INTERNATIONAL STANDARD

ISO 24060

First edition
2021-07

Ships and marine technology — Ship software logging system for operational technology

iTeh STANDARD PREVIEW
(standards.iteh.ai)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 24060:2021
https://standards.iteh.ai/catalog/standards/sist/e480fd6c-a645-4cf5-990f-
c3662e85ac86/iso-24060-2021

COPYRIGHT PROTECTED DOCUMENT

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 11, *Intermodal and Short Sea Shipping*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Ships have more and more equipment with updateable software on-board. Current requirements for on-board use of computer-based systems require a software registry for such equipment (IACS URE22rev2), but these registries are not defined, can be difficult to understand and use, and are often not updated. This is partly caused by the increasing quantity of computer equipment and applicable regulations creating additional work for crew, shipping companies and other stakeholders. This situation makes staying current on software updates more difficult, which also introduces increased risks of equipment problems. This document began its development based on a 2017 CIRM-BIMCO industry standard for software maintenance procedures.

This document defines a ship software logging system (SSLS) for shipboard equipment software. Recognizing that maintenance of shipboard software is a major undertaking, this first edition initially sets base characteristics. The SSLS can be used by various users and log data from various types of equipment. It is expected that this document will evolve over time together with related regulations and as experience on the use of the introduced concept accumulates.

This document considers the following:

— cyber risk management is incorporated into the design and use of the SSLS;

— equipment messages pass from the equipment to the SSLS automatically when possible;

— the equipment sends standard version messages with software version information on appropriate time intervals.

iTeh STANDARD PREVIEW

(standards.iteh.ai)

ISO 24060:2021
https://standards.iteh.ai/catalog/standards/sist/e480fd6c-a645-4cf5-990f-
c3662e85ac86/iso-24060-2021

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ships and marine technology — Ship software logging system for operational technology

1 Scope

This document defines a ship software logging system (SSLS) for logging and retrieving software version information and current operational status. The system facilitates software maintenance for ship operational technology equipment and associated integrated systems, including but not limited to:

— control and alarm systems;

— fire and water mist systems;

— navigation and communication systems;

— steering control systems;

— propulsion systems;

— power generation systems;

— performance monitoring systems;

— auxiliary systems.

This document sets requirements for the design and usability of a ship software logging system (SSLS) software that:

— records software versions for equipment with updateable software (hereinafter "equipment");

— sets an initial log entry when equipment is first installed or detected by the SSLS;

— includes a repository of electronic service reports associated with log entries;

— automatically logs reports sent by the equipment.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
category of update
classification assigned to a software update based upon the reason for undertaking the update, which can be any one of the below or some combination:

— initial state;

— bug fix (resolving software bugs);

— compliance update (maintaining conformity with regulations);

— critical update [critical to restoring proper performance of the *shipboard equipment* (3.10)];

— feature release (adding additional functionality);

— obsolescence update (addressing software and/or hardware that is no longer supported);

— security update (protecting against cyber threats);

— other (requires explanation).

3.2
controlled network
shipboard network designed to operate such that it does not pose any unacceptable safety and security risks to any connected network nodes

3.3
critical update
software update identified as critical to restoring proper performance of the *shipboard equipment* (3.10)

3.4
data
quantities, characters, or symbols on which operations are performed by computers of *shipboard equipment* (3.10)

3.5
equipment
devices involved in the operation of a ship

Note 1 to entry: See also *shipboard equipment* (3.10) and *operational technology* (3.7).

3.6
integrated system
interconnected system combining a number of different *shipboard equipment* (3.10)

3.7
operational technology
OT
devices, sensors, software and associated networking that monitor and control onboard systems

3.8
removable external data source
REDS
user removable non-network data source, including, but not limited to, compact discs, memory sticks and Bluetooth™[1)] devices

3.9
ship software logging system
SSLS
software maintenance logging system for onboard equipment software

---

1) Bluetooth ™ is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of this product.

3.10
shipboard equipment
system comprising a combination of hardware, software and *data* ([3.4](#)), performing a specific function on board a ship

Note 1 to entry: See also *operational technology* ([3.7](#)).

3.11
shipowner
shipping company
owner of the ship or any other organization or person such as the manager, or the bareboat charterer who has assumed responsibility for operation of the ship and who is responsible for initiating *software maintenance* ([3.14](#)) of the *shipboard equipment* ([3.10](#))

3.12
software
programs and operating instructions used in shipboard operational technology equipment, including any updatable firmware and configuration

3.14
software maintenance
checking, updating, re-configuring, or upgrading the software of *shipboard equipment* ([3.10](#)) in order to prevent or correct faults, maintain regulatory compliance, and/or improve performance

3.15
system integrator
stakeholder that combines *shipboard equipment* ([3.10](#)) into an *integrated system* ([3.6](#))

3.16
uncontrolled network
shipboard data network other than *controlled network* ([3.2](#))

3.17
version message
message automatically sent by connected equipment containing an indication of the current device software version, including operating system (if operating system is updatable) and configuration (if configuration is an updatable part of the device's software)

Note 1 to entry: An example of one way to provide compliant information from equipment to an SSLS is a data sentence message structure defined as the VER specified in IEC 61162-1 and sent by equipment implementing this standard (encapsulated in 450 protocols with UDP datagrams).

4 Technology design

4.1 Updateable equipment inventory

4.1.1 General

For any given ship, an SSLS shall apply to any on board equipment that contains software which can be updated. An inventory of equipment should have the ability to be automatically generated from connected equipment, or manually entered. Some targeted systems for the SSLS to track include, for example, control and alarm systems; fire and water mist systems; navigation and communication systems; steering control systems; propulsion systems; power generation systems; performance monitoring systems; and auxiliary systems.

4.1.2 Equipment details

Where equipment as listed in 4.1.1 has been identified, the SSLS shall enable an initial log entry containing the following equipment details for each piece of equipment:

a) device type;

b) manufacturer;

c) unique identifier, which is any specific equipment identifier;

d) serial number;

e) manufacture date;

f) model number, which can be a model code set by a manufacturer;

g) date and time of log entry;

h) software version.

> NOTE   This log entry can be setup automatically from the first version message received from connected equipment or entered manually. See description of the VER sentence from IEC 61162-1 for specifics on how several of these details can be captured automatically from a VER sentence.

4.2 SSLS software and hardware requirements

4.2.1 General requirements

The SSLS shall be able to do the following.

— Constantly monitor one or more network connections for version messages from operational equipment.

— Create log entries for any automatically received data messages with new information. Received data messages with no new information need not be logged.

— Prevent editing of any data logged from automatically received data messages.

> NOTE   Correction of errors in automatic entries can be accomplished by copying the details and entering a newer manual log entry with the value that needed to be changed.

— Log data both automatically and manually. Capture and represent the method with which data were logged (automatic or manual) when viewed in the user interface.

— Display a list of equipment and log entries per equipment.

— Display the complete log and allow searching by equipment details in 4.1.2 and log details in 4.2.3.

— Enable storage of service report PDFs or pictures (JPEG or PNG) in association to one or more log entries; if a service report does not result in a software change a log entry duplicating the existing status of the associated equipment should be generated for the service date and associated with the service report.

— Require name of the service provider as in identity of the technician (first name, last name, company) when entering a service report.

— Enable user comments to be entered in association with service reports.

— Automatically and periodically backup the log database to enable recovery in case of failure.

— Require login credentials for users accessing the SSLS.