IALA GUIDELINE

G1130
TECHNICAL ASPECTS OF INFORMATION EXCHANGE BETWEEN VTS AND ALLIED OR OTHER SERVICES

Edition 2.0
December 2022

urn:mrn:iala:pub:g1130:ed2.0

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 2017	1st issue	Council 65
January 2022	Edition 1.1 Editorial corrections published January 2022, in alignment with IMO Resolution A.1158(32) Guidelines for Vessel Traffic Services.	Council 74
December 2022	Edition 2.0 Added new section 3.5.1 on cyber security considerations	Council 76

CONTENTS

1. INTRODUCTION

1.1. PREAMBLE

As outlined in IALA Guideline *G1102* VTS *Interaction with Allied or Other Services* [9], a vessel traffic service (VTS) is recognized as a valuable asset to reduce incidents resulting from conflicts in vessel traffic. Also, the role of VTS is well established, and its services are well positioned in the maritime domain.

It is recognized that information, collected by a VTS, could be used to support allied and other services in order to improve efficiency and reduce cost. In addition, information from these parties could be useful for improving the VTS operation.

1.2. OBJECTIVE

As part of their operation, VTS providers compile a real-time picture of the maritime traffic within the VTS area and may also collect additional information pertaining to the traffic flow and the environment. This information can assist allied or other services with their own tasks, and it is likely that allied or other services may have information that can assist a VTS provider.

There may be situations where allied and other services collect the same data as the VTS provider but through independent means. By establishing mutual agreements on the exchange of information, information only needs to be collected once. This:

- increases the consistency and reliability of the information;
- improves the efficiency of all parties involved; and
- may lead to considerable cost savings.

This Guideline describes, from a technical point of view, the issues to be considered and the principles to be applied for interaction between VTS and allied or other services.

2. INFORMATION EXCHANGE BETWEEN VTS AND ALLIED OR OTHER SERVICES

2.1. THE TECHNICAL INTERFACE

Guideline *G1102* contains an overview of allied and other services that may want to exchange information with a VTS. It also provides guidance on setting up an agreement to cover the operational and legal aspects of the information exchange. This will, in general, include a service level agreement which will have an impact on the technical realization. Additionally, an agreement should be made on the specific technical aspects of the information exchange.

The technical aspects of information exchange should be consolidated in a technical interface description. Where possible, applicable standards, such as S-100, should be considered and used. The technical interface is mostly determined by the type and timing aspects of the information. So, it is possible that the same technical interface applies to information exchange with different allied or other services.

As far as VTS information is concerned, the following types of data could be exchanged:

1 Voyage related data, containing information on past, present and future voyages of vessels and their cargo*

2 Traffic image data, containing information on the position, speed and identity of vessels*

3 Surveillance sensor data, such as radar, Automatic Identification System (AIS) and Electro Optic System (EOS)

4 Meteorological, geographical and hydrographical information

5 Voice communication data such as VHF, and telephone.

Note * - for Items 1 and 2 the reader is referred to IALA Recommendation *R0145 Inter-VTS Exchange Format Service (V-145)*, which defines an appropriate standard

Another important factor to consider, when defining a technical interface, is timing. This factor can be further divided into:

- Real-time, i.e., data that changes on a timeframe in a matter of seconds
- Non-real-time, data that changes on a timeframe in a matter of minutes
  - Static/semi-static, pertinent data or data that changes infrequently
  - Historical, i.e., recorded data.

2.2. DEFINING THE TECHNICAL INTERFACE

At least, the following aspects should be considered when defining the technical interface:

- The data format, i.e., how will the information be represented:
  - Communication channel characteristics
  - Data model, including semantics
  - Version control
- Timing of the information exchange:
  - Messaging pattern
  - Time stamping
- Availability and data integrity:
  - Availability of equipment and services
  - Availability of data
  - Data integrity
- Security of the information:
  - Data confidentiality
  - Data accessibility
  - Audit trails

2.3. HISTORICAL DATA

VTS and allied or other services may be legally required to maintain records of historical data. There may also be other uses of historical data, e.g., to gather statistics for strategic decision making or for research purposes.

When exchanging historical data, special consideration should be given to:

- The data to be retained, which could be a subset of the available data
- The time period to store data on-line/off-line
- Adequate storage capacity to cover the required time period
- Facilities for searching through and providing access to historical data

Most, if not all, considerations regarding the technical aspects of information exchange (as covered in section 0) apply to the exchange of historical data as well.

3. TECHNICAL ASPECTS OF INTERACTION WITH ALLIED OR OTHER SERVICES

3.1. INTRODUCTION

This chapter addresses the specific technical aspects of data exchange. Each section addresses a particular aspect of the technical interface in more detail.

3.2. DATA FORMAT

3.2.1. COMMUNICATION CHANNEL CHARACTERISTICS

The transfer of data between sender and receiver requires connectivity via a network. A network comprises appropriate hardware and software interconnected by communication channels which may be wired or wireless. Each communication channel has a limited capacity and characteristics that affect the speed at which data can be transferred. The design of the data exchange should consider the characteristics of the underlying communication channel(s).

3.2.2. DATA MODELS

Exchange of information requires an understanding of how information is encoded, i.e., how data values are represented and an unambiguous description of their meaning (including the appropriate business context). This is captured in a data model which describes:

- the structure of the data in terms of data fields;
- the semantics of the data fields, including the appropriate context; and
- the permissible ranges of a data field, including representation of invalid/not available data.

The IHO S-100 standard [9] (*ISO 19xxx*- series) is a specific framework standard for the development of data models for a variety of common and maritime-specific information. S-100 data models are maintained in the IHO GI Registry and IALA was assigned its own section within this registry.

3.2.2.1. Version Control

Version control procedures should be established to allow additions to and/or further development of the technical interface. Preferably, versioning should be defined as a part of the technical interface.

3.3. TIMING

3.3.1. MESSAGING PATTERN

Different messaging patterns may be used, depending on the specific data sharing requirements. In particular, data may be sent from one sender to exactly one receiver or from one sender to many receivers. The following patterns are most common:

- Publish versus Subscribe; with “publish”, the sender determines what data will be made available and when (independent of any receivers); with “subscribe” the receiver requests what (and, sometimes, when) data will be sent.
- Push versus Pull; with “push” the sender determines what data will be sent and when; with “pull” the receiver requests what data will be sent and when.
- Request/response; with “request” the receiver sends a request for data to the sender; with “response” the sender determines when the requested data will be sent to the receiver.
- Continuous data connection (possibly with a “heart beat” to allow redundancy).
- Time stamping

In principle, data should be appropriately time stamped. The time stamp should preferably be at the time of origin of the data. If this is not possible, the data should be time-stamped when received.

Proper time stamping is a pre-requisite e.g., for proper sequencing of the data and recording and replay.

3.4. AVAILABILITY AND DATA INTEGRITY

3.4.1. AVAILABILITY OF EQUIPMENT AND SERVICES

Careful consideration should be given to the required availability as part of the agreement between VTS and allied or other services. A trade-off should be made between availability and cost. High levels of availability require more complex system architectures and correspondingly higher costs.

A simple means of improving availability is by having spare parts readily available (which reduces the repair time). More complex solutions use redundant hardware and/or services.

3.4.2. AVAILABILITY OF DATA

Consideration should be given to proper backup of data. This means that data can be restored in case it gets corrupted or deleted:

- Backup frequency (incremental/full)
- Backup media (disk/tape/cloud/paper punch)
- Retention of backup copies
- Time needed to restore data from backup
- Safekeeping of backup copies (protection, geographic diversity)

3.4.3. DATA INTEGRITY

Data integrity is a key concern for both users and providers of data. This means that, in general,

- data should be traceable to its origin;
- data corruption/alteration should be detectable;

- data should be properly time-stamped and should, preferably, have a quality attribute; and
- data providers should have procedures in place to ensure the proper functioning of the data capture/generation process.

Data that is not available or is detected as invalid should be represented as such.

3.5. SECURITY

3.5.1. CYBER SECURITY

It is recommended to adopt an appropriate cyber-security framework that defines the measures to safeguard uncompromised system operation and to prevent unauthorised access. These measures may include:

- revising system and network architecture;
- reconsidering system access procedures for both internal and external users;
- establishing procedures to maintain software updated to the latest security patches, including software on network- and housekeeping devices;
- monitoring and validating system network dataflows; and
- properly safeguarding legacy systems that are still in operation.

Where, traditionally, systems operated in closed environments, increasingly, VTS systems need to share data with external stakeholders. This requires due consideration of authentication and authorisation of these external stakeholder, but also of measures to protect the data exchange as outlined in the following sections.

3.5.2. DATA CONFIDENTIALITY

The data exchanged between VTS, and allied or other services may have considerable business value and/or contain data that is privacy-sensitive. Therefore, proper care should be taken to protect this data while stored and during transmission.

It is recommended to use an appropriately secured transmission channel, e.g., a virtual private network (VPN), to avoid unauthorized access during data transmission. Also, when sensitive data is stored, it may be appropriate to encrypt the data.

Specific legal constraints may apply to data that can be related to the identity of persons.

3.5.3. DATA ACCESSIBILITY

Access to data should be properly governed, which means that proper procedures should be set-up to limit access to sensitive data to authorized personnel only.

3.5.4. AUDIT TRAILS

It may be appropriate to maintain audit trails of access to sensitive data. Additionally, it may be necessary to attach audit trails to the sensitive data itself, e.g., recording all transactions that were executed with that particular data.

4. ADDITIONAL LEGAL ASPECTS AND CONSTRAINTS

Legal aspects and constraints with respect to operational use of shared information are already considered in IALA Guidelines *G1102 VTS Interaction with Allied or Other Services* and *G1086 Global Sharing of Maritime Data and Information,* in particular.

Further legal requirements may be applicable to the technical realization, such as:

- Privacy, e.g., there may be requirements for access to and storage of data
- Storage, e.g., limitations on the maximum allowed period

5. DEFINITIONS

The definitions of terms used in this Guideline can be found in the *International Dictionary of Marine Aids to Navigation* (IALA Dictionary) and were checked as correct at the time of going to print. Where conflict arises, the IALA Dictionary should be considered as the authoritative source of definitions used in IALA documents.

6. ABBREVIATIONS

AIS	Automatic Identification System
EOS	Electro-Optical System
GI	Geospatial Information Registry (IHO)
IHO	International Hydrographic Organization
IMO	International Maritime Organization
SOLAS	International Convention for the Safety of Life at Sea (1974, as amended)
S-100	IHO universal hydrographic data model (i.e. the product framework governing the Geospatial Information Registry)
VPN	Virtual private network
VTS	Vessel traffic service or vessel traffic services (dependent on context)

7. REFERENCES

[1] IMO. SOLAS Chapter V, Regulation 12 Vessel Traffic Services

[2] IMO. Resolution A.1158(32) Guidelines for Vessel Traffic Services

[3] IALA. Recommendation R0127 Operational Procedures for Vessel Traffic Services (V-127)

[4] IALA. Recommendation R0128 VTS Systems and Equipment

[5] IALA. Guideline G1086 Global Sharing of Maritime Data and Information

[6] IALA. VTS Manual

[7] IALA. NAVGUIDE

[8] IALA. Guideline G1018 Risk Management

[9] IALA. Guideline G1102 VTS Interaction with Allied or Other Services

[10] IHO. S-100

[11] IALA. Recommendation R0145 Inter VTS Exchange Format (IVEF) (V-145)