# No. 153 (Sep 2018) Recommended procedures for software maintenance of computer based systems on board

## 1. Scope

1.1 These procedures:

- are supplemental to IACS UR E22 “On Board Use and Application of Computer based systems” and apply to the use of computer based systems which provide control, alarm, monitoring, safety or internal communication functions which are subject to classification requirements.

- apply also to systems not subject to classification requirements but which, when integrated with or connected to classed equipment or equipment with an impact on safety, can expose the vessel to cyber-risks and have an impact on the safe and secure operation of the ship.

- are applicable to vessels built after the introduction of the recommendation but may also be applied to ships already in service.

- may be applied to additional systems at the request of the owner.

1.2 Shipboard equipment and associated integrated systems to which these procedures apply can include, but are not limited to:

- Bridge systems;
- Cargo handling and management systems;
- Propulsion and machinery management and power control systems;
- Access control systems;
- Ballast water control system;
- Communication systems; and
- Safety system.

1.3 If the software maintenance leads to hardware maintenance, the hardware used should be suitable for the equipment or system according to applicable requirements of the Classification Society

## 2. References

For the purpose of application of this REC, the latest in force version of the following standards can be used for reference:

- ISO/IEC 14764 Standard for Software Engineering – Software Life Cycle Processes – Maintenance

- IACS UR E22 On Board Use and Application of Computer based systems

- The Guidelines on Cyber Security onboard Ships (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI)

- Industry standard on software maintenance of shipboard equipment (CIRM/BIMCO )

## 3. Process of software maintenance

3.1 A process of software maintenance should comprise the following sub-processes:

- Identification
- Planning
- Execution
- Validation

3.2 Each of the four sub-processes is described below:

3.2.1 Software maintenance identification

The software maintenance identification is identification of need for software maintenance of computer based system on board. The information including Category of maintenance should be provided to relevant stakeholders.

3.2.2 Software maintenance planning

The software maintenance should be properly planned before it is executed in order to optimize its arrangements and to achieve the best possible outcome. Close communication between all relevant stakeholders should be ensured. The specific planning requirements for the maintenance event depend on computer based system on board.

3.2.3 Software maintenance execution

When software maintenance is actually carried out on computer based system on board, it should be conducted in accordance with software maintenance planning

3.2.4 Software maintenance validation

Following completion of the software maintenance execution sub-process, communication between the relevant stakeholders should continue in order to validate the software maintenance, and to provide information which can be used to increase the effectiveness and success of future software maintenance event.

## 4. Responsibilities of Stakeholders

### 4.1 Producer of software or System Integrator

4.1.1 The Producer of software or System Integrator should have a quality system for software lifecycle activities, which documents relevant procedures, responsibilities and configuration management, including deliveries from sub-suppliers, taking into account cyber-security considerations.

4.1.2 When the Producer of software or System Integrator has identified the need for software maintenance, this information should be relayed to relevant stakeholders as necessary timely. The information pertaining to the maintenance should be made available by website or email/bulletin, including the Category of maintenance and the method of maintenance supported for undertaking it.

4.1.3 The Producer of software or System Integrator should identify the necessary technical competencies of the service technicians and provide training in the maintenance operation to Service Provider so that he can carry out satisfactorily the software maintenance.

## 4.2 Data provider

4.2.1 Data provided should carry out data production and distribution operations in accordance with a quality system, covering:

- Data quality (production, delivery, testing and integration);
- Standardization of data import;
- Means to ensure the continuous availability of data maintenances;
- Prevention/detection/protection from unauthorized modification;
  Prevention of the distribution of malware.

4.2.2 When data provider has identified the need for a maintenance of data and/or the software using the data, this information should be relayed to relevant stakeholder as necessary timely. The information pertaining to the data maintenance should be made available, e.g. by website or email/bulletin, including the category of maintenance, the method of maintenance supported for undertaking it.

4.2.3 Data provider should provide training in the updating operation to Service Provider.

## 4.3 Service Provider

4.3.1 Service Provider should carry out maintenance-related operations in accordance with a quality system, covering:

- Competence management;
- Coordination and call-entrance procedures;
- Remote maintenance procedures (if applicable);
- Reporting procedures;
- Shipboard operations safety briefing;
- Cyber-security.

4.3.2 Service Provider should establish quality standards and internal training for technicians in line with maintenance and competency requirements of the Producer of software and/or System Integrator and include them in a quality manual.

4.3.3 Service technicians should be trained by Producer of software, System Integrator, or qualified trainer recognized by Producer of software or System Integrator. Producer of software and system integrators should, as part of their contractual obligations, be required to identify the necessary technical competencies of the service technicians and supply the necessary documentation in order to make the work of the technicians effective.

4.3.4 Service Provider should carry out the software maintenance in accordance with the Health, Safety, Security and Environment (HSSE) instructions provided by the Shipowner.

4.3.5 Service Provider should coordinate remote maintenance with the Shipowner. In case of remote maintenance, a time slot for when the computer based system is connected and powered up should be agreed. Procedures should be agreed in order to determine when the shipboard connection can be closed, after concluding the maintenance procedures.

4.3.6 Qualified technicians from Service Provider should prepare all necessary tools and resources needed to access the shipboard equipment for software maintenance (for example:

laptop, media device, specific tools recommended by the Producer of software or System Integrators, etc.).

4.3.7 As far as practicable, Service Provider should avoid direct connection of uncontrolled equipment to a controlled network.

4.3.8 If portable computer, removable media/storage devices are intended to be used in the maintenance process, the Service Provider should confirm that such devices have been subject to a malware check before the maintenance is carried out.

4.3.9 Service Provider should obtain authorization from Shipowner before carrying out remote maintenance. Additionally, authorization should be obtained from the ship's Master before every remote maintenance session. (See also IACS Rec. No. 163 "Remote Update/ Access")

4.3.10 It should be the Service Provider's responsibility to be satisfied that the system functions as intended after the software maintenance has been concluded.

### 4.4 Shipowner

4.4.1 The Shipowner should ensure that software maintenances are carried out in accordance with an appropriate International Safety Management (ISM) Code system and operational procedures. If the software maintenance is relevant to class related services, the Shipowner should inform the Classification society before the operation of the software maintenance is carried out.
Shipowner may delegate some responsibilities to the vessel operating company or assigned system integrator.

4.4.2 The Shipowner can initiate software maintenance:

- As part of the after-sales support for the shipboard equipment;
- As a preventative or corrective maintenance operation;
- Due to operational anomalies;
- In response to a request by the Data Provider, Producer of software, System Integrator or Service Provider.

4.4.3 The Shipowner should have procedures in place in order that software is kept up to date with the requirements of the Producer of software, System Integrator, or Data Provider.

The following types of checks should be included in these procedures:

- Automatic maintenance, when specifically permitted, and how these are carried out in a secure, coordinated and safe manner;

- Scheduled maintenance (e.g. Annual Performance Tests, clean-ups, diagnostics) and instructions for when this should take place and how;

- Remote access configuration of the downloading computer.

4.4.4 The Shipowner should maintain on board an on board software log listing the current and previous software versions installed on shipboard equipment.

4.4.5 When the Producer of software, System Integrator, or Data Provider has advised of the need for a software maintenance, including the Category of maintenance and Method of maintenance, or when maintenance has been requested by the Shipowner, the Shipowner

No. 153 (Cont)

should prepare a maintenance plan in accordance with the type of maintenance in question. The following considerations should be included in the maintenance plan:

- Identification of the need for additional familiarization, changes to operating procedures, and changes to on board documentation;

- Description of how to avoid security risks including unauthorized access and spread of malware;

- Identification of the software, computer based system, and network to be maintained;

- Identification of all computer based system affected due to their interface connections to other computer system requiring the software maintenance;

- Identification of individual responsible for the maintenance and possible supervision of technician from Service Provider;

- Procedures for restoring previous stable software version in the event that errors are encountered during maintenance;

- Preparation for remote access, if this is required during the maintenance;

- Authorization of appropriate crew member(s) to conduct or assist with the maintenance;

- Authorization of technician from Service Provider to conduct the maintenance;

- Procedures for validating the maintenance after completion;

- Coordination with the Master for safety of navigation.

4.4.6 When an operational anomaly has been identified, the Shipowner should provide information about the equipment and connections used on board, and related configurations and software versions, necessary port information and agent details, to the Service Provider.

4.4.7 The Shipowner should plan and agreed upon with the Service Provider maintenance requirements for the equipment at hand.

4.4.8 When the Producer of software, System Integrator or Data Provider Role has determined the need for a critical maintenance and provided the necessary means, this maintenance should be planned between the Service Provider and Shipowner in order that it will be undertaken as soon as possible and that downtime of the shipboard equipment is minimized.

4.4.9 The Shipowner should communicate any specific Health, Safety, Security and Environment (HSSE) instructions to the Service Provider so that these may be adhered to in the Service Provider’s Plan of Approach.

4.4.10 The Shipowner should have procedures in place to protect shipboard equipment from malicious or unintentional security threats. Safety procedures should include the following considerations:

- Service Provider selection and use of competent technicians;

- Ensuring secure communications and remote access;

- Identification of technician(s) form Service Provider coming on board;

- Access management for technician(s) from Service Provider

- Avoiding, as far as practicable, direct connection of uncontrolled equipment to a controlled network

- Confirmation from the Service Provider that any portable computers, removable media/storage devices intended to be used in the maintenance process have been subject to a malware check before the maintenance is carried out.

4.4.11 The Shipowner should record each software maintenance activity performed on computer based system in the on board software log and link it to the associated electronic service report provided by the Service Provider. Such recordings may be made available on request by the Service Provider in support of future software maintenance.

4.4.12 Following maintenance, if the Producer of software, Provider or System Integrator has confirmed that new functionalities, changes or improvements have been implemented, the Shipowner should ensure that crew familiarization with the computer based system is carried out.

### 4.5 Classification Society

4.5.1 The society should be informed by the Shipowner of any software maintenance relevant to class related services.

4.5.2 Documentation as per IACS UR E22 should be submitted by the Shipowner prior to the execution of maintenance for consideration by individual classification society.

4.5.3 The test of software maintenance should be witnessed by the classification society as required.

4.5.4 The classification society should be presented with an updated Inventory for computer based system on board (see appendix 1) post satisfactory testing, which should be kept on board.

## 5. General requirements for computer based systems on board

5.1 Computer based system should allow access for maintenance purposes and should provide protection against unauthorized access.

5.2 Computer based system should support procedures to roll back to a previous software version and configuration during software maintenance, after a software maintenance has been attempted. Roll back procedures could be based on a previous software version stored in the computer based system or on previous software versions that can be uploaded by the Service provider.

5.3 Where appropriate, computer based system should include a mechanism to generate an on-the-spot diagnostic report after maintenance has been performed, which also identifies the software version running on the equipment or system. The equipment or system should also provide a means to check that interfaces and functionality are operating as expected after maintenance has been completed. This mechanism should be described in the software maintenance manual, including the method of execution.

5.4 Computer based system should provide the means to display, on demand, the current software version.

## 6. Testing

6.1 After the software maintenance execution has been concluded, the following tests should be carried out by the Service Provider for validation:

- Regression tests
- New functionalities and/or improvements tests;
- Load tests.

The objective of software testing after maintenance is to verify that the equipment subject to software maintenance, integrated in the relevant system or sub-systems, behaves according to the specification and according to the applicable requirements.

6.2 During the software maintenance planning the Producer of software or System Integrator and/or the Data Provider should issue a Test Plan specifying the tests to be executed. Test Cases covering both normal operation and failure conditions should be specified in the Test Plan.

6.3 Regression tests are aimed at verifying that no functionality which is expected to be still present after the maintenance has been impaired.

6.4 The purpose of testing new functionalities and/or improvements is to verify that the software maintenance has had the intended effect.

6.5 The Load test should be conducted to verify the behavior of the system under a specific expected load, under both normal and peak conditions.

6.6 The tests should cover each equipment subject to the maintenance and their integration in the system or sub-system they are part of.

6.7 Testing process should be subdivided into the following activities:

- **Test Plan**

The Test Plan should determine the scope and risks associated to the software maintenance and identify the objectives of testing, the method of testing, the expected time and resources required for the testing process.
It should provide clear information on how the tests are carried out and how to verify the success or failure of each tests.

- **Selection of Test Cases**

Test cases should be selected on the basis of requirements, design specifications, risk analysis and interfaces of the equipment subject to software maintenance.

- **Test Execution**

After the tests have been executed, the results of the executed tests should be recorded, including the versions of the software under tests.

- **Test Results Evaluation**

The results of the executed tests should be discussed and analyzed in order to check which planned software updates can be actually delivered and to confirm that no failure has been detected during the test activities. In case of failure, corrective action should be planned and an updated Test Plan should be issued.

## 7. Failure recovery

7.1 The process of software rollback recovery of paragraph 5.2 should be made available prior to any software maintenances by Service Provider

7.2 The intent of the rollback process is to return the failed state of the system to a previous known stable state.

7.3 The process should consider the implications and any risks associated that could result from the rollback and identify appropriate testing performed post roll back in order to satisfy the administration and class of satisfactory working condition of the system.

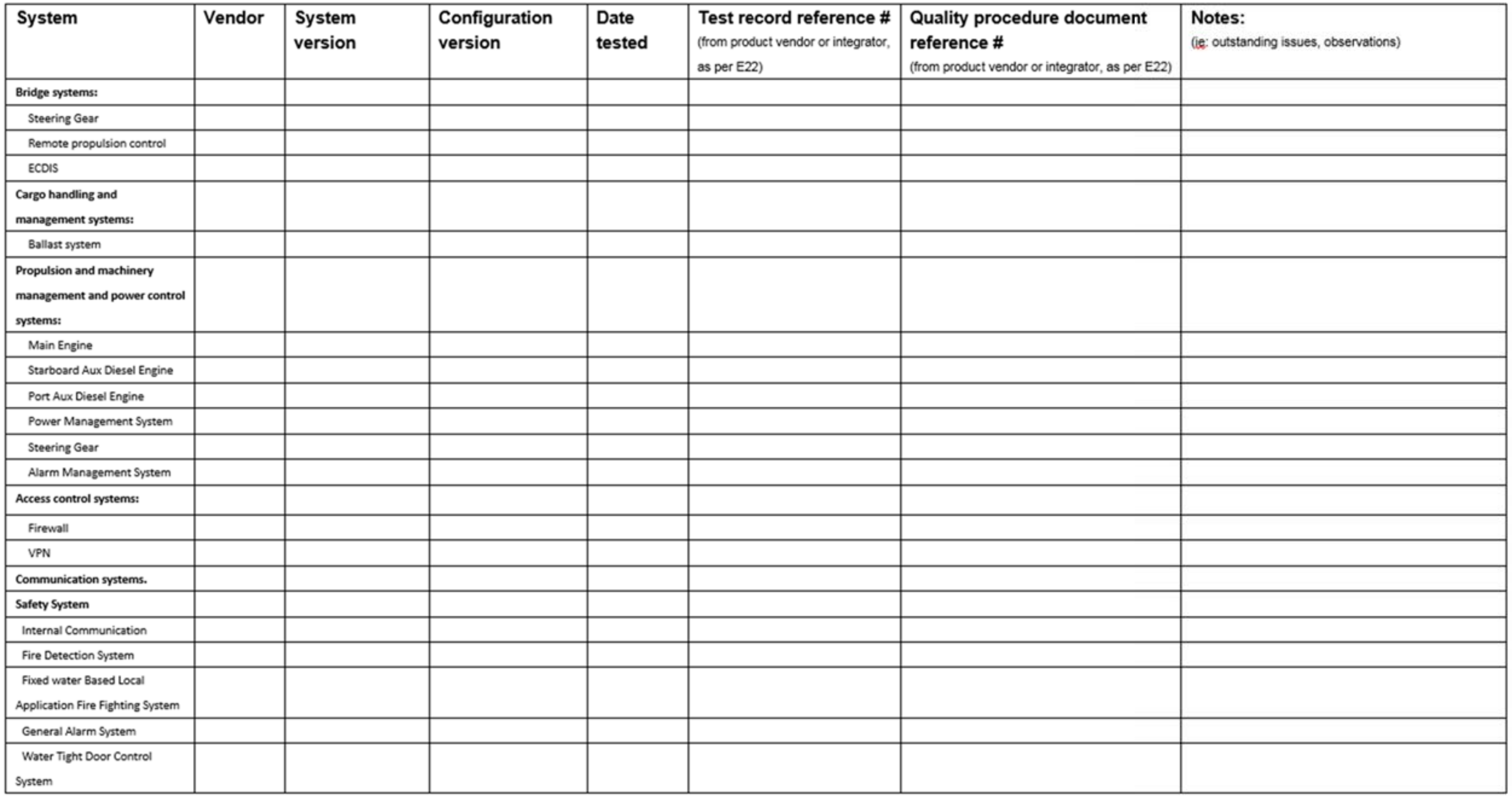
7.4 Rollback procedures should be demonstrated to the classification society when required

7.5 Proposals for alternative solutions should be presented to the classification society.

**Appendix 1:**

**Example template showing a traceable computer based system on board Inventory Matrix.**

Note: this table is not complete and is only an example; the table should list all computer based systems on board essential for the purpose of propulsion, steering and safety.



| **System** | **Vendor** | **System version** | **Configuration version** | **Date tested** | **Test record reference #** (from product vendor or integrator, as per E22) | **Quality procedure document reference #** (from product vendor or integrator, as per E22) | **Notes:** (ie: outstanding issues, observations) |
|---|---|---|---|---|---|---|---|
| **Bridge systems:** | | | | | | | |
| Steering Gear | | | | | | | |
| Remote propulsion control | | | | | | | |
| ECDIS | | | | | | | |
| **Cargo handling and management systems:** | | | | | | | |
| Ballast system | | | | | | | |
| **Propulsion and machinery management and power control systems:** | | | | | | | |
| Main Engine | | | | | | | |
| Starboard Aux Diesel Engine | | | | | | | |
| Port Aux Diesel Engine | | | | | | | |
| Power Management System | | | | | | | |
| Steering Gear | | | | | | | |
| Alarm Management System | | | | | | | |
| **Access control systems:** | | | | | | | |
| Firewall | | | | | | | |
| VPN | | | | | | | |
| **Communication systems.** | | | | | | | |
| **Safety System** | | | | | | | |
| Internal Communication | | | | | | | |
| Fire Detection System | | | | | | | |
| Fixed water Based Local Application Fire Fighting System | | | | | | | |
| General Alarm System | | | | | | | |
| Water Tight Door Control System | | | | | | | |

**Appendix 2:**

**Definitions**

**Data Provider:** The stakeholder that supplies data necessary for the functioning of the computer based system on board.

**System Integrator:** The stakeholder that combines shipboard equipment into an integrated system.

**Service Provider:** The stakeholder that performs the software maintenance.

**Controlled network:** Shipboard network that has been designed to operate such that it does not pose an unacceptable safety or security risks to connected network nodes.

**Integrated system:** Interconnected system combining a number of interacting computer based system on board organized to achieve one or more specified purposes

**Removable media/storage devices:** Portable equipment used during software maintenance.

**Category of maintenance:** Classification assigned to a software maintenance based upon the reason for undertaking the maintenance, which may be:

- Bug Fix (resolving software bugs);
- Feature Release (adding additional functionality);
- Compliance Update (maintaining conformity with regulations);
- *Security Update (protecting against cyber threats);*
- *Obsolescence Update (addressing software and/or hardware that is no longer supported).*

Or some combination of the five.

**Test Case:** Set of conditions, methods and expected results under which a tester will determine whether a software application is working according to the design specifications or not.

End of
Document