Input paper: ENAV28-5.1.3.4[[1]](#footnote-1)

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

□ ARM □ ENG □ PAP **☑** Input

**☑** ENAV□ VTS □ Information

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

Technical Domain / Task Number2 …………………………………

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

Proposal for the development of Guideline on AIS/VDES VDL integrity monitoring

# Summary

In resolution MSC.140 (76) the IMO recognizes a compelling need to ensure the integrity of the AIS VDL and recommends that administrations 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 getting increased with the development of AIS. According to this situation, the risk of AIS VDL overloading emerged and shows the vulnerability of AIS. VDES has larger data transfer rate and more complex services. Its VDL is also more vulnerable. Therefore, it is necessary to make monitoring the VDES VDL integrity as a shore-based service to ensure the effectiveness of the AIS/VDES services.

# Purpose of the document

This document proposes a Guideline on AIS/VDES VDL Integrity Monitoring for IALA Members to ease the vulnerability of AIS/VDES VDL.

# Action requested

The committee is invited to consider the draft guideline provided in the Annex, and jointly supplement the contents of the guideline.

|  |
| --- |
| IALA Guideline |

GUIDELINE ON AIS/VDes vdl integrity monitoring

Version x.x

Text date

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

|  |  |  |
| --- | --- | --- |
| Date | Page/Section Revised | Requirement for Revision |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1 Introduction 5

1.1 Purpose 5

1.2 Scope 5

1.3 Text structure 5

2 Background 5

3 Source of VDL vulnerability 5

3.1 Fake message 5

3.2 Public VDL signalling 5

3.3 DOS (Denial of-service) attack 6

3.4 Substandard devices 6

3.5 Attack on the VDES protocol vulnerability 6

4 Function of VDL integrity monitoring 6

4.1 Definition 6

4.2 Function 7

5 Service architecture 8

5.1 Service process implementation 8

5.2 Data access services 8

5.3 Pre-processing service 8

5.4 VDL monitoring services 8

5.5 Man-machine interface service 8

5.6 Interoperable interface service 8

6 Terms and abbreviations 9

7 References 9

List of pictures

Figure 1 Figure 1 5

Figure 2 Figure 2 7

# Introduction

## Purpose

This document provides information to IALA national members to monitor AIS/VDES VDL integrity and ease the vulnerability of AIS/VDES VDL.

……

## Scope

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

……

## Text structure

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

Chapter 3 lists the source of AIS vulnerability.

Chapter 4 defines and details the functional requirements of the AIS/VDES's VDL monitoring.

Chapter 5 outlines the services of AIS/VDES monitoring.

# Background

AIS/VDES VDL is the carrier of AIS/VDES services. It has 2 AIS channels (2087 and 2088), 2 ASM channels (2027 and 2028), 2 LAIS channels (2075 and 2076), and 12 VDE channels (1024, 1084, 1025, 1085, 1026, 1086, 2024, 2084, 2025, 2085, 2026 and 2086). ITU also provided for administrations to designate “regional frequency channels for AIS” where channels 2087 and 2088 are unavailable.

In resolution MSC.140 (76) the IMO recognizes a compelling need to ensure the integrity of the AIS VDL and recommends that administrations 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 getting increased with the development of AIS. According to this situation, the risk of AIS VDL overloading emerged and shows the vulnerability of AIS. VDES has larger data transfer rate and more complex services. Its VDL is also more vulnerable. Therefore, it is necessary to make monitoring the VDES VDL integrity as a shore-based service to ensure the effectiveness of the AIS/VDES services.

# Source of VDL vulnerability

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

## Fake message

AIS/VDES messages should carry real information and services. But the fake messages carry information based on sources or needs not actually exist. Such fake messages can be fake dynamic data in AIS, false hydrometeorology and distress information in ASM, and etc.. They may significantly reduce the VDL reliability, and mislead the crew in making decisions.

## Public 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 broadcasting by bulletin boards and other signaling. The bulletin board should use PKI for signature authentication, but the terminals also accept the ones of authentication failure. This means public VDL signaling can easily destroy the signaling mechanism of AIS/VDES, and crash the system.

## DOS (Denial of-service) attack

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

## Substandard devices

If the device is not designed in strict accordance with standards, or the device itself is defective, it will lead to abnormal time slot access, channel selection, broadcast interval, etc., and may cause time 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.

## Attack on the VDES protocol vulnerability

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.

# Function of VDL integrity monitoring

## Definition

The purpose of VDL integrity monitoring is to help administrations to monitor the performance of AIS/VDE VDL, to identify and verify signaling and content of messages, so as to identify [substandard](C:/Program%20Files%20(x86)/Youdao/Dict/8.9.6.0/resultui/html/index.html#/javascript:;) devices, abnormal broadcasts and attack behaviors. For the traceable VDL signaling messages, the system should automatically give instructions to cope with abnormal VDL signaling to eliminate the impact.

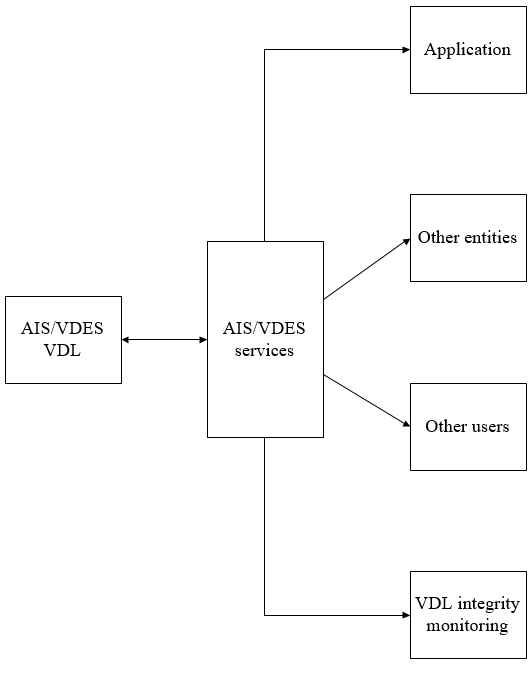


Figure 1 Relationship between AIS Services and VDL integrity monitoring

## Function

### AIS/VDES VDL integrity monitoring includes following services.

……

### Monitor AIS/VDES shore-based network status.

……

### Analyze whether AIS/VDES messages are licensed or not.

……

### Monitor dynamic/static/voyage AIS information.

……

### Monitor VDL slots access.

……

### Monitor AIS/VDES device protocol compliance.

……

### Monitor AIS VDL management messages.

……

### Monitor VDE bulletin boards.

……

### Match VDE protocol vulnerability libraries to identify attacks.

……

### Eliminate abnormal VDL signaling.

……

# Service architecture

## Service process implementation

To realize the AIS/VDES integrity monitoring service, following should be included:

1. Human Machine Interfaces (HMI).
2. Data access service.
3. Pre-processing service.
4. VDL monitoring services.
5. Interoperating service.



Figure 2 VDL integrity Monitoring Service Architecture

## Data access services

……

## Pre-processing service

……

## VDL monitoring services

……

## Man-machine interface service

……

## Interoperable interface service

……

# Terms and abbreviations

VDL: VHF Data Link

VHF: Very High Frequency

AIS: Automatic identification System

VDES: VHF Data Exchange System

IMO: International Maritime Organization

IALA: International Association of Marine Aids to Navigation and Lighthouse Authorities

ASM: Application Specific Messages

PKI: Public Key Infrastructure

DOS: Denial of Service

# References

……



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