NR690 DT R00 APRIL 2024

DATA-CENTRIC EVALUATION

NR690 - APRIL 2024

RULE NOTE

BUREAU VERITAS

BUREAU VERITAS
RULES, RULE NOTES AND GUIDANCE NOTES

The PDF electronic version of this document available on the Bureau Veritas Marine & Offshore website https://marine-offshore.bureauveritas.com/ is the official version and shall prevail if there are any inconsistencies between the PDF version and any other available version.

These rules are provided within the scope of the Bureau Veritas Marine & Offshore General Conditions, enclosed at the end of Part A of NR467, Rules for the Classification of Steel Ships. The latest version of these General Conditions is available on the Bureau Veritas Marine & Offshore website.

BUREAU VERITAS MARINE & OFFSHORE

Tour Alto
4 place des Saisons
92400 Courbevoie - France
+33 (0)1 55 24 70 00

marine-offshore.bureauveritas.com/rules-guidelines

NR690

DATA-CENTRIC EVALUATION

Section 1	Data-centric Evaluation
Appendix 1	For Information Only, Guidance for Specific Systems
Appendix 2	For Information Only, Implementation Examples
Appendix 3	For Information Only, Reporting Based on Data-centric Evidence

April 2024

Table of Content

Section 1 Data-centric Evaluation

1 General 4

1.1 Scope
1.2 Classification notation
1.3 Documentation to be submitted
1.4 Definitions
1.5 Approval of DE Service Supplier (DESS)
1.6 Type approval of DE digital solutions

2 General requirements for Data-centric Evaluation 10

2.1 Requirements to EUT
2.2 Configurations
2.3 Class non-compliant configurations and responses
2.4 Test protocols
2.5 Automatic Test Completion (ATC)
2.6 Semi-Automatic Test Completion (SATC)
2.7 Automatic Data-centric Evaluation (ADE)
2.8 Semi-automatic Data-centric Evaluation (SADE)
2.9 DE results
2.10 DE user interface

3 Requirements for Data-centric Evaluation Onboard Digital Solution (DE ODS) 15

3.1 Inputs
3.2 Functions
3.3 Cyber Security

4 Requirements for Data-centric Evaluation Shore Digital Solution (DE SDS) 17

4.1 Functions

5 Reporting process 18

5.1 Parties to the reporting process
5.2 DE workflow
5.3 Non-compliance (NC) follow-up plan

6 Initial Survey 21

6.1 Data-centric Evaluation Onboard Digital Solution (DE ODS)
6.2 Data-centric Evaluation Shore Digital Solution (DE SDS)
6.3 Initial audit of the process

Appendix 1 For Information Only, Guidance for Specific Systems

1 General 22

1.1 Purpose
1.2 Liquefied Natural Gas as Cargo
1.3 Offshore Access System
1.4 Energy Storage Systems
1.5 Unmanned Surface Vessel (USV) Systems
1.6 Dynamic Positioning (DP) Systems
1.7 Process systems on board Offshore Units and Installations
1.8 Electrical installations
1.9 Integrated bridge systems

Appendix 2 For Information Only, Implementation Examples

1 Use Cases 25

1.1

Appendix 3 For Information Only, Reporting Based on Data-centric Evidence

1 Enhanced reporting process 29

1.1 Data-centric evaluation framework
1.2 Reporting safety precursor events
1.3 Defect reporting aligned with contractual clauses

Table of Content

2 Data ownership and access 31

2.1 Data ownership
2.2 Event-based access to the data

Section 1 Data-centric Evaluation

1 General

1.1 Scope

1.1.1 Data-centric Evaluation (DE)

Data-centric Evaluation (DE) is the evaluation of the required functionalities for an equipment or a system by a digital solution with a secure data acquisition.

The scope of the Data-centric Evaluation is limited to:

a) equipment and systems selected by the Owner in accordance with this Rule Note

b) functional capability analysis and functional tests supported by the data acquired regularly.

1.1.2 Exclusions

The scope of the Data-centric Evaluation excludes:

a) tests which depend on temporarily connecting the Equipment Under Test (EUT) to a standalone device designed to introduce faults, unless the standalone device received a certificate of type approval as an element of the EUT

b) any statutory survey in the scope of the IMO Survey Guidelines under the Harmonized System of Survey and Certification (HSSC).

1.2 Classification notation

1.2.1 The additional class notation **DATA-CENTRIC** addresses the digital solutions which are to collect and manage the data for regular Data-centric Evaluation between the periodical surveys carried out for the maintenance of class. Data collection from the ship, evaluation methods and access to the data by the users on board and from shore through dedicated digital interfaces are covered.

1.2.2 The additional class notation **DATA-CENTRIC** may be assigned to a ship or an offshore unit, when the following framework is complied with:

- Two digital solutions are provided as follows and type approved by the Society:
  - Onboard computer based system, further referred to as Data-centric Evaluation Onboard Digital Solution (DE ODS), performing the collection of data necessary for the evaluation of the required functionalities as per [3] on board the ship. The DE ODS is to be available for the onboard users to monitor regularly the status of the test completion and to obtain a relevant decision-support.
  - Shore digital solution, further referred to as Data-centric Evaluation Shore Digital Solution (DE SDS), is to be available for the shore users to manage the test schedule, monitor regularly the evaluation status and to obtain relevant decision-support as per [4].
- Data-centric Evaluation Service Supplier (DESS) is certified by the Society as per [1.5] to manage the tests and to perform the evaluation of the data via DE ODS and DE SDS.
- Reporting process is established between the Owner, the DESS and the Society on the basis of the data collected and evaluated in DE ODS and DE SDS as per [5]. The reporting of the defects is supported by the provision of the relevant data in the DE SDS. The reporting process covers the notifications due from the Owner to the Society in the event of damage which affects or may affect the class of the ship in accordance with NR467, Pt A, Ch 2, Sec 2, [6.2.1] for the scope selected by the Owner. The reporting process may also include other stakeholders at the discretion of the Owner as described in App 3.
- Test protocols are developed by the DESS and approved by the Society for implementation within DE ODS and DE SDS as per [2.4].
- Required functionalities are defined by the DESS in agreement with the information provided by the Original Equipment Manufacturer for the outputs of the data producers.

The evaluation of the required functionalities is to be performed in the DE SDS as indicated in Fig 1 and Fig 2. The corresponding computer based system and shore digital solution are to comply with the requirements of this Section.

Figure 1 : Functional blocks

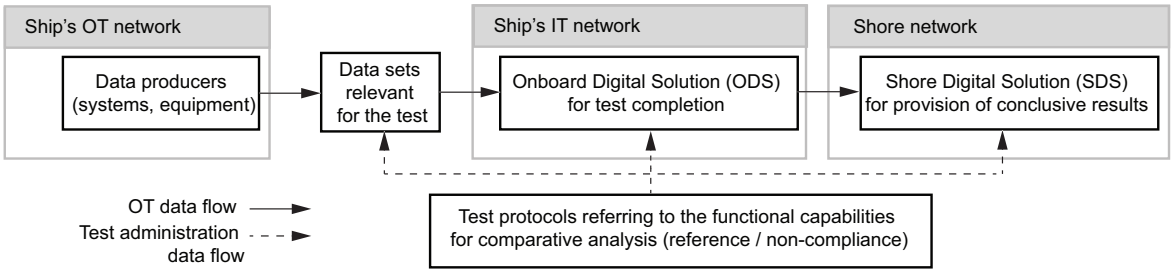
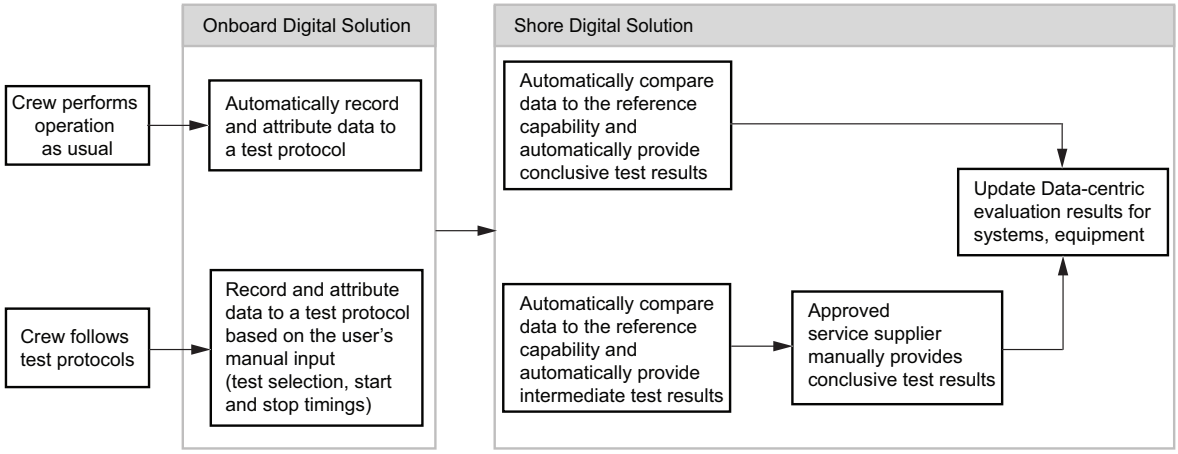


Figure 2 : Interaction between the crew, service supplier, onboard and shore digital solutions



1.2.3 The scope of the additional class notation **DATA-CENTRIC** is to be specified in a memorandum by listing:

a) The equipment and systems selected by the Owner, and the corresponding functionalities selected for the implementation of the Data-centric Evaluation.

b) The references to the requirements of the Society which are used for the compliance checks by DE and which are the basis for Category A non-compliance (NC-A results) as defined in [1.4.6].

c) The reference to the version of the Master Data approved as per [2.4.5].

1.2.4 The DE ODS is to be of a type approved by the Society as per [1.6] and is to comply with the requirements of [3].

1.2.5 The DE SDS is to be of a type approved by the Society as per [1.6] and is to comply with the requirements of [4].

1.2.6 The assignment of the additional class notation **DATA-CENTRIC** is subject to an initial survey detailed in [6].

1.2.7 In accordance with NR467, Pt A, Ch 2, Sec 2, the maintenance of the additional class notation **DATA-CENTRIC** is subject to compliance with the periodical surveys defined in NR467, Pt A, Ch 5, Sec 5.

1.2.8 The ship is to comply with the requirements for assigning one of the notations **CYBER RESILIENT** or **CYBER SECURE** as defined in NR659 "Rules on Cyber Security for the Classification of Marine Units". Additional requirements for cyber security of the DE ODS are given in [3.3].

1.3 Documentation to be submitted

1.3.1 The documentation to be submitted for assigning the additional class notation **DATA-CENTRIC** is listed in Tab 1.

Table 1 : Documentation to be submitted

No.	A/I **(1)**	Description
1	A	Master Data document as per [2.4.5] with the reference capabilities and the non-compliant capabilities
2	A	Templates of DE reports generated to reflect results as described in [2.9.1]
3	I	List of the test and reporting plan to be complied with by the DE ODS and the DE SDS
4	I	Description of the methods used for calculating the DE results
5	A	Description of the data transfer procedures to send the DE data ashore
6	I	List of alerts and notifications generated for onboard and shore users
7	I	Description of the EUT with the functional links to connected systems and equipment, e.g. in a form of FMEA
(1) A = to be submitted for approval; I = to be submitted for information		

No.	A/I **(1)**	Description
8	I	List of computer based systems involved in onboard functions to calculate DE results. For each system, the list is to include: • functional designation • manufacturer.
9	A/I	Documentation as required in NR467, Pt C, Ch 3, Sec 3 for the computer based systems forming the DE ODS
10	A	Table listing the types of user accounts with a description of the corresponding access rights
11	I	Description of the DE SDS architecture with functional diagrams, data flow, process description, location of the hosting servers
12	A	Description of the communication between the DE ODS and the DE SDS including the data transfer procedures and the cyber security measures
13	I	Manual describing the coordinated use of the DE ODS and the DE SDS in the framework of the DE reporting by each type of user
14	I	Service agreement with a DESS approved by the Society
15	I	Type Approval Certificate of the DE ODS and the DE SDS
(1) A = to be submitted for approval; I = to be submitted for information		

1.4 Definitions

1.4.1 For the purpose of this Rule Note, the following definitions are listed in:

- [1.4.2] for network components
- [1.4.3] for testing types
- [1.4.4] for Data-centric Evaluation functions (DE functions)
- [1.4.5] for measured, derived and reference values
- [1.4.6] for Data-centric Evaluation results.

1.4.2 Network components

- Connected Unit: equipment or system interfaced or functionally related with the EUT and which provides a response correlated to the response of the EUT.
- Data producers: sources of data for DE ODS which are located in the OT segment of the onboard network, including EUT, Connected Unit, system providing the global function, units redundant to EUT as in Fig 9.
- Demilitarized zone (DMZ): a physical or logical perimeter network segment that contains and exposes an organization's external-facing services to an external network. Its purpose is to enforce the internal network's security policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.
- Digital solution: computer based system that incorporates functions for collection, transmission, analysis and visualisation of data, as well as the relevant calculations.
- Equipment Under Test (EUT): equipment or system subject to evaluation.
- Information Technology (IT): equipment, software and associated networking focusing on the use of data as information, as opposed to Operational Technology (OT).
- Inspection and Decontamination Gate (IDG): anti-malware digital solution which is to detect malicious signatures, suspicious behaviour and network intrusion.
- Operational Technology (OT): equipment, sensors, software and associated networking that monitor and control onboard systems. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes.
- Unidirectional link: network security equipment which provides a one-way communication and disables any reverse traffic by the use of an analog isolation, e.g. network diode. Secure SHell (SSH) and File Transfer Protocol (FTP) protocols cannot be considered as unidirectional links.

1.4.3 Testing types

- Test: assessment method that is characterized by the process of observing objects under specified conditions to compare actual with expected behaviour for the purpose of the data-centric evaluation. It may be limited to the monitoring of the object without a human intervention.
- Test protocol: a test procedure documented as per [2.4].
- Detection test: functional test of alarms, warnings and other indications which inform operator about a degraded state of the EUT; checking that all single failures critical for EUT are clearly indicated to an operator at the dedicated workstation without creating a potential hidden failure.

- Performance test: checking performance of the EUT by:
  - functional testing
  - capability and operational limit assessment (e.g. checking full load or output capability)
  - checking resolution and accuracy.
- Protection test: functional test of protective arrangements:
  - upon which the redundancy of configuration depends, e.g. Advanced Generator Protection (AGP)
  - which maintain the EUT within the safe operational limits, e.g. blackout prevention in Power Management System (PMS).
- Redundancy test: checking redundancy of a EUT's configuration in the event of a single point failure following which the global function of the EUT is to be maintained without any operator intervention; validating segregation of redundant groups by confirming that failures do not propagate beyond the perimeter of a redundant group in which the single point failure is introduced.

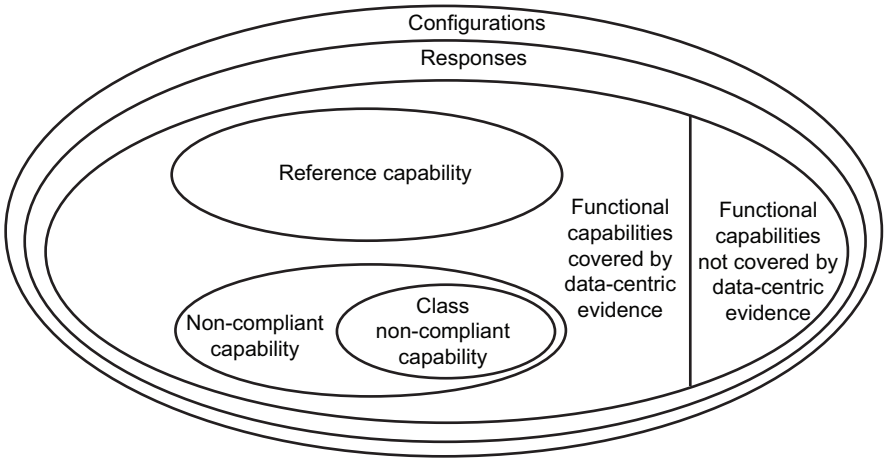
1.4.4 Data-centric Evaluation functions (DE functions)

- Automatic Data-centric Evaluation (ADE): algorithm-based evaluation based on the data-centric evidence obtained from the operation of the equipment or system without a need for the human operator's intervention to evaluate compliance to the reference capability.
- Automatic Test Completion (ATC): an acquisition of a complete set of the data-centric evidence without a need for the human operator's intervention to initiate the functional responses as per the approved test protocols.
- Data-centric Evaluation (DE): evaluation of the required functionalities for an equipment or a system by a digital solution with a secure data acquisition. The evaluation can be automatic (ADE) and semi-automatic (SADE).
- Semi-Automatic Data-centric Evaluation (SADE): algorithm-based evaluation based on the data-centric evidence obtained from the operation of the equipment or system with a need for the human operator's intervention to evaluate compliance to the reference capability.
- Semi-Automatic Test Completion (SATC): an acquisition of a complete set of the data-centric evidence with a need for the human operator's intervention to initiate the functional responses as per the approved test protocols.

1.4.5 Measured, derived and reference values

A Venn diagram providing the relations between measured, derived and reference values is shown in Fig 3.

Figure 3 : Venn diagram for the functional capabilities and configurations



In addition, the following definitions are used for describing measured, derived and reference values:

- Data-centric evidence: data generated by equipment or system, which corroborates the technical evaluation. The data is to be provided in a form of time series and/or event data, which may be complemented by manual electronic log entries.
- Event data: collection of time-stamped messages produced by a monitoring function of a system, e.g. alarms, alerts, notifications.
- Time series: time-stamped states of a system indexed in time order.
- Regular expressions: string of characters that allows patterns to be used to match search results for event data.

Note 1: As defined in ISO/IEC/IEEE 26531:2023 Systems and software engineering - Content management for product life cycle, user and service management information for users.

- Geofencing: determination of the ship's presence within a predefined geographic area.
- Configuration: a setup of equipment or system including all states with an impact on its global function, e.g. parameters and alarms. The setup(s) can be provided in a tabulated format at system and subsystem levels with a specific operating mode and status identified for each element. Configuration may include the parameters which cannot be acquired as a data-centric evidence. Two configurations are used to characterise a response. The equipment or system can be in only one of a finite number of configurations at any given moment. An example of a tabulated configuration is given in Tab 2.

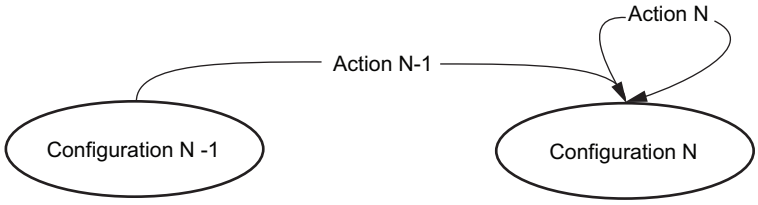
- Action: an input to the equipment or system. A test action is an action as per a test protocol aimed at producing a specific response.

Note 2: For ATC, actions may include running in a certain load range, variation of an operational parameter within specific limits, etc. For SATC, actions may include intentional triggering of alarm systems, shutting down elements, etc.

- Response: response of equipment or system to the test actions and/or exposure to the operating conditions in a form of a transition between two configuration as in Fig 4. A response may include a parameter change or an event message generated. A response may include the change of parameters which cannot be acquired as a data-centric evidence.

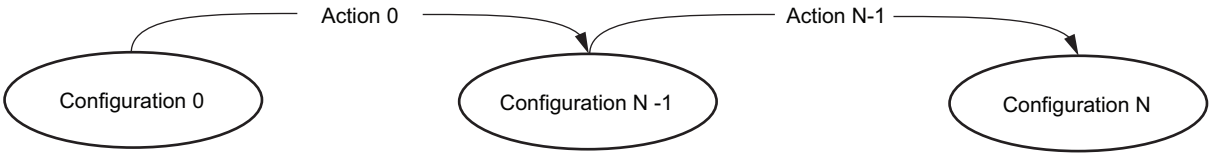
Note 3: A response may be a transition between two identical configurations, i.e. an action may result in equipment or system not demonstrating any change in the configuration, as in the example on Fig 4 after the Action N.

Figure 4 : Response



- Functional capability (functionality): capability of the equipment or system to provide responses to the test actions and/or exposure to the operating conditions. A functional capability is characterised by a set of responses as in Fig 5.

Figure 5 : Functional capability



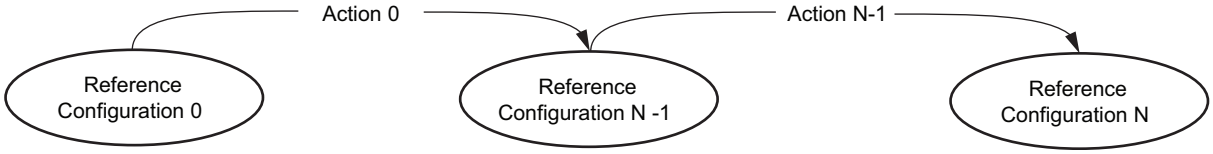
- Functional capability analysis: analysis of the functional capabilities by means of anomaly detection and diagnostics. The analysis can be based on continuous and intermittent monitoring and testing.

Note 4: Anomaly detection and diagnostics are defined in ISO 13372:2012 Condition monitoring and diagnostics of machines - Vocabulary.

- Reference capability: mapping to functional capabilities from a set of the Rules of the Society, ship's contractual requirements and Owner's internal procedures.

  The description of the reference capabilities are to be provided by the DESS and submitted for information to the Society. All configurations within a reference capability are to be acquirable as a data-centric evidence. Reference capabilities are a subset of the functional capabilities and do not contain any non-compliant configurations or responses as in Fig 6.

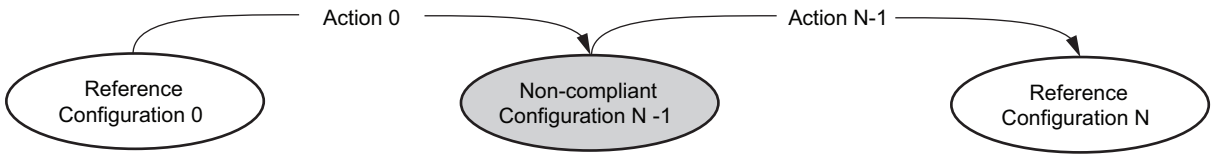
Figure 6 : Reference capability



- Non-compliant capability: mapping to functional capabilities from a set:
  - of conditions indicative of danger to humans, ships, the environment, or
  - of a non-compliance to requirements of the Society, ship's contractual requirements and Owner's internal procedures.

  The description of the non-compliant capabilities are to be provided by the DESS and submitted for information to the Society as a part of the Master Data defined in [2.4.5]. All configurations within a non-compliant capability are to be acquirable as a data-centric evidence. Non-compliant capabilities are a subset of the functional capabilities, and contain at least one non-compliant configuration or response as in Fig 7.

Figure 7 : Non-compliant capability



- Class non-compliant capability: mapping to functional capabilities from a set of conditions indicative of a non-compliance to the requirements of the Society.

  Class non-compliant capabilities are a subset of the functional capabilities, and contain at least one class non-compliant configuration or response as in Fig 8.

Figure 8 : Class non-compliant capability

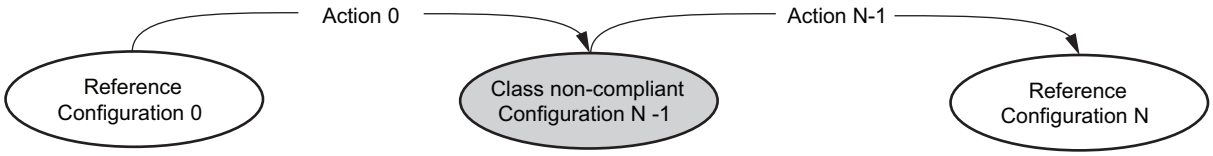


Table 2 : Example of a configuration, extract from a setup of LNG cargo system for ESD test

No.	Components and functional elements	Status
1	ESD valves	Open
2	ESD system power supply	Available
3	Intergrated Automation System's PLCs in the field stations of the LNG cargo system	Online
4	Fiber optic link	Connected
5	Pneumatic link	Connected
6	Pneumatic link's air pressure	Above the trip setting
7	Power plant 440V MSB Bus B to 440V ESB E Breakers	Closed
8	ESD system mode	Port mode
9	Hydraulic oil pressure low low alarm	Not present
10	ESB and Bus B blackout alarms	Not present
11	Cargo pumps	Online

1.4.6 DE results

DE result includes the conclusive status of a completed test and the associated data-centric evidence per each test step. The following definitions are used for describing the status of DE results:

- Satisfactory: the functional capability corresponds to the reference capability.
- Category A non-compliance (NC-A): the functional capability does not correspond to the reference capability and includes Class non-compliant configurations, e.g. loss of the steering control loop of a thruster.
- Category B non-compliance (NC-B): the functional capability does not correspond to the reference capability and includes non-compliant system configurations and responses related to the non-critical faults and warnings, with the exception of those covered by the NC-A, e.g. evidence of not following the OEMs recommendation for the warming up in a generator start-up sequence, early signs of degradation which have not yet compromised the functional capability.
- Test pending (TP): the test protocol has not been followed to obtain the results, e.g. test actions with the prescribed duration have not been completed yet or deviated from the test protocol.

1.5 Approval of DE Service Supplier (DESS)

1.5.1 A Data-centric Evaluation Service Supplier (DESS) is defined as a company approved by the Society, which at the request of an Owner acts in relation to an onboard system or connected equipment and provides services for a ship or a offshore unit. The services may include data-centric evaluation, decision support, operational monitoring, data storage and processing. The results of the services are used by the Owner and the parties to the process described in Article [5].

Note 1: For details about the approval of the DESS, see NR533 Approval of Service Suppliers.

1.5.2 The company operating the DE ODS and DE SDS, and involved in the process described in the Article [5], is to be approved as DESS as per the applicable requirements given in Rule Note NR533 Approval of Service Suppliers.

The DESS can be approved as:

a) Original Equipment Manufacturers (OEM) of the equipment subject to DE, or

b) a service supplier independent from OEM at the discretion of the Society on a case-by-case basis.

If the DESS is not the OEM, the DESS is to provide one of the following:

1) submit a written agreement of the OEM for the DESS to perform the Data-centric Evaluation (DE) for the concerned EUT as defined in [1.4.4],

2) demonstrate that the results of DE are consistent with the available information from the OEM or other standard recognised by the Society. This is to be demonstrated through limiting the NC-A results of DE to the timeseries and event data which are described as non-compliant capabilities in the available manuals from OEMs or in the recognised standards. The versions of the corresponding manuals or standards are to be indicated in the Master Data described in [2.2.2].

1.6 Type approval of DE digital solutions

1.6.1 The design, construction, commissioning and maintenance of DE ODS is to be in accordance to the requirements of NR467, Pt C, Ch 3, Sec 3 and are to comply at least to the requirements for Category I systems.

1.6.2 Hardware components forming a part of the DE ODS are to be type approved in accordance to NR467, Pt C, Ch 2, Sec 15, [2].

Note 1: Only the hardware installed on board the ship is considered in the scope of the present Rule Note.

1.6.3 The DE ODS is to be type approved as per the requirements for cyber security given in [3.3].

1.6.4 The DE ODS and the DE SDS are to be type approved in accordance with the Society's type approval scheme described in NR320, which consists of the following steps (Tab 3):

- documentation review
- type test of the hardware of DE ODS
- type test of software functionalities for deployment on board and on shore
- issuance of Type Approval Certificate.

Table 3 : Applicability of the requirement to provide the type approved components

Digital solution	Type approved components are required	
	Hardware	Software
DE ODS	Yes	Yes
DE SDS	No	Yes

1.6.5 When the DE ODS and the DE SDS require a specific software configuration or the definition of installation parameters, they are to be identified and listed with indication of their values or settings in the documentation submitted to the Society.

1.6.6 The Type Approval of the DE ODS and the DE SDS is to reference the requirements (e.g. Rules of the Society) used for the evaluation.

1.6.7 On a case-by-case basis. hardware and software may be approved by the Society, subject to:

- submission of adequate documentation, and
- satisfactory outcome of any required test, at the request of the Society.

2 General requirements for Data-centric Evaluation

2.1 Requirements to EUT

2.1.1 Built-in test functionalities forming a part of EUT are not covered by the requirements of this Section. Such functionalities are to be checked as a part of the type approval of the EUT or as a part of the applicable class or statutory survey.

2.1.2 The data producers are to be connected to the data infrastructure to transfer the data to the DE ODS. If the data producers are provided with a fallback consisting of the means of logging and log extraction to external portable devices, the extracted data is to be encrypted.

Note 1: The data infrastructure and the ship-shore communication system may be compliant with the applicable requirements related to the assignment of the additional class notations **ASYNC-COM** and **DATA-INFRA**, given respectively in NR467, Pt F, Ch 4, Sec 3 and Sec 4.

2.1.3 If the tests depend on temporarily connecting the EUT to the standalone device designed to introduce faults through wired interfaces, and the standalone device received a certificate of type approval as an element of the EUT, the standalone device is to comply with the following requirements:

a) any fault in the test device is not to be able to propagate to the EUT

b) verifiable means are to be in place to ensure that the test device is removed from circuit when the test is not being performed

c) galvanic isolation is to be provided for the wired interfaces between the EUT and the test device.

2.2 Configurations

2.2.1 For each test step of a test protocol, the configurations and responses are to be identified as per Fig 9:

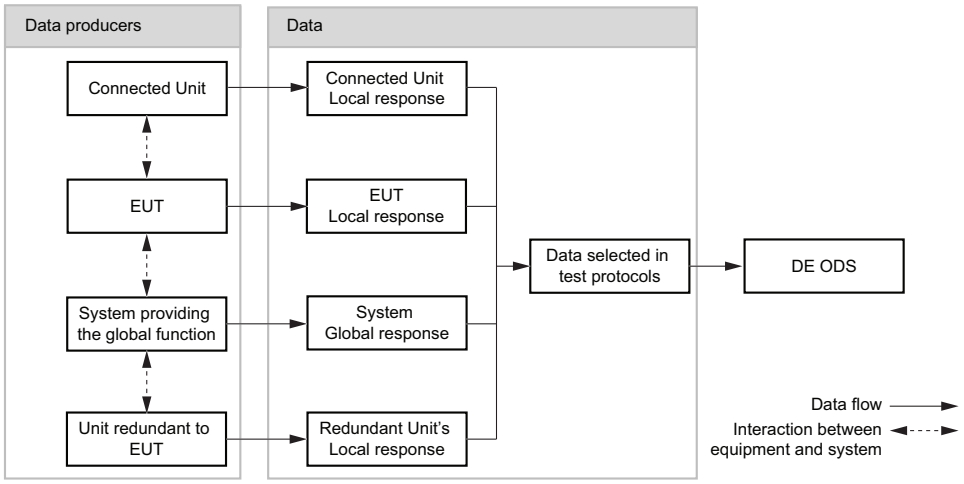
a) locally for EUT

b) globally for the system providing the global function to which EUT contributes

c) locally for the Connected Units

d) locally for units redundant to EUT, if redundancy testing is to be performed.

Figure 9 : Data flow to DE ODS from the data producers



2.2.2 The configurations are to be documented as a list of the timeseries and event data for which the following is to be identified:

- corresponding range of the values
- if a sliding window is used in DE ODS, the size of the sliding window, weighting parameters
- if a filter is used in DE ODS, the type of the filter and its parametrisation
- unique ID of the data producer on the ship
- attribution to the data producer categories as in Fig 9: EUT, connected unit, system with a global function supported by EUT
- if a redundant design is applicable, attribution to redundant groups with unique ID
- sampling rate for the timeseries
- data type, e.g. integer, float, string
- attribution to the input type category (timeseries and event data)
- units of measurement, if applicable, e.g. rpm
- for logical timeseries, an explicit wording of the logical check, results of which are represented by the timeseries, e.g. “is the pump running?”
- regular expressions for filtering the pertinent event data
- for coded timeseries, a definition of the codes, e.g. bitcoded operational modes “2 - in autopilot”, “16 - in automatic positioning”
- if geofencing is used, the acceptable georeferenced zone ID
- if specific logged activities are to be simultaneous, the reference to the activity type and the electronic log
- reference to the documents defining the requirement applicable to the functionality (Applicable Rules of the Society, OEM’s manuals, Owner’s procedures, Charterer’s requirements, etc.).

2.2.3 Configurations are to be presented in a tabulated format grouped by ship’s systems and subsystems with detailed descriptions of the parameters and status of breaker, valves, settings, modes selected. A rationale for the initial configurations is to be provided in a form of a comment in a dedicated column.

2.2.4 The final reference configuration in a test is not to present a danger to humans, ships, the environment and is not to disrupt the functioning of the essential onboard systems.

2.3 Class non-compliant configurations and responses

2.3.1 At least one class non-compliant capability is to be identifiable. Detecting it within the data-centric evidence is to trigger reporting of a NC-A finding.

2.4 Test protocols

2.4.1 Test protocols consist of test steps. A test step is a time bound response subject to a test action.

Note 1: It is recommended to build the test protocols as a proving method for the EUT’s FMEA conclusions on protection, detection, redundancy and performance.

2.4.2 In SATC, a single test action by an operator is to be prescribed for each test step.

2.4.3 Test protocols are to be used to guide the process of testing and to record the test results. Test protocols are to document the performance, protection, detection and redundancy test by identifying:

a) test ID and a short name

b) version of the test protocol

c) EUT

d) purpose of the test

e) initial configuration

f) references to relevant drawings, user manuals

g) applicable types of testing: protection, detection, redundancy, performance

h) references to relevant parts of FMEA and FMECA, if applicable

i) minimum required means of the visual representation of the responses in the DE SDS interface, e.g. trend views for predefined groups of timeseries, widgets such as gauges and mimics similar to onboard EUT's interfaces.

2.4.4 Each test step is to include:

a) A clear description of the test method with the exact action required to be performed including, where applicable, the identification of the breakers, valves, functions to be operated, disconnected, shut down, activated, etc. The equipment cabinet and compartment names are to be included, where an action applied locally to a hardware element by an operator is required.

b) Minimum and maximum duration of the test action or of the test step is to be specified.

c) Reference configuration at the end of the test step including event data generated and parameter values.

d) Configuration not covered by data-centric evidence at the end of the test step including status such as shut down, fail-as-set, fail-to-open, fail-to-close, fail-to-zero, fail-to-full thrust.

2.4.5 Master Data document is to be issued to store the collection of the test protocols and to describe the minimum required data. Master Data is to be provided in a form of a human-readable database with a structure allowing to pull the following information with the corresponding metadata:

a) test protocols with metadata listed in [2.4.3]

b) test steps with the corresponding test protocols' IDs with metadata listed in [2.4.4]

c) reference configurations provided as per [2.2.2] with the corresponding test steps' IDs

d) timeseries with the corresponding reference and non-compliant configuration ID

e) event data regular expressions with the corresponding reference and non-compliant configuration ID

f) initial configurations provided as per [2.2.2] with the corresponding test protocols' IDs

g) class non-compliant configurations provided as per [2.2.2] with the corresponding test protocols' IDs and required to generate NC-A results

h) non-compliant configurations provided as per [2.2.2] with the corresponding test protocols' IDs and required to generate NC-B results

i) unique timeseries

j) unique event data regular expressions

k) version history of the Master Data with a modification tracking list.

2.4.6 Each test is to include the checking of

- connectivity status between the DE ODS and the data producers at the beginning of data acquisition
- data integrity status by validating the range, type and format during the data acquisition
- uptime statistics for the timeseries at the end of data acquisition.

2.5 Automatic Test Completion (ATC)

2.5.1 Automatic Test Completion (ATC) is to be performed as per the Fig 10. Means of automatically detecting the compliant reference configurations are to be provided to generate the timestamped records for the start and for the end of the ATC session.

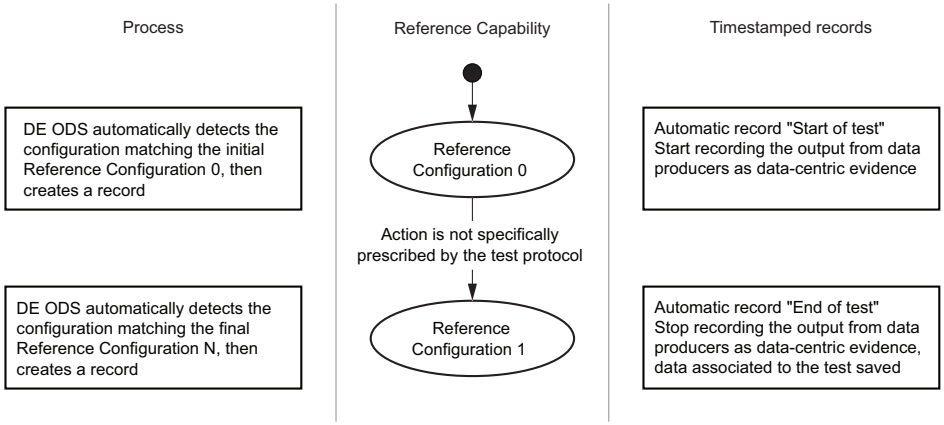
Note 1: ATC is generally intended to form a part of the performance tests.

2.5.2 If the EUT's response is not fully produced during the ATC session in the maximum time specified as per [2.4.4], the ATC session is to be automatically closed and a record of the DE result is to be created of the test being suspended.

2.5.3 ATC sessions are to include not more than a single test step. Multiple ATC sessions may run simultaneously.

2.5.4 The ATC is to be able to run on the historical data and in real-time.

Figure 10 : ATC session



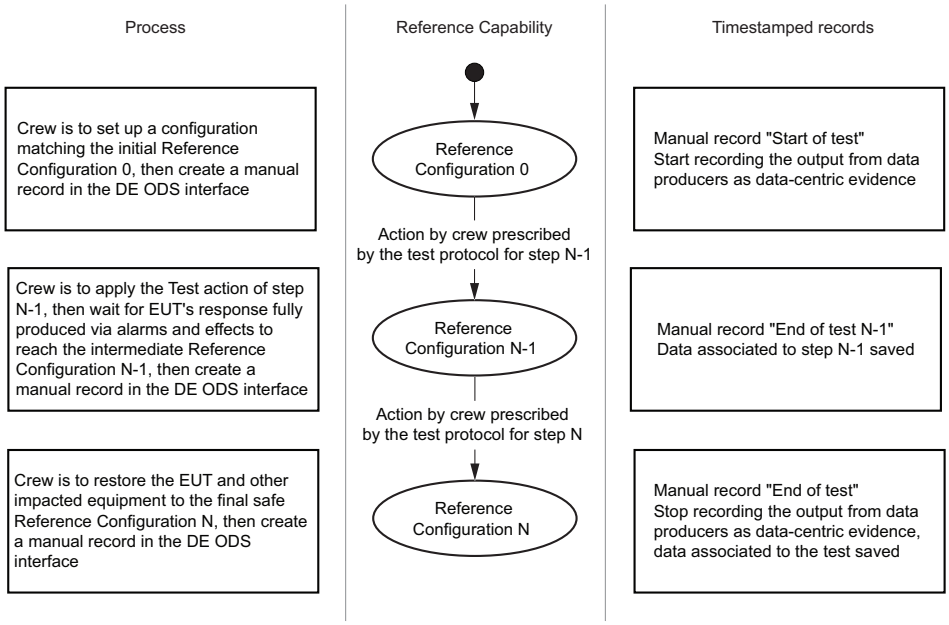
2.6 Semi-Automatic Test Completion (SATC)

2.6.1 The Semi-Automatic Test Completion (SATC) is to be performed as per the Fig 11. Means of manually creating the timestamped records for the start and for the end of the SATC session are to be provided.

2.6.2 SATC sessions may include more than a single test step. Not more than a single SATC session is to run at a time to avoid interference between the independent sessions and to avoid introducing a biasing into the data-centric evidence.

2.6.3 The SATC is to be able to run on the historical data and in real-time.

Figure 11 : SATC session



2.7 Automatic Data-centric Evaluation (ADE)

2.7.1 ADE is to use the Master Data to provide an automatic validation of the test data recorded by ATC or SATC. ADE is to compare the test data to the reference configurations and responses and to provide one of the resultant values listed in [2.9.1].

2.7.2 If a class non-compliant configuration is detected, the ADE is to provide a result corresponding to NC-A category.

2.7.3 If all observed configurations and responses correspond to the reference capability, the ADE is to provide a result corresponding to Satisfactory outcome.

2.7.4 ADE is to be deterministic in comparing the EUT's configurations and responses to the reference capability, when TP or NC-A results are produced. ADE may not be deterministic, when Satisfactory or NC-B results are produced.

2.8 Semi-automatic Data-centric Evaluation (SADE)

2.8.1 SADE is to use the Master Data to provide a decision support to a DESS operator who is to validate the test data recorded by ATC or SATC. The decision support is to compare the data-centric evidence to the reference capabilities and to provide the DESS operator with one of the resultant values listed in [2.9.1].

2.8.2 The decision support is to include the automatic creation of time stamps for the estimated test action, e.g. by means of a change point detection algorithm.

2.8.3 If the test protocol includes multiple steps, the SADE is to provide the intermediate result validation for the individual test steps.

2.8.4 The DESS operator is to provide the validated result equivalent to one of the listed in [2.9.1].

2.9 DE results

2.9.1 DE results are to provided for each test as per the groups below as per the definitions in [1.4.6]:

a) Satisfactory

b) Category A non-compliance (NC-A)

c) Category B non-compliance (NC-B)

d) Test pending (TP).

2.9.2 NC-A results are to be acknowledged by the Owner in the DE SDS.

2.10 DE user interface

2.10.1 User interface is to include a visual representation for all data-centric evidences as given in the Master Data unique item lists (unique timeseries and unique event regular expressions).

2.10.2 User interface is to include trending of timeseries with vertical lines indicating:

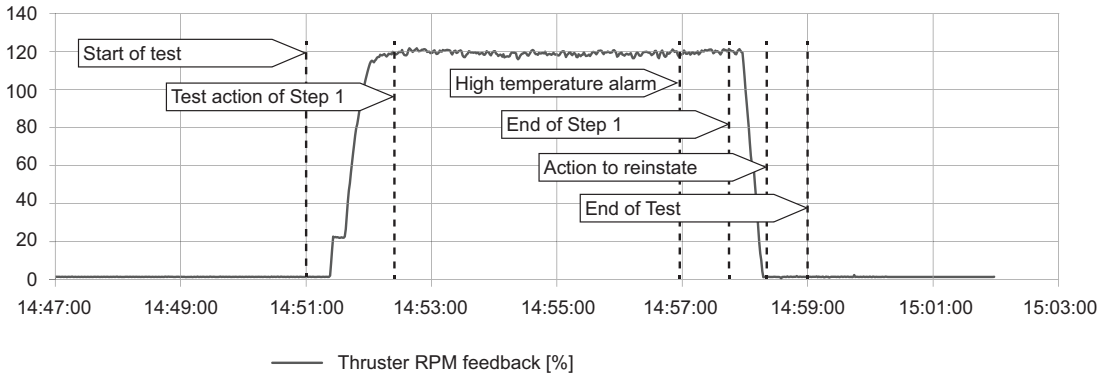
a) timestamped records of the SATC and ATC

b) selected event data (alarms, warnings, notifications).

An example of the visualisation is provided in Fig 12.

2.10.3 Visual representation is to include mimics based on a simplification of the onboard control and/or monitoring system's human machine interfaces where the IDs are indicated for EUT, connected units and systems providing the global function to which the EUT contributes.

Figure 12 : Trending of timeseries with vertical lines for timestamped records and event data



2.10.4 Where the data-centric evidence is provided for more than ten interconnected or dependent pieces of equipment or systems, the DE user interface is to include their graph representation. The graph nodes are to present the data producers, timeseries and event data, the graph edges are to present the existing interconnectivity (power supply, Ethernet communication, etc.) and dependencies.

Note 1: The graph representation is a simplification of the electrotechnical diagrams used in conjunction with IEC 60617:2012 Graphical symbols for diagrams. The simplified presentation is expected to be derived from the applicable diagrams including, but not limited to, single-line, circuit, connection and network diagrams.

2.10.5 The mimics are to be provided with a historical playback function permitting to view the evolution of parameters at a selected time span. The playback is to have a speed modifiable by the user.

2.10.6 The user interface is to include a visual representation of the comparison between the configuration measured and the reference configuration for the initial, intermediate and the final stage of the test. DE results are to be provided for each reference timeseries and event data. An example of the user interface for the ATC and SATC session result and the DE result presentation is given in Fig 13.

Figure 13 : DE interface for comparing with the reference capability - Example for a performance testing of a diesel generator

Data producer	Type	Timeseries/Event data	Reference state Initial	Measured	Reference state Step N-1 Intermediate	Measured	Reference state Final	Measured	DE result
Diesel Generator 1 Active Power	EUT	DG_SFI_CODE_KW	<1360	343	1300-1360	1330	<1360	656	Satisfactory
Diesel Generator 1 Frequency	EUT	DG_SFI_CODE_Hz	57-63	60	57-63	60	57-63	60	Satisfactory
DG NDE Bearing Temperature	EUT	DG_SFI_CODE_NDE_TT	<145	60	<145	150	<145	135	NC-B
IAS	System supported by EUT	Blackout prevention - Automatic load reduction	0	0	0-1	1	0	0	Satisfactory
Diesel Generator 1 Circuit Breaker	Connected unit	DG_SFI_CODE_In Closed	1	1	1	1	1	1	Satisfactory

3 Requirements for Data-centric Evaluation Onboard Digital Solution (DE ODS)

3.1 Inputs

3.1.1 ATC and SATC are to be provided with a maintenance mode where the functionality for generating the data-centric evidence from ATC and SATC can be checked on predefined synthetic datasets.

3.1.2 Means of monitoring and recording the following data are to be available on board with inputs to the DE ODS:

a) time series and event data as per the items listed for all reference configurations

b) UTC time

c) ship's geographic position.

3.1.3 If DE ODS collects data through SATC, means of a manual entry for the following data are to be provided:

a) start of a specific test

b) end or suspension of a test

c) end of a specific test step

d) names and ranks of the users performing the test

e) comments from the user.

3.2 Functions

3.2.1 The DE ODS is to collect the data-centric evidence by means of at least one of the options below:

a) Automatic Test Completion (ATC)

b) Semi-Automatic Test Completion (SATC)

Examples of use cases are listed in the App 1 and App 2.

Note 1: For example:

- the ATC may include:
  - a regular acquisition of the alarms generated by an integrated bridge system during a time span of 24 hours; or
  - a regular acquisition of the electric distribution system's configuration while the ship operates in an offshore safety zone of a windpark; or
  - a regular acquisition of the offshore access system critical alarms for HPU (Hydraulic Pumping Unit), PLC (Programmable Logic Controller), valves, actuators and position sensor when the control mode for the automatic motion compensation is activated;
  - a regular acquisition on a time span of 24 hours of the level and pressure alarms generated by an integrated automation system (IAS) on a LNG carrier during a sea transit when the sea transit mode is manually activated in IAS; or
  - acquisition of the component responses subject to a manual Emergency Shutdown Test on an LNG cargo system.
- the SATC may include:
  - diagnostics of engine malfunctions based on a long-term performance dataset analysis; or
  - algorithms developed for ATC are being tested with a human-in-the-loop.

3.2.2 The sequences in ATC and SATC are to be based on the approved test protocols as per [2.4].

3.2.3 The DE ODS is to provide the uptime statistics for the timeseries listed in the Master Data document.

3.2.4 A user interface for the monitoring of the ATC according to [2.5] is to be provided.

3.2.5 A user interface for the control of the SATC according to [2.6] is to be provided.

3.2.6 The DE ODS is to provide the following dashboards and reports:

a) a dashboard with the status of the test completion as per the schedule

b) a report for the summary of the test results

c) a dashboard for the failed tests and the corresponding EUT component

d) a report of the pending actions as per the Article [5].

3.2.7 The DE ODS is to provide the following functions:

a) indicate the last date and UTC time of synchronisation with the database of the DE SDS and maintain a log of such synchronisations

b) export data to non-encrypted delimited text file in an easily readable format.

c) store a minimum of 30 days of the data-centric evidence

d) generate notifications for missing the scheduled test completion date

e) generate notifications for failing the DE.

3.2.8 When the ADE is performed on board, the DE ODS is to indicate a discrepancy with the ADE results on shore, if detected.

3.2.9 The DE ODS is to be able to import, export and view the Master Data entries.

3.2.10 The DE ODS is to be configured to the ship specific parameters, which are to be accessible in a single aggregated presentation in the digital user interface.

3.2.11 Access to the DE ODS is to be password protected and all users are to be identified, as a minimum with their names and their roles, when logged in. Each modification of the manual records is to be digitally signed when completed by an authorized signature.

3.2.12 Means of encrypted data exchange with the DE SDS are to be provided. The exchanges are to be automated and completed at least every 5 days with a notification provided to the user in the event of not performing the exchange in a due time.

3.2.13 The DE ODS is to support a completion of multiple attempts for a test during the permitted period set by the DESS, unless the test protocol requires a dataset for the full duration of the period, e.g. daily ATC on the basis of 24 hour datasets (see App 2, Tab 1).

3.2.14 The DE ODS is to log every test completion (ATC and SATC) with a unique sequence ID and a hash value.

Note 1: The hash values are the output of hash-functions defined in ISO/IEC 10118-1:2016 Information technology — Security techniques — Hash-functions — Part 1: General.

3.3 Cyber Security

3.3.1 The DE ODS software is to be of a type approved by the Society according to NR659 Chapter 5.

3.3.2 The data exchanges between the DE ODS and the DE SDS are to be secured with the means of checking the message integrity, e.g. the data is hashed, the hash value is sent with the message and validated at the recipient to check if the data exchange has been tampered with.

3.3.3 If data producers, DE ODS and DE SDS are permanently connected, they may communicate through the arrangements compliant with the requirements of NR659, Ch 4, Sec 4. With the example on Fig 14, this includes a provision of:

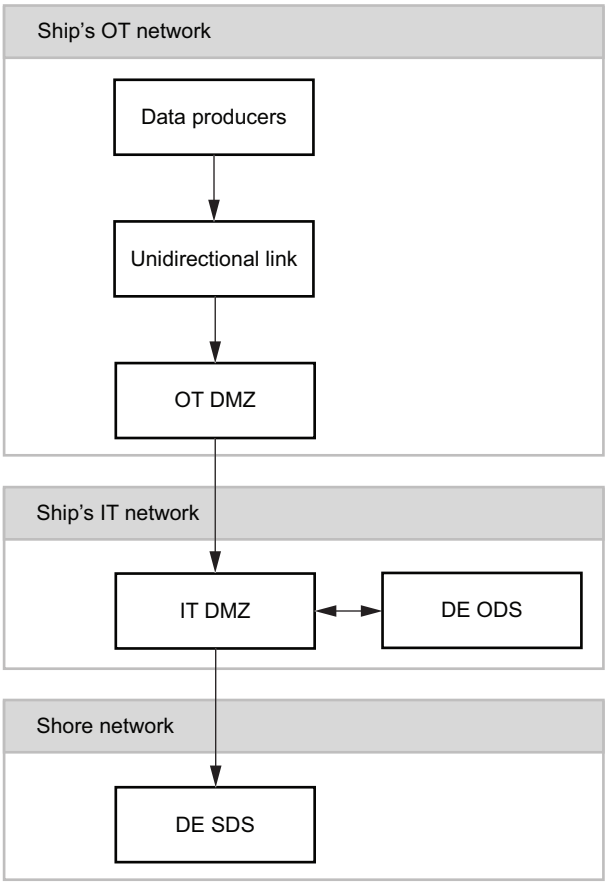
a) unidirectional link from the data producers to OT DMZ

b) DE ODS connected to OT DMZ via IT DMZ

c) IT DMZ between DE ODS and DE SDS.

3.3.4 As a temporary fallback measure in the event of a failure of the connectivity, the data producers, DE ODS and DE SDS may use the portable media for the exchange of the data provided that a decontamination process is established via the IDG capture points. IDG solutions are to be Type Approved as per NR659 Chapter 5.

Figure 14 : Connections between EUT, DE ODS and DE SDS



4 Requirements for Data-centric Evaluation Shore Digital Solution (DE SDS)

4.1 Functions

4.1.1 Means of automatic encrypted data exchange with the DE ODS are to be provided.

4.1.2 Means of access to the DE report in a form of tabulated summaries and trends are to be provided for the users, which are to include the representatives of the Owner, the DESS, the Society, the Flag Administration, Regional Authorities and the Charterer when applicable. The means of access for the OEM are to be provided, if the OEM is different from the DESS.

4.1.3 For the users groups described in [4.1.2], the access hierarchy is to be provided in the following order:

a) Owner as a top user

b) DESS

c) OEM, if the OEM is different from the DESS

d) the Society

e) Flag Administration, Regional Authorities

f) Charterer.

4.1.4 The DE SDS functions are to include:

a) items available for the DE ODS as described in [3.2.6], [3.2.7], [3.2.10]

b) view the log of the test completions described in [3.2.14]

c) support for the reporting process described in [5]

d) granting a full or a partial access to the data as per the access hierarchy

e) for the Owner as a top user, acknowledging non-compliance notifications

f) for DESS, test scheduling for DE ODS

g) storing a minimum of 5 years of the DE results with underlying data-centric evidence

h) provide comparison of the present functional capability to the historical data

i) calculate the difference between the selected actual EUT's configuration and the corresponding reference configuration.

4.1.5 When the calculation of the ADE results as per [2.9.1] is performed by the DE ODS and by the DE SDS, the DE SDS is to provide the following functions in addition to [4.1.5]:

a) the ADE results presented by the DE SDS are to indicate whether each calculation was done by the DE ODS or by the DE SDS

b) provide alerts to the top user in the access hierarchy, in case any discrepancy is detected between the ADE results calculated by the DE ODS and by the DE SDS.

4.1.6 Access to the DE SDS is to be password protected and any user is to be identified with a name, unique ID, role and the name of the organisation, when logged in. Each modification of the comments for the onboard records, approval, granting of a full or a partial data access and submission to another user is to be digitally signed when completed by an authorized signature.

4.1.7 The reports generated by the DE SDS are to indicate the digital signature and comments from the last approver.

4.1.8 The DE SDS is to be provided with a maintenance mode where the ADE and SADE functionality of generating the DE results from data-centric evidence can be checked on a predefined synthetic datasets.

4.1.9 The maintenance mode of the DE SDS is:

a) to be clearly indicated in the user interface when active

b) not to compromise the normal operational entries

c) to generate the same type of outputs as in the normal operational mode.

4.1.10 The DE SDS is to provide a user interface with a list of all NC-A results registered for the period specified by a user.

5 Reporting process

5.1 Parties to the reporting process

5.1.1 The following parties are required to establish a documented collaboration to achieve the effective shared use of the DE ODS and DE SDS as per Fig 15:

a) Owner

b) DESS

c) the Society

d) Charterer, if identified by the Owner for the process.

Note 1: When the ship requires a regulatory exemption for a novel technology or an authorisation to operate in the framework of a critical infrastructure, the Flag Administration or Regional Authority may participate in the process and request an access to the DE SDS for the scope of the supervision.

Note 2: To the benefit of the Flag Administration, DE may support the reporting related to the process of maintenance of conditions after survey in line with SOLAS Chapter I, Part B, Regulation 11(c).

Note 3: If the OEM is different from the DESS, the OEM may participate in the process with data shared as per [5.1.6].

5.1.2 The Owner is to decide about the scope of DE ODS and DE SDS implementation by selecting the EUT subject to DE and by selecting its functional capabilities relevant for the operation of the ship. The selected EUT and functionalities are a basis of the Master Data developed by the DESS.

5.1.3 The approved DESS is to be employed by the Owner to provide the DE services in the scope of the monitoring subject to the contractual terms of the subscription between the Owner and the DESS. The approved DESS is responsible for the provision of the DE report as per [4.1.2]. In the event of a major service disruption impacting the provision of reports, the DESS is to inform as soon as possible the ship, the Owner and the Society.

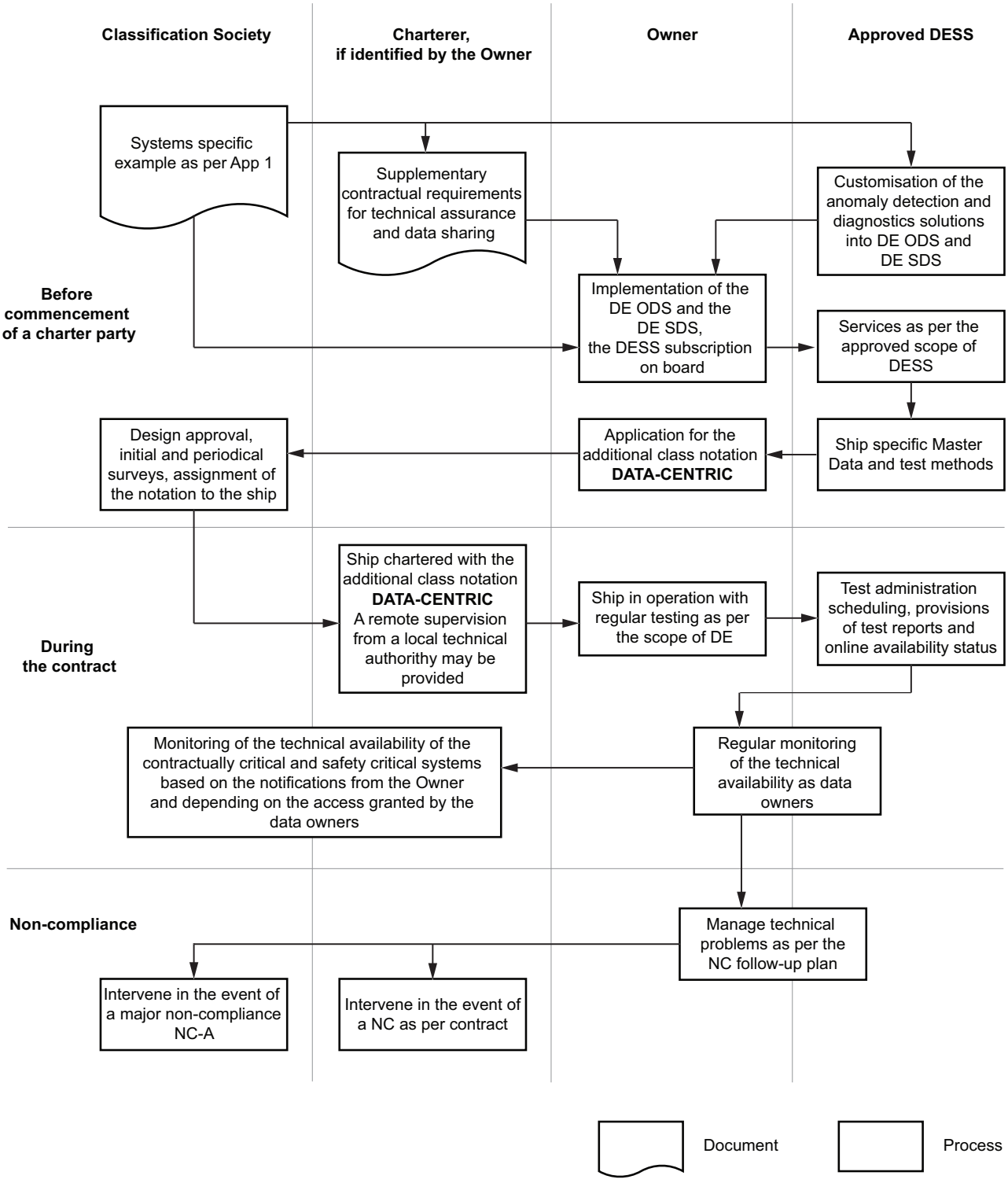
Note 1: The temporary suspension of the service in such instance is not to be considered as a non-compliance on ship's part.

5.1.4 The Society is to be informed by the Owner about the non-compliances of the NC-A category as per [5.3.1].

5.1.5 The Charterer may request an access to the DE SDS for the scope of the defect reporting subject to the contractual terms of the charter party between the Charterer and the Owner.

5.1.6 Owner, OEM and DESS, as data owners in respect of the data-centric evidence and of the DE results, are to establish a data sharing agreement with the Society. The data sharing agreement may also include Charterer, Flag Administration and Regional Authorities. The data sharing agreement is to include the access to the DE SDS for the each of the parties through the dedicated user interfaces.

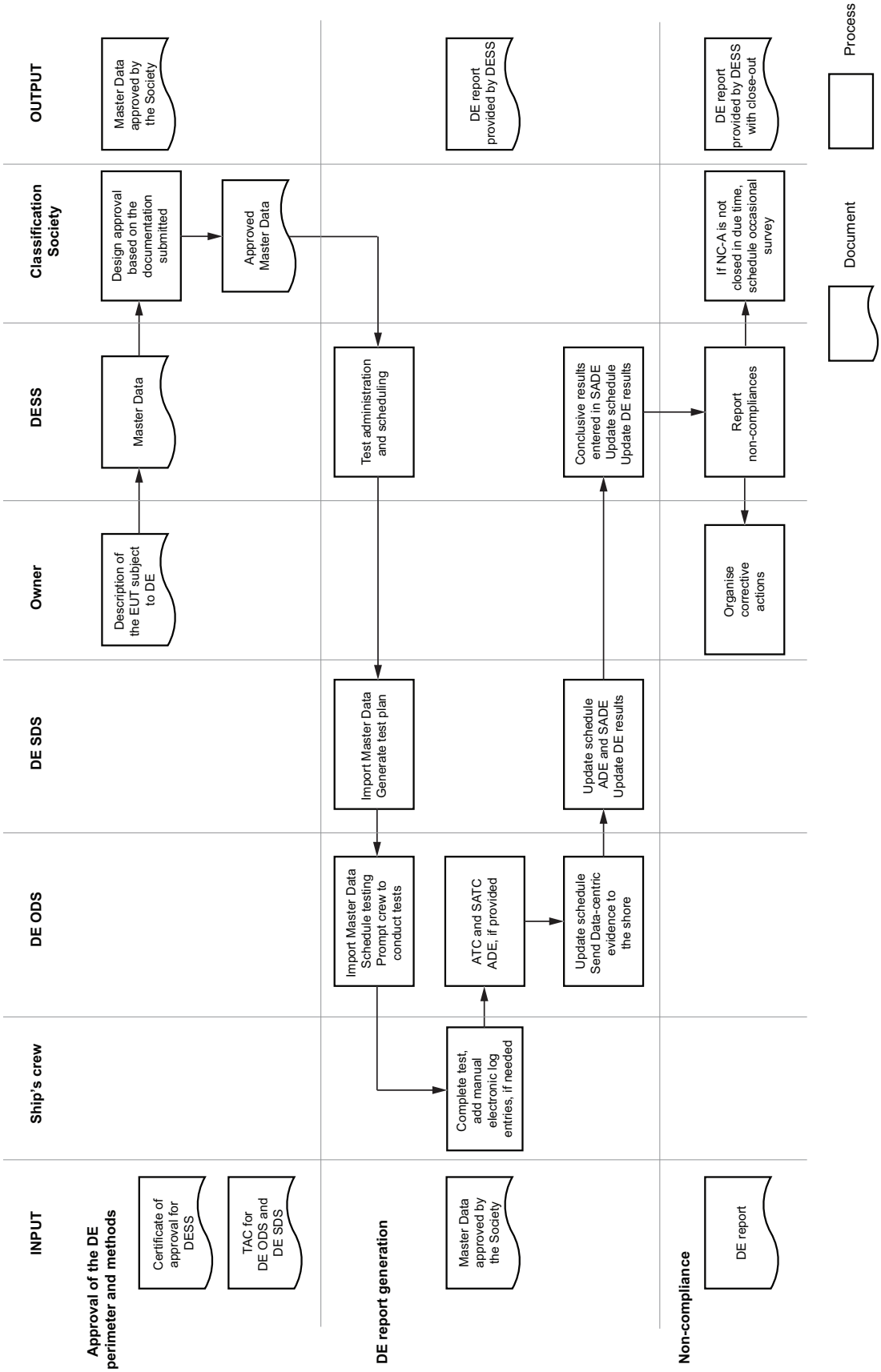
Figure 15 : DE reporting process workflow between Owner, DESS, Charterer and Classification Society



5.2 DE workflow

5.2.1 The DE workflow is described Fig 16. An equivalent block diagram is to be provided as a part of the contract for DESS subscription by the Owner.

Figure 16 : DE reporting process workflow between Owner, DESS and Society



5.3 Non-compliance (NC) follow-up plan

5.3.1 In the event of a NC-A the Society is to be informed by the Owner as soon as possible as per NR467, Pt A, Ch 2, Sec 2, [6.2.1] and the following is to be provided via the DE SDS user account dedicated for the Society:

a) DE report upon the detection of NC-A

b) action plan for the close-out of the NC-A

c) DE report following the close-out of the NC-A.

Note 1: It is not to be construed that the Society is informed when the access is granted. The Society is informed when the process for reporting defects is followed according to NR467, Pt A, Ch 2, Sec 2, [6.2.1] and the representative of the Society in charge of the ship is contacted.

5.3.2 Any pending test and NC-B are to be closed out within the period defined by the contractual terms of the subscription between the Owner and the DESS.

5.3.3 The non-compliance (NC) follow-up plan is to be provided by the Owner to the Society and is to include the maximum periods permitted for a non-compliance close-out as consistent with the test schedule and the contractual terms of the subscription between the Owner and the DESS.

5.3.4 The Owner is to maintain a record of the NC close-out with a day count of the lead time and the delays in the test completions. The contractual terms of the subscription between the Owner and the DESS are to include the maximum permitted lead time and delays in the test completion.

6 Initial Survey

6.1 Data-centric Evaluation Onboard Digital Solution (DE ODS)

6.1.1 Onboard function tests are to be witnessed by a Surveyor.

6.1.2 During the onboard test witnessed by a Surveyor, the system and EUT are to be operated to:

a) carry out each test, confirming that the “End of test” timestamped record is reachable in the sequence of ATC or SATC and confirming that the data-centric evidence is generated

b) if SATC function is provided, create manual entries as described in [3.1.3]

c) generate reports and access dashboards as described in [3.2.6], [3.2.7] and [3.2.10]

d) demonstrate integration into the ship’s communication network, including wireless network testing where applicable

e) while DE ODS is in a maintenance mode, load the test datasets described in [3.1.1] into the DE ODS, confirm that the results obtained from the DE ODS are identical to baseline corresponding to the test datasets

f) check the Type Approval Certificate with regards to the applicable EUT and confirm the software version.

6.2 Data-centric Evaluation Shore Digital Solution (DE SDS)

6.2.1 During the remote test witnessed by a Surveyor, the DE SDS is to be accessed by means of an external Internet connection to:

a) obtain access for each type of the user categories described in [4.1.3]

b) confirm availability of the items described in [4.1.4]

c) while DE SDS is in a maintenance mode, load the test datasets described in [4.1.9] into the DE SDS, confirm that the results obtained from the DE SDS are identical to baseline corresponding to the test datasets

d) check the Type Approval Certificate with regards to the applicable EUT and confirm the software version.

6.3 Initial audit of the process

6.3.1 A Surveyor is to examine the evidence of the process including

a) evidence of the documented collaboration in a form of agreements, contracts and memorandums of understanding as listed in [5.1]

b) non-compliance follow-up plan as per [5.3.3]

c) record of non-compliance close-outs as per [5.3.4].

Appendix 1 For Information Only, Guidance for Specific Systems

1 General

1.1 Purpose

1.1.1 Regular Data-centric Evaluation may be of interest for Owners and Charterers as a source of:

- insights into system's performance permitting to prevent technical downtimes and incidents
- improved fleet monitoring to feed the risk management
- insights into the workability and safe operational limits.

1.1.2 By analogy with the impact of the testing on the Safety Integrity Levels (SIL) described in IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems", regular DE may be used to monitor the reduction of probability of failure on demand for the Equipment Under Test (EUT) through:

- frequency of testing and
- test coverage defined by the pertinence of the selected data to failure detection.

1.1.3 The present Appendix provides basic sets of the use cases for the regular Data-centric Evaluation to facilitate the customisation of the anomaly detection and diagnostics digital systems towards DE ODS and DE SDS.

1.2 Liquefied Natural Gas as Cargo

1.2.1 The following scope could be covered by the DE ODS and DE SDS:

a) Detection tests: check high liquid level alarms as per NR467, Pt D, Ch 9, Sec 13, [3.1.1], check if alarms as per NR467, Pt D, Ch 9, Sec 13, [1.1.5] related to LNG containment and machinery are persistent with or without permanent manual alarm overrides and inhibits introduced.

b) Protection tests: Emergency Shut Down (ESD) testing, partial stroke testing for master valve.

c) Performance tests: Electro-hydraulic valve actuator health check through testing and recording the time to open and the time to close. Cargo and spray pump health check while in operation, confirm the correct start, stop sequences, performance against the capacity/current chart. Vapour return compressor health check while in operation. Confirmation that the nitrogen generation system is in working order to comply with the requirements for the barrier space atmosphere control as per NR467 Pt D, Ch 9, Sec 9 [1.2.1],[1.4.6], [1.4.7].

d) Functional testing equivalent to the scope of the annual survey as described in NR467, Part A, Ch 4, Sec 5, [3].

1.3 Offshore Access System

1.3.1 The following scope could be covered by the DE ODS and DE SDS:

a) Detection tests: Alarms as per NI629, Sec 3, [2.4.2]. Alarms for failures of the redundant motors on which the operation of motion compensation actuators is dependant.

b) Protection tests: Emergency retraction. Check if alarms defined in NI629, Sec 3, [2.4.2] are persistent with or without permanent manual alarm overrides and inhibits introduced.

c) Redundancy tests: Automatic changeover to redundant components.

d) Performance tests: normal condition with a load while in operation.

Note 1: NI629 Certification of Offshore Access Systems.

1.4 Energy Storage Systems

1.4.1 The following scope could be covered by the DE ODS and DE SDS:

a) Detection tests: testing of alarms as per NR467, Pt F, Ch 14, Sec 2, [3.7.3].

b) Redundancy tests: automatic connection of ESS to the bus bar following a partial blackout on the bus bar.

c) Performance tests: switching of charging and discharging modes for the Energy Storage System (ESS), response to load step changes, depletion test.

d) Functional testing equivalent to the scope of the annual survey as described in NR467, Part A, Ch 5, Sec 15, [3.2].

1.5 Unmanned Surface Vessel (USV) Systems

1.5.1 The following scope could be covered by the DE ODS and DE SDS:

a) Detection tests: Alarms as per NI641, Sec 3, [2.4.5], [3.4.1], [4.6.2], [5.4.3], [6.4.2], [6.5.2], Sec 4, [4.2.6], [4.3.4], NR681, Sec 3, [1.2.3], Sec 6, [1.2.3]. Regular status report specifying the technical availability status of the ship's systems providing essential services as per NI641, Sec 3, [8.2.1].

b) Protection tests: Activation of fallback modes as per NI641, Sec 3, [8.2.2], [8.2.3].

c) Redundancy tests: Tests of redundant components associated with essential services while at sea with the Navigating Automation System in running condition as per NR467, Pt A, Ch 5, Sec 12, [4.1.2]. The USV is to maintain the global system functions after a single failure, tests should include the scenario of a worst case failure of the electric power supply system.

d) Performance tests: Tests of propulsion to deliver the 100% thrust output for 15 minutes or until associated machinery temperatures stabilise while at sea with the Navigating Automation System in running condition. The tests should be performed to confirm the station-keeping capability envelope in the degraded and worst case failure modes for the propulsion. Confirmation that the USV is operated without exceeding the approved operational envelope. Regular actuator fault diagnostics, e.g. on the basis of the adaptive exogenous Kalman filter.

Note 1: NI641 Guidelines for Autonomous Shipping.

1.6 Dynamic Positioning (DP) Systems

1.6.1 The following scope could be covered by the DE ODS and DE SDS:

a) Detection tests: Alarms as per NR467, Pt F, Ch 11, Sec 5, [4.8.2], [4.9.4], [4.10.4], [11.5.1].

b) Protection tests: Activation of black out prevention, load shedding on the power plant.

c) Redundancy tests: Automatic changeover to redundant components.

d) Performance tests: Tests of propulsion to deliver the 100% thrust output for 15 minutes or until associated machinery temperatures stabilise. Tests of generators to deliver the 100% power output for 15 minutes or until associated machinery temperatures stabilise. Regular checking configuration for compliance to approved FMEA while within the offshore installation safety zone as enabled by geofencing.

e) Procedural compliance tests: Regular checking compliance of configuration to sets of the requirements specific to the offshore installation safety zone as prescribed by Owner or Charterer, e.g. speed limits, power plant configurations, duration of on site pre-entry checks, minimum separation distances steel-to-steel, maximum excursions and other limits as defined in the Activity Specific Operating Guidelines (ASOG).

1.7 Process systems on board Offshore Units and Installations

1.7.1 The following scope could be covered by the DE ODS and DE SDS with a reference to Rule Note NR445 Offshore Units:

a) Detection tests: Alarms for fire protection systems as per NR445, Pt C, Ch 4, Sec 5, [3] and gas detection systems as per NR445, Pt C, Ch 4, Sec 5, [4], alarms for failures and abnormal conditions as per NR445, Pt C, Ch 3, Sec 7. Fault detection as per NR459, Sec 2, [11.6.2].

b) Protection tests: Safety systems as per NR445, Pt C, Ch 3, Sec 7 and ISO 16904, [6] including, but not limited to, Emergency Release System (ERS), ESD, monitoring, alarm, shut-down systems.

c) Redundancy tests: Applicable tests as per NR445, Pt C, Ch 3, Sec 7, [7], NR459, Sec 2, [4.5] for component changeovers, partial blackout tests.

d) Performance tests: Diesel engine tests as per NR445, Pt C, Ch 1, Sec 11, [3.2.4], operational tests as per NR459, Sec 2, [4.5], applicable tests as per NR445, Pt C, Ch 3, Sec 7, [7.1.2], regular checking of the configuration on the basis of the approved lists of monitored parameters for alarm/monitoring and safety systems.

e) Safety Instrumented System (SIS) tests: Monitoring of test outcomes and test frequency for the SIS against the scope and schedule prescribed to attain the required SIL (Safety Integrity Level) for the process plant, e.g. monthly partial stroke test for a safety valve.

Note 1: NR445 Rules for the classification of offshore units, NR459 Process systems onboard offshore units and installations.

1.8 Electrical installations

1.8.1 The following scope could be covered by the DE ODS and DE SDS:

a) Detection tests: Alarms as per the references to the detection functionalities in Tab 1.

b) Protection tests: Tests of auto-start of stand by generators, of auto-connection of busbars, of paralleling, of loading sharing, of load shedding and of power supply keeping in case of loss of normal supply. Test of the blackout prevention functions and of blackout recovery. Test of response to the communication network failures. Testing of heavy consumer start inhibits. Also refer to the tests as per the references in Tab 1.

c) Redundancy tests: Automatic changeover to redundant components.

d) Performance tests: Regular checking of the configuration on the basis of the approved lists of monitored parameters for alarm/monitoring and safety systems. Checking the operation of Engine Power Limitation (EPL) and Shaft Power Limitation (ShaPoLi)

systems. Anomaly detection and diagnostics for early signs of performance degradation. Motor current signature analysis. Oil and wear particles analysis, if available. Vibration analysis from fixed sensor, if installed. Also refer to the tests as per the references in Tab 1.

Table 1 : Testing of electrical installations recommended for DE

EUT	Tests for detection and protection functionalities	Performance tests
Control of machinery	NR467, Pt F, Ch 3, Sec 1, [4]	NR467, Pt F, Ch 3, Sec 1, [7]
Diesel engines	NR467, Pt C, Ch 1, Sec 2, [2.7.5], [2.7.6], [2.7.8]	NR467, Pt C, Ch 1, Sec 18, [3.5]
Internal combustion engines supplied with low pressure gas	NR467, Pt C, Ch 1, App 2, [2.2.6]	NR467, Pt C, Ch 1, App 2, [4.3]
Electric propulsion plants	NR467, Pt C, Ch 2, Sec 14, [4.4.4], [4.5]	NR467, Pt C, Ch 1, Sec 18, [3.9] NR467, Pt C, Ch 2, Sec 15, [5]

1.9 Integrated bridge systems

1.9.1 The following scope could be covered by the DE ODS and DE SDS:

a) Detection: confirmation that an alarm is displayed on the ECDIS in case of GNSS input failure.

b) Redundancy tests: confirmation that the ECDIS need not to be manually initialised in case of change from main to emergency power supply. Automatic changeovers to redundant network components. Check of the availability of the dual supply of ECDIS.

c) Performance tests: confirmation that the equipment is in working order, including:

- gyro compass
- radar installation (9 GHz)
- transmitting heading device
- second radar installation
- automatic radar plotting
- electronic plotting aid (EPA)
- automatic tracking aid (ATA)
- echo-sounding device
- speed and distance measuring device (SDMD) on water
- speed and distance measuring device (SDMD) on the ground
- heading control system or track control system
- ECDIS
- Bridge Navigational Watch Alarm System (BNWAS).

Appendix 2 For Information Only, Implementation Examples

1 Use Cases

1.1

1.1.1 The following use cases are given as examples in:

- Tab 1 for Use case 1: Integrated Bridge Systems
- Tab 2 for Use case 2: Fire Detection Systems
- Tab 3 for Use case 3: Emergency Shut Down (ESD) for a LNG cargo system
- Tab 4 for Use case 4: Compliance monitoring within a safety zone of offshore installation (windpark or oil and gas field).

Table 1 : Use case 1 - Integrated Bridge Systems

Time-series	Heartbeat of the components, online/offline status, alarms rendered as timeseries can be selected.
Event data	Applicable alarms can be selected as per IEC 62923-2 Maritime navigation and radiocommunication equipment and systems - Bridge alert management - Part 2: Alert and cluster identifiers and other additional features.
Manual electronic log entries	Periods of planned maintenance with equipment taken out of operation, periods in port and in transit at sea can be logged manually.
Reference Configurations	The following reference configurations can be defined: • Initial Reference Configuration is defined daily by: - the time, 00:00 UTC - the equipment status - data infrastructure's LAN is running - the status of the ship as recorded in the electronic logbook, "vessel at sea"; • Final Reference Configuration is defined by the sum of the data-centric evidence collected while at sea during a 24 hours period. The following data represents the Final Reference Configuration: - 23:59 UTC, - data infrastructure's LAN is running, - 99% uptime observed for the relevant timeseries, - consolidated list of alarms does not include alarms indicative of a loss of the essential functions of integrated bridge system (passage execution, route control and monitoring as per NR467, Pt F, Ch 4, Sec 2).
Responses	The transition between the configuration at 00:00 and the configuration at 23:59 is covered in this test protocol.
Reference capability	The transition from 00:00 to 23:59 configurations is represented by the Reference Configurations. Non-compliant configurations are not detected.
Class non-compliant configurations	Consolidated list of alarms includes alarms which are indicative of a loss of the essential functions of integrated bridge system (passage execution, route control and monitoring, see NR467, Pt F, Ch 4, Sec 2).
ATC	The data-centric evidence is automatically extracted for the 24 hour period and a consolidated list of alarms is generated with the duration of their active conditions. Manual electronic log entries are used to filter the applicable timespans.
SATC	Not applicable.
ADE	The configurations are compared to the Reference Configurations. Class non-compliant configurations are reported as NC-A.
SADE	Not applicable.

Table 2 : Use case 2 - Fire Detection Systems

Time-series	Heartbeat of the components (e.g. loop monitoring), mode (operational, test), online/offline status, alarms rendered as timeseries can be selected.
Event data	Event messages for the activation of fire detectors can be selected.
Manual electronic log entries	Periods when the crew performed the testing can be logged manually, if the event data for a mode switch to the testing mode cannot be used as the data-centric evidence.
Reference Configurations	The following reference configurations can be defined: • Initial Reference Configuration: no loop monitoring alarms, no inhibited alarms, all components online, system in test mode. • Final Reference Configuration as a sum of event data collected during the testing period: no loop monitoring alarms, no inhibited alarms, all components online, system re-instated to operational mode, all fire detectors in a selected compartment produced an alarm indicative of a successful functional check
Responses	The transition between the configuration at the start of the test recorded by the crew and the configuration at end of the test recorded by the crew is covered in this test protocol.
Reference capability	The response from the manually recorded start of the test to the end of the test is represented by the Reference Configurations. Non-compliant configurations are not detected.
Class non-compliant configurations	Event data is indicative of a loss of the essential functions of fire detection system (see NR467, Pt C, Ch 4, Sec 15 [8]), e.g. loop monitoring alarms, multiple adjacent detectors did not produce alarms upon local test activation attempt.
ATC	Not applicable
SATC	The data-centric evidence is extracted for the period manually recorded by the crew as the test start and completion.
ADE	The configurations are compared to the Reference Configurations. Class non-compliant configurations are reported as NC-A.
SADE	Not applicable.

Table 3 : Use Case 3 - Emergency Shut Down (ESD) for a LNG cargo system

Time-series	The following timeseries could be used: • EUT: Heartbeat of local control PLCs, LAN status, valve status (closed, open), valve actuator command and feedback (as a percentage), emergency shut down loop monitoring system status, pump and compressor status, emergency shutdown push button status. Timeseries cover the response for the cargo, stripping pumps, compressors, master valve, spray master valves, fill valves, manifold valves. • Connected units: Tank protection system heartbeat.
Event data	The following event data could be used: • EUT: ESD activation alarm, ESD link (fiber optic, pneumatic, etc.) status change. • Connected units: Tank protection system alarms.
Manual electronic log entries	Start and stop of the test, status of the shore facilities, records of the cargo operation linked to the preparatory ESD testing can be logged manually.
Reference Configurations	The following reference configurations can be defined: • Initial Reference Configuration: no loop monitoring alarms, no inhibited alarms, all components online. • Intermediate Configuration as a sum of timeseries and event data during 30 seconds after the activation of the ESD: liquid piping system ESD valves are fully closed within the given time (IGC Code, 18.10.2.1.3), ESD activation alarms produced, pumps, compressors are shut down. • Final Reference Configuration as a sum of event data collected from the end of the previous test step to the end of the test: no loop monitoring alarms, no inhibited alarms, all components online, system returned to operational mode. The ESD test may be completed for the whole system or only for a selected part of it as selected by the Owner. The difference in the configurations for the full and partial testing will require a provision of a separate test for each distinct set of configurations.
Responses	The transition covered in this test protocol is between: a) configuration at the start of the test, the start time is recorded by the crew b) configuration 30 seconds after the activation of the ESD, time is estimated automatically based on the ESD event data c) configuration at end of the test, the end time is recorded by the crew.
Reference capability	The responses from the manually recorded start of the test to the end of the test are represented by the Reference Configurations. Non-compliant configurations are not detected.
Class non-compliant configurations	Event data is indicative of a loss of the essential functions of ESD system as per NR467, Pt D, Ch 9, Sec 5, [5], e.g. an ESD valve's actuator does not respond to the command to close and, as a result, the system cannot be isolated.
ATC	Not applicable
SATC	The data-centric evidence is extracted for the period between the start and the end which are manually recorded by the crew. The limits of the intermediate step can be automatically identified from the time of the ESD's activation and the maximum time allowed for the resulting effects to produce, e.g. as per IGC Code, 18.10.2.1.3.
ADE	The configurations are compared to the Reference Configurations. Class non-compliant configurations are reported as NC-A.
SADE	Not applicable.

Table 4 : Use case 4 - Compliance monitoring within a safety zone of offshore installation (windpark or oil and gas field)

Time-series	The following timeseries can be used: • Ships position and heading, overall DP configuration as per NR467, Pt F, Ch 11, Sec 5, [4.8.2]. • Geofencing timeseries related to tracking which part of the safety zone the ship is in (e.g. identifier of installation, drift-on or drift-off area, concentric zones defined by steel-to-steel distance).
Event data	Alarms as per NR467, Pt F, Ch 11, Sec 5, [4.8.2] and operator commands can be selected.
Manual electronic log entries	Operational activity to crosscheck geofencing timeseries can be logged manually.
Reference Configurations	The following reference configurations can be defined: • Initial Reference Configuration: - 50 m to the border of the safety zone, - data acquisition infrastructure's is running; • Final Reference Configuration: Sum of the data-centric evidence collected until exit from the safety zone for the following data: - data acquisition infrastructure running, - 99% uptime of the timeseries, - consolidated list of alarms does not include alarms indicative of a loss of the essential functions of DP system (station-keeping and heading control as per NR467, Pt F, Ch 11, Sec 5, [1.4.1]).
Responses	The transition between the configuration at the zone entry and the configuration at zone exit is covered in this test protocol.
Reference capability	The response from the automatically recorded start of the test to the end of the test is represented by the Reference Configurations. Non-compliant configurations are not detected.
Class non-compliant configurations	Consolidated list of alarms includes alarms indicative of a loss of the essential functions of DP system (station-keeping and heading control as per NR467, Pt F, Ch 11, Sec 5, [1.4.1]).
ATC	The data-centric evidence is automatically extracted for the period spent in the safety zone or every 24 hours if longer than 24 hours. A consolidated list of alarms is generated with the duration of their active conditions. Geofencing timeseries are used to filter the applicable timespans.
SATC	Not applicable.
ADE	The configurations are compared to the Reference Configurations. Class non-compliant configurations are reported as NC-A.
SADE	Not applicable.

Appendix 3 For Information Only, Reporting Based on Data-centric Evidence

1 Enhanced reporting process

1.1 Data-centric evaluation framework

1.1.1 The present Rule Note provides a framework for the exchange of the data-centric evidence. The results of the data-centric evaluation can be used by stakeholders to corroborate the existing defect and breakdown reporting.

1.2 Reporting safety precursor events

1.2.1 Where the Owner is required by Authorities to report specific failures of equipment, loss of the required functionalities or exceeding the limits of the permitted operational conditions, the Owner could support the reporting with the data-centric evaluation results. For the ships engaged in the critical infrastructure or using the novel technology for essential services on board, the regular data-centric evaluation may help detecting the safety precursors and near miss events. For example, it may include automatic and autonomous mode disengagements for dynamic positioning and autonomous navigation modes respectively. Such a reporting corroborated with the data-centric evidence may reduce the probability of failures. An example of using the data-centric evaluation by Authorities is given in Tab 1.

Table 1 : Use of data-centric evaluation by Authorities

Example of regional requirements for unmanned units	Application of the data-centric evaluation to improve the reporting process for the Authorities
The operator is to be able to detect and record the anomalies indicative of: • non-compliance with the functional requirements prescribed by the Authorities • exceeding the operating conditions and limits in which the unmanned unit is authorised to be operated according to the registration certificate • dangerous conditions for humans, ships and the environment. The list of the automatically detectable anomalies is to be declared to the Authority by the Owner. Anomalies detected in service are to be transmitted to the Authority by the Owner	• The anomalies can be detected via the data-centric evidence collected from the unit. Failures can be linked to NC-A and NC-B notifications for systems selected by the Authorities • Selected instances of the inability to comply can be reformulated as: - failing a functional test - combination of the operational conditions and alarms

1.3 Defect reporting aligned with contractual clauses

1.3.1 Traditional reporting

In the traditional reporting, the failures of the equipment on the critical path may not be immediately detected, interpreted as a breakdown as per a given contract and further reported by the Owner. The application of the time charter day rates could not correspond to the actual status of the ship if a variation is prescribed based on the technical availability and if the date of the breakdown is not established correctly. Time with the full hire rate may be lost on the close-out of the corrective action aimed to restore the lost functionality as the Charterer may require the evidence or onboard inspection to accept the corrective action.

1.3.2 Comparison

Where the Owner is required by a Charterer to report breakdowns and failures leading to the inability of the ship to perform the contracted services, the Owner may support the defect reporting with the data-centric evaluation results. The defect reporting enhanced by the data-centric evaluation framework could offer an improved assessment of the ship's status when compared to the traditional reporting, as indicated on Fig 1.

1.3.3 Reporting enhanced with data-centric evaluation

In the data-centric evaluation framework, the failures of the equipment on the critical path may be detected with the periodicity of the regular data-centric evaluation. This periodicity may be improved by the automatic means. As the datasets conclusive of the failure are established at the design approval stage and that there is an automated reporting, the failures may be faster communicated by the DESS to the Owner, who in turn may share the information with the interested parties. As the subsets of anomalies indicative of a potential condition of class (NC-A) are identified for the classed ship at the design approval stage and prioritised, the interested parties may be in relation in a short time. When the Owner completes the remedial action, the close-out could be validated remotely by the Charterer based on the corroborating data-centric evidence. An example of using the data-centric evaluation by Charterers is given in Tab 2.

Figure 1 : Comparison of the traditional and the DATA-CENTRIC reporting methods

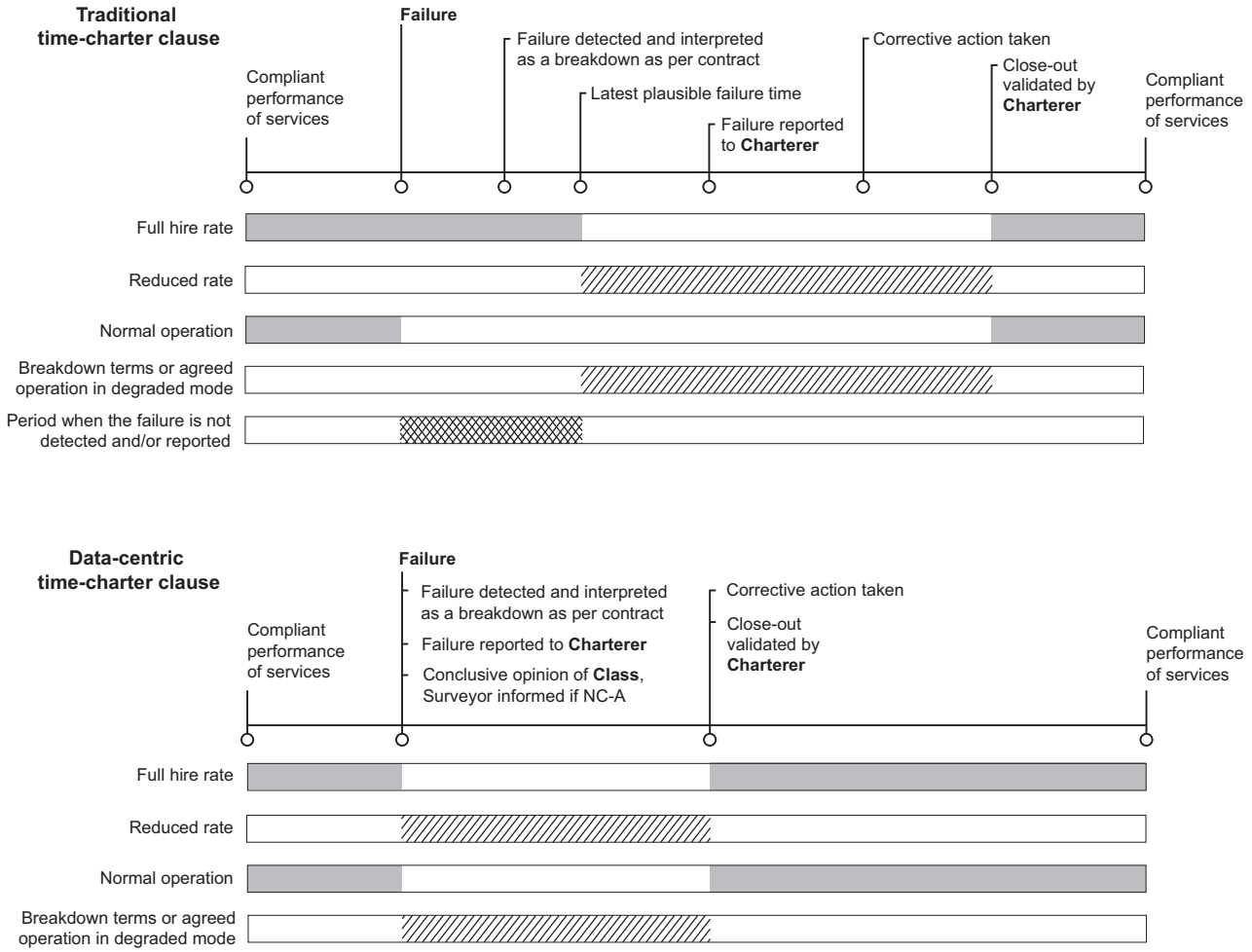


Table 2 : Use of data-centric evaluation by Charterers

Example of time-charter party contractual terms	Application of the data-centric evaluation to improve the reporting process for the Charterer
Definitions: Breakdown: inability to perform the contracted services on the critical path due: • to failure of the ship, to failure to deliver the maximum continuous capacity	• The failures may be detected via the data-centric evidence collected from the ship. Failures can be linked to NC-A and NC-B notifications for systems selected by the Charterer • Selected instances of the inability to comply can be reformulated as: - failing a functional test - combination of the operational conditions and alarms
Technical requirements: • The Owner is to ensure that all marine equipment is in continuous documented compliance with the requirements o the Classification Society for the vessel type, equipment and service • Dynamic Positioning systems are to be compliant with IMO MSC.1/Circ 1580 with the requirements of the Classification Society f for notation **DYNAPOS AM/AT-R** or equivalent. Sensors and monitoring systems are to be as per the requirements of the Classification Society • Bulk Methanol Capability: All control systems related to loading, onboard storage and discharge are to be fully redundant	
Technical assurance: The Owner is to ensure that: • the ship is under a defect reporting system which alerts the staff responsible for maintenance onboard and ashore when items become due • any condition of class is closed out in due time	The defect reporting may be automated for the selected equipment in the critical path. The condition of class may be issued and closed out based on the automated reporting of the pre-agreed NC-A

2 Data ownership and access

2.1 Data ownership

2.1.1 The present Rule Note is based on the assumption that the Owner and the DESS have access to the data at a periodicity sufficient to perform the data-centric evaluation as per the Master Data document. For the purpose of this Rule Note, the access to the data for the Society, Authorities, Charterer and other interested parties is event-based and controlled by the Ship Owner acting as the Owner of the operational data. The provision of operational data is deemed to be supported by the DESS and the OEM as per the present Rule Note.

2.2 Event-based access to the data

2.2.1 The Society cannot continuously monitor the data-centric evidence in the online portal of DE SDS. The Society should only access the data between the periodical surveys in case the Shipowner has duly notified the Society about a NC-A. The notifications correspond to the traditional reporting of defects as per SOLAS Ch I Reg 11 (c). The notification about NC-A may trigger an occasional survey and an issuance of a condition of class.

2.2.2 The Charterer and Authorities do not continuously monitor the data-centric evidence in the online portal of DE SDS. The Charterer and Authorities should only access the data in case the Owner notifies them about a NC-A or NC-B according to the data-sharing agreement between these parties.

2.2.3 For Charterers, the notifications may correspond to the contractual definition of the breakdown and may trigger the application of the reduced day rate.

2.2.4 For Authorities, the notifications may correspond to the non-compliance with the functional requirements and exceeding safe operational limits defined in the safety case and/or permit to operate.

BUREAU VERITAS MARINE & OFFSHORE

Tour Alto
4 place des Saisons
92400 Courbevoie - France
+33 (0)1 55 24 70 00

marine-offshore.bureauveritas.com/rules-guidelines

BUREAU VERITAS
1828
BUREAU
VERITAS

Shaping a World of Trust