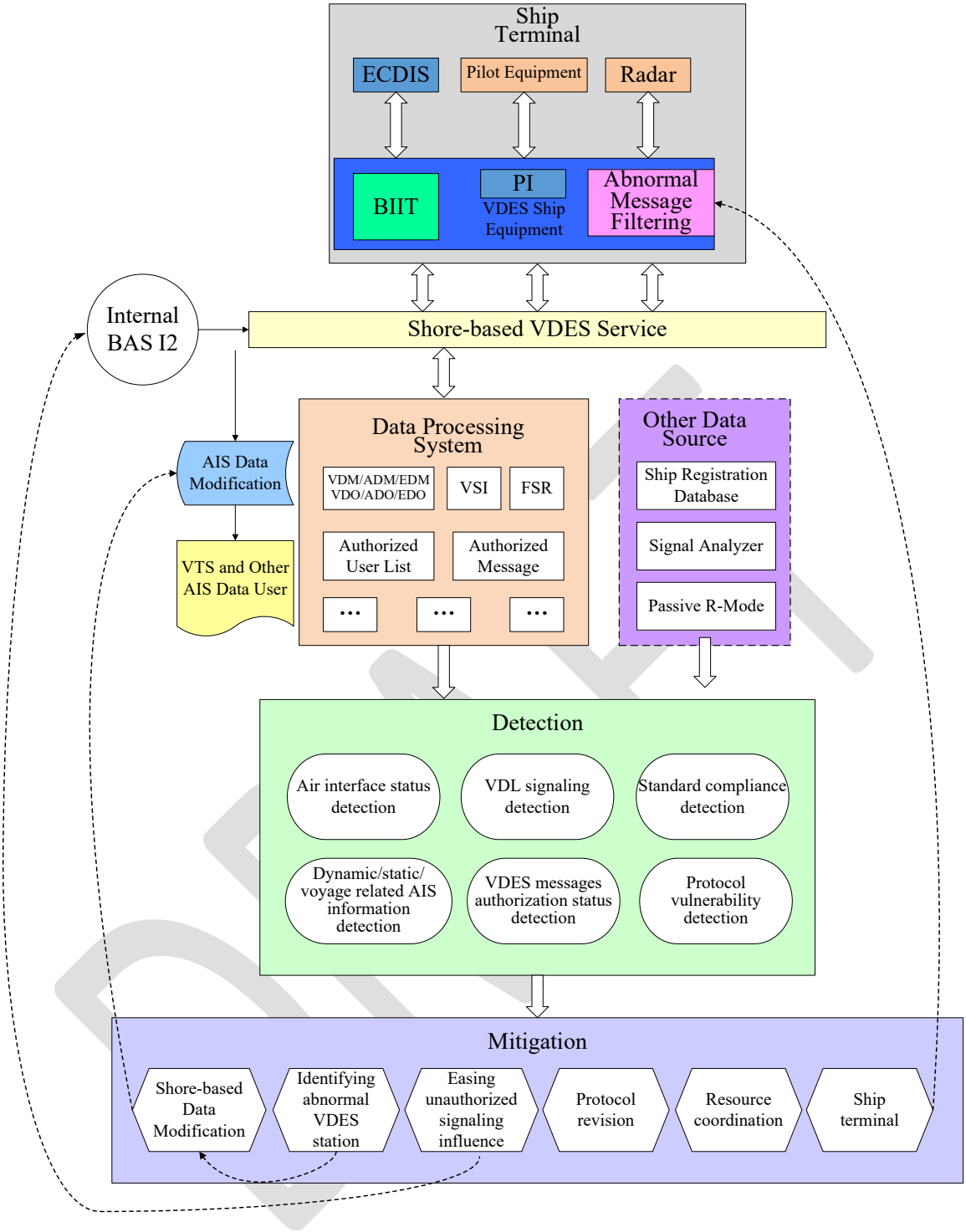

Figure 1 VDL Integrity Monitoring Service

12. TERMS AND ABBREVIATIONS

ADM	ASM VHF Data-Link Message
ADO	ASM VHF Data-Link Own-Vessel Report
AIS	Automatic Identification System
ASM	Application Specific Messages
BAS	Basic AIS Service
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
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
PSS	Physical Shore Station
ROT	Rate of Turn
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

13. REFERENCES

[1] IMO Resolution MSC.140 (76), Recommendation for the protection of the AIS VHF data link, December 2002

[2] IALA R0124 on The AIS Service

[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 on VHF Data Exchange System (VDES) Overview

[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.