No. 157 Data assurance

(Sep 2018)

1 Introduction

1.1 The purpose of this document is to supplement the UR E22 with regards to digital data assurance of Category I, II and III computer based system on board, ship to ship and ships to shore systems.

1.2 Objective

1.2.1 Regulation strongly focuses on system hardware and software development, however, data related aspects are poorly covered comparatively. Data available on ships has become very complex and in a large volume, meaning a user is unlikely to spot an error and it would be unreasonable to expect them to do so. Cyber systems depend not only on hardware and software, but also on the data they generate, process, store and transmit. These systems are also becoming more data intensive and data centric, often used as decision support and advisory systems and for remote digital communication.

2 Scope

2.1 Data Assurance may be intended as the activity, or set of activities, aimed at enforcing the security of data generated, processed, transferred and stored in the operation of computer based systems on board ships (as defined in UR E22 par. 1.1 Scope).

Security of data includes confidentiality, integrity and availability; the scope of application of Data Assurance covers data whose lifecycle is entirely within on board computer based system, as well as data exchanged with shore systems connected to the on board networks.

2.2 Data assurance has many stakeholders; they have a level of responsibility which needs to be assigned based on impact and appropriate risk assessment due to potential break in Data assurance:

- Computer based system manufacturer/provider ("Supplier", according to UR E22 2.1.3)
- Computer based system component manufacturer/provider ("Supplier", according to UR E22 2.1.3),
- System Integrator/Shipyard ("System Integrator" according to UR E22 2.1.2),
- Ship Owner / Ship Master ("Owner" according to UR E22 2.1.1)

3 Exclusion

3.1 This document is not intended to be used for data assurance of computer based system, which is not required by Classification Society, such as Information Technology (IT) systems or personal information protection, etc.

4 Data Categories

4.1 Data should be categorized by the supplier or system integrator according to the possible consequences of a breach of data assurance. FIPS 199 (Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems) is a United States Federal Government standard that

No. 157 (Cont)

establishes security categories of information systems and may be helpful in assigning data appropriately.

4.2 Security Objectives are defined as follows:

– CONFIDENTIALITY – a loss of confidentiality is the unauthorized disclosure of information.

– INTEGRITY – a loss of integrity is the unauthorized modification or destruction of information.

– AVAILABILITY – a loss of availability is the disruption of access to, or use of an information system.

4.3 The potential impact of loss of data assurance should be categorized as follows:

– LOW: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on human safety, safety of the vessel and / or threat to the environment.

– MODERATE: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on human safety, safety of the vessel and / or threat to the environment.

– HIGH: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on human safety, safety of the vessel and / or threat to the environment.

4.4 The following table (Table 1) shows how to assign system with categories based on their effects on system confidentiality, integrity and availability.

Table 1 System categories

Category	Effects	System functionality	Confidentiality	Integrity	Availability
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Monitoring function for informational / administrative tasks	Low	Moderate	Low
II	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Alarm and monitoring functions Control functions which are necessary to maintain the ship in its normal operational and habitable conditions	Moderate	High	Moderate

No. 157 (Cont)

III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and / or threat to the environment.	Control functions for maintaining the vessel's propulsion and steering Safety functions	Moderate	High	High

4.4.1 The categorization described above should be used as guidance and definitions should be assessed on a case by case basis.

Note 4.4.a Escalation: systems involving essential services sharing data necessary for their functions might need to have the potential impact escalated to a higher level.

Note 4.4.b Confidentiality level: it is understood the confidentiality level of information might have an immediate business risk.

4.5 Data Types

4.5.1 Data types having safety implications have been identified by The Data Safety Initiative Working Group (DSIWG) of the Safety Critical Systems Club (http://scsc.org.uk/).

4.5.2 A-non-exhaustive table of data types can be found in Appendix 1 of this document.

4.5.3 Data properties are used to establish what aspects of the data (e.g., timeliness, accuracy) need to be guaranteed in order that the system operates in a safe manner.

4.5.3.1 A non-exhaustive table of data properties as identified by DSIWG can be found in Appendix 2 of this document.

4.5.3.2 Any missing property definition of data is potentially a hazard to a system. Not all property values might be necessary for the data however an analysis should be carried out with regard to why it is not necessary.

5 Secured and encrypted data

5.1 An analysis should be carried by the system integrator out to assess the value of data security and its potential impact on system performance.

5.2 The system should be provided with suitable access control measures and other technological and/or procedural measures over computer based systems or means of communication directly interacting with the system.

5.3 As part of Cyber Risk Management, the Owner should also provide appropriate training on risks related to data security to the personnel authorized to interact with cyber systems covered by this recommendation.

5.4 In general where the system has the capability for direct user interaction appropriate authorization and authentication along with diagnostics and logging should be in place.

5.5 The data securing methodology should be fit for purpose using technology currently available for the industry practice.

No. 157 (Cont)

6 Data in physical storage

6.1 Devices used to store data for category I, II or III systems should be appropriate for intended use and suitable for the marine environment, UR E10 refers.

6.2 Data used for category II or III, when stored on hard disk drives, should be stored on multiple hard disk drives to protect data in the case of a drive failure, e.g. RAID storage or equivalent. Spare compatible drives should be available on board.

6.3 Physical devices brought on-board the vessel for the purpose of the updating or upgrading Category I, II or III systems should be free from corruption. There should be a process in place to verify the data integrity before introduction to the ship's systems. (See also paragraph 4.3.8 of IACS Rec. No. 153).

6.4 Evidence should be provided to the Classification Society of the above mentioned measures upon request.

7 Data in networks

7.1 Networks protocols should ensure the integrity of control, alarm, monitoring, communication and safety related data, and provide timely recovery of corrupted or invalid data. Verification of origin and destination of data should be considered as in the scope.

8 References

NIST Special Publication 800-53 (Rev. 4)

IMO MSC96/4/1 *"The Guidelines on Cyber Security On board Ships"*, version 2.0, BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI, 2017

FIPS PUB 199

NIST "*Framework for Improving Critical Infrastructure Cybersecurity"*, version 1.0

Data Safety Guidance version 2.0 by The data safety initiative working group (DSIWG)
ISO 8000-8:2015, "Data quality — Part 8: Information and data quality: Concepts and measuring"

No. 157 (Cont)

APPENDIX 1: Data types

No.	Type	Description	Explanation	Typical containers
Context				
1	Predictive	Data used to model or predict behaviours and performance	Data for studies, models, prototypes, initial risk assessments, etc. This is the data produced during the initial concept phase which subsequently flows into further development phases.	Prototype results, evaluations, analyses
2	Scope, Assumption and Context	Data used to frame the development, operations or provide context	Restrictions, risk criteria, usage scenarios, etc. explaining how the system will be used and any limitations of use.	Concepts of operation, Safety Case Report Part 1
3	Requirements	Data used to specify what the system has to do	Data encompassing requirements, specifications, internal interface or control definitions, data formats, etc.	Formal specifications, interface control documents, user requirements documents, Safety Case Report Part 1
4	Interface	Data used to enable interfaces between this system and other systems: for operations, initialisation or export from the system	Data that exists to enable exchange between this system and other external systems. Covers start-of-life operations (data import or migration), end-of-life operations and ongoing operational exchange of data between systems.	Protocols, schemas, interface control documents, transition plans, Extract-Transform-Load tool specifications, cleansing and filtering rules
5	Reference or Lookup	Data used across multiple systems with generic usage	Data comprising generic reference information sets used by multiple systems (i.e., not produced solely for this system). Typically updated infrequently, and not specification this system.	Dictionaries, materials information, sector data reference sets, encyclopaedias

No. 157 (Cont)

No.	Type	Description	Explanation	Typical containers
Implementation				
6	Design and Development	Data produced during development and implementation	Data encompassing the design and development process artefacts: everything from design models and schemas to document review records. It also includes test documents (specification and results) but not the test data itself.	Design documents, review records, hardware, software, test scripts, code inspection reports, Safety Case Report Part 2
7	Software	Data that is compiled and executed to achieve the desired system behaviour	From some perspectives, it is helpful to consider software (e.g., source code) as another type of data.	Text files, configuration management systems
8	Verification	Data used to test and analyse the system	Data comprising the test values and test data sets used to verify the system. It may include real data, modified real data or synthetic data. It includes data used to drive stubs, and any data file used by simulators or emulators.	Test data sets, stub data, emulator and simulator file
Configuration				
9	Infrastructure	Data used to configure, tailor or instantiate the system itself	Data used to set up and configure the system for a particular installation, product configuration, or network environment.	Network configuration files, initialisation files, hardware pin settings, network addresses, passwords
10	Behavioural	Data used to change the functionality of the system	Data to enable / disable or configure functions or behaviour of the system.	XML configuration file, Comma Separated Variable (CSV) data, schemas
11	Adaptation	Data used to configure to a particular site	Data used to tailor or calibrate a system to a particular physical site or environment, incorporating physical or environmental conditions.	Configuration file

No. 157 (Cont)

No.	Type	Description	Explanation	Typical containers
Capability				
12	Staffing and Training	Data related to staff training, competency, certification and permits	Data which allows staff to perform a function within the wider context of the safety-related system. This may include training records, competency assessments, permits to work, etc.	Human Resources records, training certificates, card systems
The Built System				
13	Asset	Data about the installed or deployed system and its parts, including maintenance data	Data related to location, condition and maintenance requirements of the system under consideration. This may cover hardware, software and data.	Inventory, asset and maintenance database systems
14	Performance	Data collected or produced about the system during trials, pre-operational phases and live operations	Data produced by and about the system during introduction to service and live service itself. Includes fault data and diagnostic data. This may be the results of various phases of introduction and may include trend analysis to look for long-term problems.	Field data, Support calls, bug reports, noncompliance reports, Defect Reporting And Corrective Action System (DRACAS) data
15	Release	Data used to ensure safe operations per release instance	Explanation of particular features or limitations of a release or instance. May include specific time-limited workarounds and caveats for a release.	Release notes, Certificates of Design (CoDs), Transfer documents, Safety Case Report Part 2 or Part 3
16	Instructional	Data used to warn, train or instruct users about the system	Data that explains to users the risks of the systems and gives any mitigations that may be required to be implemented by users, e.g., by process, procedure, workarounds, limitations of use.	Manuals, Standard Operating Procedures (SOPs), on-line help, training courses, Safety Case Report Part 3

No. 157 (Cont)

No.	Type	Description	Explanation	Typical containers
17	Evolution	Data about changes after deployment	Data that covers enhancements, formal changes, workarounds, and maintenance issues. It also covers data produced by Configuration management activities, such as baselines or branch data.	Change requests, modification requests, issue and version data, Configuration management system outputs
18	End of Life	Data about how to stop, remove, replace or dispose of the system	Data covering all activities related to taking the system out of service or mothballing / storage / dormant phases.	Transition, disposal and decommissioning plans
19	Stored	Data stored by the system during operations	Data stored or utilised within the system which has end-user meaning. It may be displayed an used within the system or may be for transfer and distribution to other systems or downstream users. It is data that has some real domain meaning.	May be stored internally within the system (e.g., in databases or text file), or transferred into or out of the system through interfaces (e.g., Ethernet)
20	Dynamic	Data manipulated and processed by the system during operations	Data processed, transformed or produced by the system which has end user meaning. It may be displayed an used within the system or may be for transfer and distribution to other systems or downstream users. It is data that has some real domain meaning.	May be manipulated within the system in data structures or transferred into or out of the system through interfaces
Compliance and Liability				
21	Standards and Regulatory	Data that governs the approaches, processes and procedures used to develop safety systems.	Data predominantly in the form of documents that describe and dictate the activities, processes, competencies etc. to be used for a particular development in a particular sector.	Standards documents, guidelines, legal directives and laws

No. 157 (Cont)

No.	Type	Description	Explanation	Typical containers
22	Justification	Data used to justify the safety position of the system	Data used to justify, explain and make the case for starting or continuing live operations and why they are safe enough. Often passed to external bodies (e.g., regulators, Health and Safety Executive, Independent Safety Auditors) for their review.	Safety Case Report, certification case, regulatory documents, COTS justification file, design justification file
23	Investigation	Data used to support accident or incident investigations (i.e., potential evidence)	Data collected or produced during an incident or accident investigation which may be used in investigation reports, lessons learnt or prosecutions. This can be process data, trace data, site data (e.g., photographs of crash site) or may be derived (accident simulations, analyses, etc.).	Incident/accident investigation reports and supporting documents
Meta-Property				
24	Trustworthiness	(Meta) data which tells us how much the system can be trusted	Data which provides assurance or confidence about the other data within or about the system under consideration. This may be some of the data mentioned in the other types, but may be different.	Data audits, data quality index measures, sign-off sheets traceability records, model database

No. 157 (Cont)

APPENDIX 2: Data properties

Property	Description
Integrity	The data is correct, true and unaltered
Completeness	The data has nothing missing or lost
Consistency	The data adheres to a common world view (e.g., units)
Continuity	The data is continuous and regular without gaps or breaks
Format	The data is represented in a way which is readable by those that need to use it
Accuracy	The data has sufficient detail for its intended use
Resolution	The smallest difference between two adjacent values that can be represented in a data storage, display or transfer system
Traceability	The data can be linked back to its source or derivation
Timeliness	The data is as up to date as required
Verifiability	The data can be checked and its properties demonstrated to be correct
Availability	The data is accessible and usable when an authorized entity demands access
Fidelity / Representation	How well the data maps to the real world entity it is trying to model
Priority	The data is presented / transmitted / made available in the order required
Sequencing	The data is preserved in the order required
Intended Destination/Usage	The data is only sent to those that should have them
Accessibility	The data is visible only to those that should see them
Suppression	The data is intended never to be used again
History	The data has an audit trail of changes
Lifetime	When does the safety-related data expire
Disposability / Deletability	The data can be permanently removed when required

No. 157 (Cont)

Appendix 3

Definitions

Data - representation of information in a formalized manner suitable for communication, interpretation, or processing.

Non-Volatile Memory - include read-only memory, flash memory, magnetic computer storage devices as hard disk drives, floppy disks and magnetic tape.

Volatile Memory - only maintains its data while the device is powered.

RAID - Redundant Array of Independent Disks.

DSIWG - Data Safety Initiative Working Group

End of Document