Cyber-enabled ships

ShipRight procedure assignment for cyber descriptive notes for autonomous & remote access ships

A Lloyd’s Register guidance document

Version 2.0, December 2017
Foreword

This update of the Lloyd's Register (LR) cyber-enabled ShipRight procedure incorporates the experience gained from our involvement in a number of cyber-enabled ship projects, thus increasing clarity for readers.

In addition to autonomous operation, remote operation is now declared explicitly.

Cyber-enablement is now clearly framed within the context of engineering systems and the equipment located on board the vessel, but accessible using Information Technology (IT) remotely from the vessel.

Also added is the description of the descriptive notes related to cyber security.
## Contents

1. **Cyber enabled ships**  
   1.1 Introduction  

2. **Cyber descriptive notes**  
   2.1 Cyber descriptive notes  
   2.2 Assignment of cyber descriptive notes  
   2.3 Scope of cyber descriptive notes  
      2.3.1 Cyber functionality  
      2.3.1.1 Cyber SAFE  
      2.3.1.2 Cyber MAINTAIN  
      2.3.1.3 Cyber PERFORM  
      2.3.1.4 Cyber SECURE  
      2.3.2 Cyber assessment  
      2.3.2.1 Cyber accessibility levels (AL) for autonomous/remote access  
   2.4 Examples of cyber descriptive notes  

3. **Cyber assessment process**  
   3.1 Risk based design (RBD) assessment  
   3.2 Supporting information  

4. **Design and safety statement**  
   4.1 RBD assessment process stage one  
   4.2 Concept of operations  
   4.3 Context of use  
   4.4 System operational concept  
   4.5 Cyber functionality  
      4.5.1 Systems  
   4.6 Cyber assessment  
      4.6.1 Accessibility Levels for autonomy/remote access  
      4.6.2 Security  

5. **Risk assessment**  
   5.1 RBD assessment process stage two  
   5.2 Human interaction considerations  
      5.2.1 Scope  
      5.2.2 Goals  
      5.2.3 Function  
      5.2.4 Performance  
   5.3 Data quality considerations  
      5.3.1 Scope  
      5.3.2 Goals
5.3.3 Functions
5.3.3.1 Performance

5.4 Systems architecture considerations 13
5.4.1 Scope 13
5.4.2 Goals 13
5.4.3 Function 13
5.4.4 Performance 13

5.5 Hardware considerations 14
5.5.1 Scope 14
5.5.2 Goals 14
5.5.3 Function 14
5.5.4 Performance 14

5.6 Software considerations 14
5.6.1 Scope 14
5.6.2 Goals 14
5.6.3 Function 14
5.6.4 Performance 15

5.7 Communication network considerations 15
5.7.1 Scope 15
5.7.2 Goals 15
5.7.3 Function 15
5.7.4 Performance 15

5.8 Security considerations 16
5.8.1 Scope 16
5.8.2 Goals 16
5.8.3 Function 16
5.8.4 Performance 16

5.9 System integration considerations 17
5.9.1 Scope 17
5.9.2 Goals 17
5.9.3 Function 17
5.9.4 Performance 17

5.10 Configuration management considerations 18
5.10.1 Scope 18
5.10.2 Goals 18
5.10.3 Function 18
5.10.4 Performance 18

6. Revision and supporting studies 19
6.1 RBD assessment process stage three 19
7. Final design assessment
   7.1 RBD assessment process stage four

Appendix A
Appendix B
1. Cyber enabled ships

1.1 Introduction

This procedure details LR’s process for the assessment of cyber-enabled systems on board vessels classed by LR.

For the purposes of this document, ‘cyber-enabled systems’ are considered to be systems installed on board ships that would conventionally be controlled by the ship’s crew but which, through recent advances in IT and Operational Technology (OT), now include the capability to be monitored, or monitored and controlled, either remotely or autonomously with or without a crew on board the ship.

Also for the purposes of this document, in the context of ‘autonomous/remote monitoring and control’, ‘control’ means any changes to operating parameters, set points, software, etc. that have either a direct effect on the ship’s operation (e.g. changes to heading, speed, cargo-loading rate) or an indirect effect on the ship’s operation (e.g. changes to navigational charts, equipment settings, software versions).

Again for the purposes of this document, ‘ship’s crew’ means suitably certified staff physically located on board the ship, according to the ship’s Minimum Safe Manning Certificate and in accordance with the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW).

The functionality provided by cyber-enabled systems can range from simple remote monitoring with a crew on board through to a fully autonomous vessel without a crew on board. Consequently, as the risks can vary considerably, the assessment of cyber-enabled systems requires a risk-based approach to identify the hazards introduced by cyber-enablement and to mitigate the associated risks.
2. **Cyber descriptive notes**

2.1 **Cyber descriptive notes**

The cyber descriptive notes have the following format:

<table>
<thead>
<tr>
<th>Cyber</th>
<th>Scope of cyber functionality</th>
<th>Scope of cyber assessment</th>
<th>(Scope of cyber enabled systems)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identifies the scope of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>cyber enabled system(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Identifies the scope of cyber</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>assessment carried out (see 2.4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Indicates that one or more of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ship's system(s) are</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>cyber enabled and assessed by LR (see 2.2)</td>
</tr>
</tbody>
</table>

2.2 **Assignment of cyber descriptive notes**

The assignment of the cyber descriptive notes indicates that systems on board are cyber-enabled and have been assessed in accordance with this ShipRight procedure. The descriptive notes indicate both the scope of the cyber functionality provided and the scope of the assessment carried out.

While the ShipRight assessment takes account of any functionality provided by systems that are external to the ship, it does not verify their design and construction as part of the ShipRight assessment, unless specifically stated or exceptionally agreed prior to assessment. Similarly, it should also be noted that operational matters such as personnel training and competence, either on board or on shore, are not part of the ShipRight assessment unless specifically stated or exceptionally agreed prior to assessment.

2.3 **Scope of cyber descriptive notes**

The cyber descriptive notes indicate the following functionality:

2.3.1 **Cyber functionality**

2.3.1.1 **Cyber SAFE**

The Cyber SAFE descriptive note indicates that systems essential for the operation of the ship that have remote access to onboard operational data for the purposes of monitoring, analysis, decision making and control have been assessed in accordance with this ShipRight procedure. Monitoring, analysis, decision making and control may be performed remotely by humans or autonomously by systems located on board the ship or located ashore.

*Important notes:*

- Assignment of the Cyber SAFE descriptive note requires that the affected systems satisfy all relevant Rules and Regulations.
- Assignment of the Cyber SAFE descriptive note also requires assignment of Cyber SECURE.

2.3.1.2 **Cyber MAINTAIN**

The Cyber MAINTAIN descriptive note indicates that systems for maintenance of the ship that have remote access to onboard condition data for the purposes of monitoring, analysis, decision making and
adjustment have been assessed in accordance with this ShipRight procedure. Monitoring, analysis, decision making and adjustment may be performed remotely by humans or autonomously by systems located on board the ship or located ashore.

**Important notes:**
- Assignment of the Cyber MAINTAIN descriptive note does not indicate that condition data will be accepted by LR as an alternative to a physical survey on board, unless the additional requirements of LR's ShipRight Procedures for Machinery Planned Maintenance and Condition Monitoring are also satisfied and the ShipRight MCM or MCBM descriptive note is assigned.
- Assignment of the Cyber MAINTAIN descriptive note requires that the affected systems satisfy all relevant Rules and Regulations.
- Assignment of the Cyber MAINTAIN descriptive note also requires assignment of the Cyber SECURE descriptive note.

### 2.3.1.3 Cyber PERFORM
The Cyber PERFORM descriptive note indicates that systems for optimisation of the ship that have remote access to onboard performance data for the purposes of monitoring, analysis, decision making and adjustment have been assessed in accordance with this ShipRight procedure. Monitoring, analysis, decision making and adjustment may be performed remotely by humans or autonomously by systems located on board the ship or located ashore.

**Important notes:**
- Assignment of the Cyber PERFORM descriptive note requires that the affected systems satisfy all relevant Rules and Regulations.
- Assignment of the Cyber PERFORM descriptive note also requires assignment of the Cyber SECURE descriptive note.

### 2.3.1.4 Cyber SECURE
The Cyber SECURE descriptive note indicates that the security of the systems that have remote access have been assessed by LR. The Cyber SECURE descriptive note may be assigned to systems with or without the Cyber SAFE, MAINTAIN or PERFORM descriptive notes.

**Important notes:**
- The Cyber SECURE descriptive note must be assigned whenever a Cyber SAFE, Cyber MAINTAIN or Cyber PERFORM descriptive note is assigned.

### 2.3.2 Cyber assessment
The cyber descriptive note indicates the following scope of cyber assessment:

#### 2.3.2.1 Cyber accessibility levels (AL) for autonomous/remote access

<table>
<thead>
<tr>
<th>AL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL0</td>
<td>No cyber access – no assessment – no descriptive note – included for information only.</td>
</tr>
<tr>
<td>AL1</td>
<td>Manual cyber access – no assessment – no descriptive note – included for information only.</td>
</tr>
<tr>
<td>AL2</td>
<td>Cyber access for autonomous/remote monitoring.</td>
</tr>
<tr>
<td>AL3</td>
<td>Cyber access for autonomous/remote monitoring and control (onboard permission is required, onboard override is possible).</td>
</tr>
<tr>
<td>AL4</td>
<td>Cyber access for autonomous/remote monitoring and control (onboard permission is not required, onboard override is possible).</td>
</tr>
<tr>
<td>AL5</td>
<td>Cyber access for autonomous/remote monitoring and control (onboard permission is not required, onboard override is not possible).</td>
</tr>
</tbody>
</table>
Examples of cyber descriptive notes

An example of the Cyber SAFE descriptive note is as follows:

Cyber SAFAL2 (Propulsion)

- Propulsion system cyber-enabled
- Cyber access for autonomous/remote monitoring assessed
- Cyber access of systems providing essential operational functions provided

One or more of the ship's system(s) are cyber-enabled and assessed by LR

An example of the Cyber MAINTAIN descriptive note is as follows:

Cyber MAINTAINAL3 (HVAC)

- HVAC system cyber-enabled
- Cyber access for remote or autonomous monitoring and adjustment (onboard override is possible) assessed
- Cyber access of systems providing maintenance functions provided

One or more of the ship's system(s) are cyber enabled and assessed by LR

In this example, changes to machinery and equipment settings made remotely by humans or autonomously by systems located on board the ship or located ashore require the prior approval of the crew. The changes can be overridden by the ship's crew.

An example of the Cyber PERFORM descriptive note is as follows:

Cyber PERFORMAL4 (Trim)

- Trim system cyber-enabled
- Cyber access for autonomous/remote monitoring and adjustment (onboard override is possible) assessed
- Cyber access of systems providing optimisation functions provided

One or more of the ship's system(s) are cyber-enabled and assessed by LR

In this example, changes to machinery and equipment settings made remotely by humans or autonomously by systems located on board the ship or located ashore do not require the prior approval of the crew. The changes can be overridden by the ship's crew at any time.
An example of the Cyber descriptive note is as follows:

**Cyber Secure** *(Navigation system)*

- Navigation system cyber enabled
- Cyber security arrangements in design and construction assessed
- One or more of the ship’s system(s) are cyber enabled and assessed by LR

Example of combined Cyber descriptive notes is as follows:

**Cyber AL2 Safe Secure** *(Steering)*

- Steering system cyber enabled
- Cyber security of cyber enabled systems assessed
- Cyber access of systems providing optimisation functions assessed
- Cyber access for remote or autonomous monitoring provided
- One or more of the ship’s system(s) are cyber enabled and assessed by LR
3. Cyber assessment process

3.1 Risk based design (RBD) assessment

Cyber assessment follows LR’s ShipRight additional design procedure, risk based design (RBD).

Figure 1 – generic process for risk based designs
3.2 Supporting information

Each of the four RBD phases should be informed by the information in the following table.

<table>
<thead>
<tr>
<th>Design and safety statement</th>
<th>Risk assessment</th>
<th>Revision and supporting studies</th>
<th>Final design assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity:</td>
<td>Activity:</td>
<td>Activity:</td>
<td>Activity:</td>
</tr>
<tr>
<td>ShipRight procedure - Risk Based Designs:</td>
<td>ShipRight procedure - Risk Based Designs:</td>
<td>ShipRight procedure - Risk Based Designs:</td>
<td>ShipRight procedure - Risk Based Designs:</td>
</tr>
<tr>
<td>– Section 4.2. Stage one appraisal, design and safety statement</td>
<td>– Section 4.3. Stage two appraisal, risk assessment</td>
<td>– Section 4.4. Stage three appraisal, revision and supporting studies</td>
<td>– Section 5. Stage four appraisal, final design assessment</td>
</tr>
</tbody>
</table>

Informed by:
ShipRight Procedure – Cyber-Enabled Ships, Procedure for Assignment of Cyber Descriptive Notes (this document):
– Section 4.2 Concept of operation
– Section 4.3 Context of use
– Section 4.4 System operational concept
– Section 4.5 Cyber functionality
– Section 4.6 Cyber assessment

Informed by:
ShipRight Procedure – Cyber-Enabled Ships, Procedure for Assignment of Cyber Descriptive Notes (this document):
– Section 4.2.9 Stage one appraisal report

Informed by:
ShipRight Procedure – Cyber-Enabled Ships, Procedure for Assignment of Cyber Descriptive Notes (this document):
– Section 5.2 human interaction considerations
– Section 5.3 data quality considerations
– Section 5.4 system architecture considerations
– Section 5.5 hardware considerations
– Section 5.6 software considerations
– Section 5.7 communication network considerations
– Section 5.8 security considerations
– Section 5.9 system integration considerations
– Section 5.10 configuration management considerations

Informed by:
ShipRight Procedure – Risk Based Designs:
– Section 4.3.13 Stage two appraisal report

Informed by:
ShipRight Procedure – Risk Based Designs:
– Section 4.4.8 revised stage two appraisal report
– annex B evidence to be submitted
4. **Design and safety statement**

4.1 **RBD assessment process stage one**

In addition to the information to be included in the design and safety statement required by stage one of the RBD assessment process, the design and safety statement is also to take account of the considerations identified in this section.

4.2 **Concept of operations**

The concept of operations should establish the intentions for the operation of the ship under normal and reasonably foreseeable abnormal conditions.

The concept of operations should consider:

- Stakeholder requirements (including the owner, operator, ship’s crew on board, remote operators, etc.).
- Operational requirements e.g. operational speeds, wave heights, displacements, service area, temperatures, motions, aircraft and boat operations; arrangements under reasonably foreseeable, normal and abnormal conditions.
- System requirements, including the architecture needed for the operational performance and function.
- Statutory and classification requirements for vessel operations.
- Relevant physical, social and organisational environment characteristics.

4.3 **Context of use**

The context of use should establish how the ship’s crew, remote operators, maintainers and others are expected to interact with the cyber-enabled systems both on board the ship and ashore.

The context of use should consider the following.

- The goals of the users and the overall goals of the cyber-enablement should be identified.
- All the possible users and their interactions with the proposed cyber-enabled engineering systems/equipment should be identified and may be described in terms of goals and constraints. For example, suitably certified onboard staff, remote operators, maintenance personnel and crew.
- User group characteristics should be identified, including their required capabilities and limitations.
- The characteristics of tasks that can influence usability and accessibility for autonomy/remote access should be described; if there is a risk that the task might be completed incorrectly, this should be identified.
- Any potential adverse consequences for performance, safety and security should be identified.
- The tasks should be identified – this should include descriptions of what the user does, not only in terms of the functions or features provided by the cyber-enabled engineering systems/equipment.
- The technical environment, including the hardware, software and materials, should be identified.
- The relevant characteristics of the physical, social and organisational environment should be described – for example, the work environment both on and off the vessel, where users will interact with the cyber-enablement, and the organisational management policies and procedures that will enable users to be suitably qualified and experienced for their required tasks, including training.
Cyber-enabled ships

4.4 System operational concept
The system operational concept should describe how the cyber-enabled systems will deliver the intended operation of the ship.

The system operational concept should consider the following.

- How system architecture, configuration and criticality meet the requirements of the operational scenarios established by the concept of operations (see 4.2).
- The interaction of the ship’s crew, remote operators, maintainers and others with the cyber-enabled systems (see 4.3).

4.5 Cyber functionality

4.5.1 Systems
The systems on board the ship to be assessed should be established and categorised according to the descriptive note categorisations detailed in the table below.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAFE</td>
<td>Systems providing functions essential for the operation of the ship.</td>
</tr>
<tr>
<td>MAINTAIN</td>
<td>Systems providing functions for the maintenance of the ship.</td>
</tr>
<tr>
<td>PERFORM</td>
<td>Systems providing functions for the optimisation of the ship.</td>
</tr>
<tr>
<td>SECURE</td>
<td>Systems providing functions for the security of the ship.</td>
</tr>
</tbody>
</table>

4.6 Cyber assessment

4.6.1 Accessibility Levels for autonomy/remote access
The intended level of cyber access to be provided should be established and categorised according to the descriptive note categorisations, as detailed in the table below.

<table>
<thead>
<tr>
<th>Accessibility level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL0</td>
<td>No access – no assessment – no descriptive note – for information only</td>
</tr>
<tr>
<td>AL1</td>
<td>Manual access – no assessment – no descriptive note – for information only</td>
</tr>
<tr>
<td>AL2</td>
<td>Cyber access for autonomous/remote monitoring</td>
</tr>
<tr>
<td></td>
<td>Access for autonomous/remote monitoring of the ship’s systems is provided and has been assessed. Autonomous/remote monitoring of the ship’s systems, using internet or radio frequency (RF) connection, is enabled and possible without the physical intervention of the ship’s crew. Autonomous monitoring may be from systems located on board the ship or ashore. Control of the ship’s systems (e.g. changes to operational parameters, software, machinery set points, etc.) is not enabled.</td>
</tr>
<tr>
<td>AL3</td>
<td>Cyber access for autonomous/remote monitoring and control (onboard permission is required, onboard override is possible)</td>
</tr>
<tr>
<td></td>
<td>Access for autonomous/remote monitoring and control of the ship’s systems is provided and has been assessed. Autonomous/remote monitoring and control of the ship’s systems, using internet or RF connection, is enabled and possible. Autonomous monitoring and control may be from systems located on board the ship or ashore. Control of the ship’s systems (e.g. changes to operational parameters, software, set points, etc.) is enabled but only possible with the permission of the ship’s crew on board. Override of autonomous/remote control by the ship’s crew is possible.</td>
</tr>
<tr>
<td>Accessibility level</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| AL4                 | Cyber access for autonomous/remote monitoring and control (onboard permission is not required, onboard override is possible)  
Access for autonomous/remote monitoring and control of the ship’s systems is provided and has been assessed. Autonomous/remote monitoring and control of the ship’s systems, using internet or RF connection, is enabled and possible. Autonomous monitoring and control may be from systems located on board the ship or ashore. Control of the ship’s systems (e.g. changes to operational parameters, software, set points, etc.) is enabled and possible without the permission of the ship’s crew on board. Override of autonomous/remote control by the ship’s crew is possible. |
| AL5                 | Cyber access for autonomous/remote monitoring and control (onboard permission is not required, onboard override is not possible)  
Access for autonomous/remote monitoring and control of the ship’s systems is provided and has been assessed. Autonomous/remote monitoring and control of the ship’s systems, using internet or RF connection, is enabled and possible. Autonomous monitoring and control may be from systems located on board the ship or ashore. Control of the ship’s systems (e.g. changes to operational parameters, software, set points, etc.) is enabled and possible without the permission of the ship’s crew on board. Override of autonomous/remote control by the ship’s crew is not possible. |

4.6.2 Security
Cyber security to be provided should be established according to the descriptive note below.

Cyber SECURE
Cyber security in design and construction

An appropriate cyber security governance system is in place to mitigate the risk of introducing vulnerabilities to cyber-attack, or other unauthorised access, during the design, procurement, construction and installation of the cyber-enabled systems.
5. Risk assessment

5.1 RBD assessment process stage two

In addition to the consideration of the information included in the design and safety statement of the assessment process, the risk assessment required by stage 2 of the RBD assessment process is also to take account of the considerations identified in this section.

5.2 Human interaction considerations

5.2.1 Scope
Crew and shore staff interfaces with systems providing cyber-enabled functions.

5.2.2 Goals
User interaction with equipment and systems should be designed to take account of the expectations placed on the users in terms of roles, location and competence.

5.2.3 Function
Functional considerations include the following:

− The presentation of alarms and warnings, and the design of control stations and their environment, should meet the requirements of existing Rules.

− User interfaces should be sufficiently usable to meet requirements for situational awareness, safe monitoring and control under normal and foreseeably abnormal modes of operation.

− Information presented to the ship’s crew or shore staff should be displayed in a suitable format and at a rate that allows sufficient situational awareness to support safe decision making.

− Alerts presented for the complete installation under autonomous/remote control should be clearly distinguishable and categorised according to the urgency and type of response required by both the ship’s crew and shore staff.

− Interaction with equipment and systems should support the ship’s crew and shore staff in using systems, maintaining security, and diagnosing failures and other problems, taking account of any necessary changes required in responsibilities or competence.

− Training for crew and shore staff should include the competence necessary to meet identified responsibilities, as specified in the System Operational Concept.

− Human interactions should take account of the intended Concept of Operations, Context of Use and System Operational Concept (see Chapter 4).

5.2.4 Performance
Performance considerations include the following:

− Review the Context of Use for mental and physical capabilities, needs and limitations of the ship’s crew or shore staff that might affect safety. Typical factors include location, native language, fatigue, distraction, knowledge, culture, personal protective equipment (PPE) and posture.

− For higher accessibility levels, the development process should implement the principles and activities of human-centred design to identify and mitigate risks arising from crew or shore staff use, or reasonably foreseeable misuse, of the cyber-enabled ship or system. These principles and activities are defined in (for example) ISO 9241-210 and elaborated on in LR’s human-centred design guides. They include the involvement of crew and shore staff in design activities.

− Human-centred design should be used to identify and mitigate risk compensation (misuse of performance gains from automation), automation bias (advice provided autonomously/remote is not questioned by users), moral buffering (remoteness or algorithms justifying unethical behaviour) and affect dilemma (attributing personality to automation).

− Descriptions of alerts and presentation of information should be sufficiently understandable to give crew and shore staff adequate situational awareness to control all cyber-enabled functions.
The ship’s crew (if present) or shore-based operators shall be able to bring the ship or system to a safe state in the event of an undesirable situation arising.

User requirements derived from the analysis of the Context of Use should be specified in the Concept of Operations.

The cumulative effect of all the changes specified in the System Operational Concept on the safe performance of crew and shore staff should be assessed and taken into account in the design of interfaces and training.

Shore staff making judgements related to operations should be competent and have access to information that is at least equivalent to that of the crew on the ship.

The roles and competence of the ship’s crew and shore staff need to take account of new or changed responsibilities, as described in the System Operational Concept.

The operation of the ship should be monitored to ensure that the human component of the cyber systems is performing safely and securely and that adequate maintenance is being carried out.

Risks arising from differences between the operational Context of Use and the Context of Use used as the basis of the design and award of notation should be reassessed whenever there is a change.

5.3 Data quality considerations

5.3.1 Scope
Data acquired for the purposes of remote or autonomous monitoring and control.

5.3.2 Goals
Data quality should be appropriate for the intended cyber-enabled functions.

5.3.3 Functions
Functional considerations include the following.

- Essential data quality attributes should be defined.
- Data quality should be appropriate for the intended AL and functionality (SAFE, MAINTAIN, PERFORM), both during normal operation and in reasonably foreseeable abnormal conditions.
- Data quality requirements should take account of the intended Concept of Operations, Context of Use and System Operational Concept (see Chapter 4).

5.3.3.1 Performance
Performance considerations include:

- Data integrity, considering the intended application of the data and the consequences of any degradation in data’s integrity as a result of any alterations or the partial or total loss or corruption of data.
- Data availability, considering the intended access and functionality for both normal operation and reasonably foreseeable abnormal operation, taking account of transmission delays, available bandwidth and prioritisation of usage; the relative timeliness of different data upon which decisions are made; malicious attempts to interrupt data; and strategies for managing situations where data availability is limited, including architectural or detailed design solutions such as redundancy of communication channels, manual intervention or automated operation.
- Data authentication, considering the legitimacy of the data received from external systems; the correct timing and sequence of data; secure protocols for data transmission and advanced identification techniques; and methods that seek to validate sources of information.
- Data confidentiality, considering data stored and externally transmitted; physical security; system, equipment or component maintenance; and decommissioning of systems or components.
- Data access, considering requirements for access according to the intended access and functionality for both normal operation and reasonably foreseeable abnormal operation; renewal intervals and
Cyber-enabled ships

ShipRight procedure for assignment cyber descriptive notes for autonomous/remote access ships

− Data ownership, considering roles and responsibilities (who can do what to the data); processing authorisations and permissions (what can be done to the data); changes in data ownership as a result of processing, aggregation, or transmission using internal systems on the vessel; changes in data ownership as a result of processing, aggregation, or transmission between internal systems and external systems; and the implications of the expiry of the manufacturer’s warranty.

− Data storage, considering how and where the data is stored and processed, including physical location (e.g. private or public cloud); accessibility and monitoring; data storage solutions based on threat and vulnerability analysis and mitigations; legal jurisdiction and any associated obligations in relation to cloud-based data storage, statutory and classification requirements for data access and storage duration; and the preservation of safety-related data.

5.4 Systems architecture considerations

5.4.1 Scope
On-ship and off-ship architecture of systems providing cyber-enabled functions.

5.4.2 Goals
System architecture should provide for cyber-enabled functions which are dependable.

5.4.3 Function
Functional considerations include the following.

− System architecture should ensure that the reliability, availability, maintainability, safety and security of the system is appropriate for the intended AL and functionality (SAFE, MAINTAIN, PERFORM).

− System architecture requirements should take account of the intended Concept of Operations, Context of Use and System Operational Concept (see Chapter 4).

− System architecture should be resilient to reasonably foreseen interference, degradation and faults, both during normal operation and during reasonably foreseeable abnormal conditions.

5.4.4 Performance
Performance considerations include the following.

− The reliability, availability, maintainability, safety and security intentions should be established, either quantitatively or qualitatively, and should be appropriate for the intended access for both normal operation and in defined abnormal conditions.

− The system architecture should be designed in accordance with established Rules, Codes, standards and practices, as considered appropriate for the required reliability, availability, maintainability, safety and security intentions.

− The boundaries of the system should be identified and should include the sub-systems, equipment and components located both on board the ship and off the ship.

− The sub-systems, equipment and components should be identified and their interfaces and interdependencies established.

− The reliability, availability, maintainability, safety and security of the system should be validated, taking account of the requirements of the Concept of Operations, Context of Use and system.
5.5 Hardware considerations

5.5.1 Scope
Equipment and components of systems providing cyber-enabled functions.

5.5.2 Goals
Equipment and components should be dependable.

5.5.3 Function
Functional considerations include the following.
− Equipment and components should be sufficiently reliable, available, maintainable, safe and secure.
− Equipment and components should be suitable for their intended environment.
− Equipment and component requirements should take account of the intended Concept of Operations, Context of Use and System Operational Concept (see Chapter 4).

5.5.4 Performance
Performance considerations include the following.
− The required reliability, availability, maintainability, safety and security intentions should be established for the equipment and components according to the system performance requirements.
− The operating environment in which the equipment or components are intended to operate should be established for equipment or components both on board the ship and off the ship.
− Equipment and components should be designed in accordance with established Rules, Codes, standards and practices, as considered appropriate for the required performance and intended operating environment.

5.6 Software considerations

5.6.1 Scope
Software in systems providing cyber-enabled functions.

5.6.2 Goals
Software should provide for, and should not compromise, the ability of cyber-enabled systems to operate correctly under normal and reasonably foreseeable abnormal conditions.

5.6.3 Function
Functional considerations include the following.
− Software integrity should be appropriate for the intended AL and functionality (SAFE, MAINTAIN, PERFORM), both during normal operation and during reasonably foreseeable abnormal conditions.
− Software integrity requirements should take account of the intended Concept of Operations, Context of Use and System Operational Concept (see Chapter 4).
− Risks arising from the use of software should be established and managed.
− Software used for the mitigation of identified safety hazards (Relevant Hazards) should be identified and follow an appropriate development process.
5.6.4 Performance
Performance considerations include the following.

- Software lifecycle activities should satisfy the established Rules, Codes, standards and practices considered appropriate for the required performance.
- Software used for the mitigation of identified hazards – Relevant Hazards – should be developed in accordance with the established Rules, Codes, standards and practices considered appropriate to the risk.
- Relevant Hazards should be identified using appropriate risk assessment techniques and corresponding Relevant Hazard Requirements for the software established.
- Software should be considered regardless of the device on which it is stored or executed, whether it is designed to have user interaction or not and whether it is on board or within the shore-based centre. The boundaries of the system with which it is associated should be defined.
- Non-deterministic, machine-learning or artificial-intelligence software should be identified and evidence should be provided to demonstrate that it could not affect the safe operation of the ship.

5.7 Communication network considerations

5.7.1 Scope
On-ship and off-ship communication networks, their systems, equipment and components providing cyber-enabled functions.

5.7.2 Goals
Communication networks should provide for sufficient and dependable data transfer between the ship and the remote systems.

5.7.3 Function
Functional considerations include the following.

- Communication network capacity, reliability, availability, maintainability, safety and security should be appropriate for the intended AL and functionality (SAFE, MAINTAIN, PERFORM), both during normal operation and during reasonably foreseeable abnormal conditions.
- Communication network performance requirements should take account of the intended Concept of Operations, Context of Use and System Operational Concept (see Chapter 4).
- Communication network performance should take account of the variability and vulnerability of wireless data communications, private data communications and public data communications networks utilised.

5.7.4 Performance
Performance considerations include the following.

- The required communication network capacity, reliability, availability, maintainability, safety and security performance should be established and appropriate for the intended access and functionality.
- The required communication network capacity, reliability, availability, maintainability, safety and security performance should consider both normal and defined abnormal conditions.
- The communication network architecture should satisfy the established Rules, Codes, standards and practices considered appropriate for the required performance.
- The communication network architecture should provide for sufficient resilience to interference, degradation and failures.
The impact of deterioration or a complete loss of wireless communications as a result of variations in natural phenomena (e.g. atmospheric conditions, loss of coverage, shadows) and man-made phenomena (e.g. electromagnetic interference) should be considered.

The non-deterministic nature of data communications using public data communication links should be considered.

Communication network routes should be identified according to the AL and functionality they provide.

The communication network routes to and from the ship should be defined in terms of satellite communications, WiFi connections and VHF radio links, and should include all beginning and end points such as navigation systems, power management systems, engine controllers, hotel services, remote shore stations, mobile access points, etc.

5.8 Security considerations

5.8.1 Scope
Systems, equipment, components and procedures providing cyber-enabled functions.

5.8.2 Goals
Systems providing cyber-enabled functions should be protected against cyber-attack or unauthorised access.

5.8.3 Function
Functional considerations include the following.

The system security measures should not cause deterioration in functions required for safety.

Security arrangements should be appropriate for the intended AL and functionality (SAFE, MAINTAIN, PERFORM), both during normal operation and during reasonably foreseeable abnormal conditions.

Security requirements should take account of the intended Concept of Operations, Context of Use and System Operational Concept (see Chapter 4).

Security arrangements should take account of the full system lifecycle, including equipment procurement and disposal.

Security arrangements should consider the identification of potential security threats, the protection of the system from such security threats, the detection of security events, the response to such security events and the recovery from such security events.

5.8.4 Performance
Performance considerations include the following.

The required system security performance should be established and appropriate for the intended access and functionality.

The required system security performance should consider both normal operation and defined abnormal conditions, and should include the impact of failures of the system security on the functions required for safety.

The system security architecture should consider both on-ship and off-ship systems, equipment, components and procedures.

The system security architecture, equipment, components and procedures should satisfy the established Rules, Codes, standards and practices considered appropriate to the required performance.

System security processes and procedures applied should mitigate the risks from cyber threats and vulnerabilities being introduced during the design, procurement, construction, integration and commissioning of the cyber-enabled systems. Considerations should include, but are not limited to,
access control, both physical and cyber; password specification and management; patch management; loss of data; unauthorised modification of data or software; installation of unauthorised software, including malware; control of auto executable program files; unauthorised connections to uncontrolled or insecure networks or devices, including WiFi and near-field communications; and removable external data sources.

- Configuration management should be applied to the system security of the cyber-enabled systems from procurement through to delivery. This should include things such as version control and access control lists.
- The system security measures applied should be documented, kept secure and supplied with the cyber-enabled system.

5.9 System integration considerations

5.9.1 Scope
Integration of systems, sub-systems, equipment and components providing cyber-enabled functions.

5.9.2 Goals
System integration should ensure individual sub-systems, equipment and components of the system and the system as a whole function correctly following integration; this should be the case under both normal and reasonably foreseeable abnormal conditions.

5.9.3 Function
Functional considerations include the following.
- Systems and their sub-systems, equipment and components to be integrated should be clearly defined and compatible.
- Overall responsibility for the integration of sub-systems, equipment and components should be assigned and managed.
- Integration should be carried out in accordance with an agreed and defined procedure that includes verification and validation.

5.9.4 Performance
Performance considerations include the following.
- Interfaces between sub-systems, equipment and components should be clearly identified and include electrical, mechanical, software, data and physical interfaces.
- Interfaces with humans, equipment and components should be identified and verified according to the intended AL and functionality (SAFE, MAINTAIN, PERFORM), both for normal operation and reasonably foreseeable abnormal operation.
- The integration procedure should identify the roles, responsibilities and requirements associated with the integration of the individual sub-systems, equipment and components and their interfaces.
- The integration procedure should define the sequence and stages for integrating individual sub-systems, equipment and components and the points at which verification is to be carried out.
- The integration procedure should verify the correct integration of individual sub-systems, equipment and components and validate the functionality of the system.
- The integration procedure should consider any integration issues critical to the performance of the system.
5.10  Configuration management considerations

5.10.1  Scope
Systems, equipment and components, including hardware, software and operational procedures, providing cyber-enabled functions, both on-ship and off-ship.

5.10.2  Goals
The configuration of systems, equipment and components providing cyber-enabled functions should be controlled and documented throughout the lifecycle.

5.10.3  Function
Functional considerations include the following.
- Changes to items essential to the correct operation of the system that can be expected during the lifetime of the system should be identified and controlled.

5.10.4  Performance
Performance considerations include the following.
- Configuration management procedures should satisfy the established Rules, Codes, standards and practices considered appropriate to the required intentions.
- Changes to configuration controlled items should be identified, evaluated and approved prior to implementation and verified and recorded following implementation.
- Configuration control items include sensors, actuators, instrumentation, IT, OT, software and procedures.
- Configuration management should be active from initial implementation, during the in-service period and through to disposal.
- Configuration management should consider systems both on-ship and off-ship.
6. Revision and supporting studies

6.1 RBD assessment process stage three

See stage three - Lloyd’s Register Risk Based Design (RBD) process, May 2016
7. Final design assessment

7.1 RBD assessment process stage four
See stage three - Lloyd’s Register Risk Based Design (RBD) Process, May 2016
Bibliography

Lloyd’s Register Risk Based Design (RBD) Process, May 2016
ISO 17894: 2005, Ships and marine technology – Computer applications – General principles for the development and use of programmable electronic systems in marine applications
IMO Code on Alerts and Indicators: 2009
Lloyd’s Register Provisional Rules and Regulations for Software to be used in Naval Ships, January 2016
National Institute of Standards and Technology (NIST), V.01 2014, Framework for Improving Critical Infrastructure Cybersecurity
IEC 61162 Series, Maritime navigation and radiocommunication equipment and systems
IEC 62443, Industrial communication networks – Network and system security
United States Coast Guard (USCG) ‘Cyber Strategy’, June 2015
ISO 31010 Risk Assessment Techniques
Allied Naval Engineering Publication (ANEP) 77

Further information and reading
The Human-Centred Approach, A Best Practice Guide for Equipment Manufacturers, sections 4.1 and 4.2.2
IMO MSC Circ. 1512 Guideline on Software Quality Assurance and Human-Centred Design for e-Navigation
ISO 9241-110 Dialogue principles
Appendix A

Definitions

Context of Use
The Context of Use consists of the users’ characteristics (and their associated individual cognitive and physical factors) and their goals and interactions with tasks, stakeholders, physical operating environments (e.g. the work environment where the cyber-enabled system is being used), and social and management environments (e.g. training, the company and its management policies and procedures). The Context of Use appropriately takes into account relevant aspects of socio-technical systems.

Concept of Operations
The concept of operations describes the vessel’s intended service in terms of purpose and function and is to include, but not be limited to, information on the following: crewing, operational speeds, wave heights, displacements, service area, temperatures, motions, and aircraft and bot operations, as well as arrangements under reasonably foreseeable, normal and abnormal conditions.

The Concept of Operations is to be provided by the owner. LR may accept alternative documents where these provide the information that would be included within the Concept of Operations. In such cases, the relevant sections providing the information required to demonstrate equivalence with the Concept of Operations are to be identified.

Cyber-enabled systems
These are systems installed on board ships that would conventionally be controlled by the ship’s crew but which, through recent advances in IT, now include the capability to be monitored, or monitored and controlled, remotely or autonomously with or without a crew on board the ship.

Reasonably foreseeable abnormal condition
An event, incident or failure that has happened and could happen again, has not happened but is considered possible (where the likelihood is considered extremely unlikely or the consequences are trivial, and no further prevention or mitigation action is to be taken, then this is to be justified), or is planned for – for example, emergency actions cover such a situation, or maintenance is undertaken to prevent it.

These conditions should be identified using analysis techniques suitable for revealing abnormal conditions, employing a mix of personnel to apply the processes, including designers, operators who carry out maintenance (with relevant domain knowledge and understanding), and competent safety/risk professionals. They should reference relevant events and historic data and document the results of the analysis.

Relevant Hazard Requirements
These are software requirements that cover how the software mitigates a Relevant Hazard Cause, including, but not limited to,

− specific functional behaviour to mitigate Relevant Hazard Causes, fault indications, accuracy and response times;
− what it must not do; and
− the degree of reliance placed on the achievement of the Relevant Hazard Requirements.

A Relevant Hazard Requirement can be separated into components corresponding to sub-systems, each of which is itself called a Relevant Hazard Requirement.
**System Operational Concept**

A System Operational Concept is a description of the intended operation of each of the major vessel systems, meaning those comprised of sub-systems and equipment referenced within the Rules. The System Operational Concept is to demonstrate that the systems’ architecture, configuration and criticality meet the requirements of the operational scenarios defined by the Concept of Operations.

The System Operational Concept statements are to be agreed between the designer and the owner. LR may accept alternative documents where these provide the information that would be included within the System Operational Concept. In such cases, the relevant sections providing the information required to demonstrate equivalence with the System Operational Concept are to be identified.

**Ship’s crew**

Sufficient and suitably qualified personnel, as required by statutory regulations.
## Appendix B

### Relevant standards and guidance

| Relevant rules, standards and guidance for Cyber SAFE, MAINTAIN and PERFORM |
|---|---|---|---|---|
| **RBD assessment process stage one** (**see 4.1**) | **AL2** | **AL3** | **AL4** | **AL5** |

| **Concept of Operations** (**see 4.2**) | **AL2** | **AL3** | **AL4** | **AL5** |
| Detailed description of how the cyber-enabled functionality will impact on the operation of the ship, compared to the operation of a conventional ship | Detailed description of how the cyber-enabled functionality will impact on the operation of the ship, compared to the operation of a conventional ship | Allied Naval Engineering Publication (ANEP) 77 – Naval Ship Code | Allied Naval Engineering Publication (ANEP) 77 – Naval Ship Code |

| **Context of Use** (**see 4.3**) | **AL2** | **AL3** | **AL4** | **AL5** |
| Detailed description of how the cyber-enabled functionality will impact on the ship’s crew, compared to the crew of a conventional ship | Detailed description of how the cyber-enabled functionality will impact on the ship’s crew, compared to the crew of a conventional ship | Full Context of Use description (**see 4.3**) | Full Context of Use description (**see 4.3**) |

| **System Operational Concept** (**see 4.4**) | **AL2** | **AL3** | **AL4** | **AL5** |
| Detailed description of the cyber-enabled system(s) that will deliver the intended operation of the ship | Detailed description of the cyber-enabled system(s) that will deliver the intended operation of the ship | Full System Operational Concept description (**see 4.4**) | Full System Operational Concept description (**see 4.4**) |

| **Cyber functionality** (**see 4.5**) | **AL2** | **AL3** | **AL4** | **AL5** |
| Details of cyber-enabled system(s) and the functionality they provide, and intended descriptive note(s) to be assigned, including details of the intended accessibility level(s) and details of the intended security level(s) | Details of cyber-enabled system(s) and the functionality they provide, and intended descriptive note(s) to be assigned, including details of the intended accessibility level(s) and details of the intended security level(s) | Details of cyber-enabled system(s) and the functionality they provide, and intended descriptive note(s) to be assigned, including details of the intended accessibility level(s) and details of the intended security level(s) | Details of cyber-enabled system(s) and the functionality they provide, and intended descriptive note(s) to be assigned, including details of the intended accessibility level(s) and details of the intended security level(s) |

| **Cyber assessment** (**see 4.6**) | **AL2** | **AL3** | **AL4** | **AL5** |
| Details of system(s) to be assessed | Details of system(s) to be assessed | Details of system(s) to be assessed | Details of system(s) to be assessed |

<p>| <strong>Risk assessment</strong> (<strong>see 5.1</strong>) | <strong>AL2</strong> | <strong>AL3</strong> | <strong>AL4</strong> | <strong>AL5</strong> |</p>
<table>
<thead>
<tr>
<th>Human interaction considerations (see 5.2)</th>
<th>AL2</th>
<th>AL3</th>
<th>AL4</th>
<th>AL5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules for Ships, Pt6, Ch1, 1.2 Control engineering requirements, General requirements</td>
<td>Rules for Ships, Pt6, Ch1, 1.2 Control engineering requirements, General requirements</td>
<td>ISO 9241-210 Ergonomics of human system interaction, Human centred design for interactive systems</td>
<td>ISO 9241-210 Ergonomics of human system interaction, Human centred design for interactive systems</td>
<td></td>
</tr>
<tr>
<td>Rules for Ships, Pt6, Ch1, 2.3 Control engineering requirements, Essential features for control, alarm and safety systems</td>
<td>Rules for Ships, Pt6, Ch1, 2.3 Control engineering requirements, Essential features for control, alarm and safety systems</td>
<td>Details relating to the mitigation of risks identified by the risk assessment required by 5.1 RBD assessment process stage two</td>
<td>Details relating to the mitigation of risks identified by the risk assessment required by 5.1 RBD assessment process stage two</td>
<td></td>
</tr>
<tr>
<td>Rules for Ships, Pt6, Ch1, 3 Control engineering requirements, Ergonomics of control stations</td>
<td>Rules for Ships, Pt6, Ch1, 3 Control engineering requirements, Ergonomics of control stations</td>
<td>Details relating to the mitigation of risks identified by the risk assessment required by 5.1 RBD assessment process stage two</td>
<td>Details relating to the mitigation of risks identified by the risk assessment required by 5.1 RBD assessment process stage two</td>
<td></td>
</tr>
<tr>
<td>Details relating to the mitigation of risks identified by the risk assessment required by 5.1 RBD assessment process stage two</td>
<td>Details relating to the mitigation of risks identified by the risk assessment required by 5.1 RBD assessment process stage two</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data quality considerations (see 5.3)</th>
<th>AL2</th>
<th>AL3</th>
<th>AL4</th>
<th>AL5</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>System architecture considerations (see 5.4)</th>
<th>AL2</th>
<th>AL3</th>
<th>AL4</th>
<th>AL5</th>
</tr>
</thead>
<tbody>
<tr>
<td>To be established on a project by project basis</td>
<td>To be established on a project by project basis</td>
<td>To be established on a project by project basis</td>
<td>To be established on a project by project basis</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hardware considerations (see 5.5)</th>
<th>AL2</th>
<th>AL3</th>
<th>AL4</th>
<th>AL5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules for Ships, Pt6, Ch1, 1 Control engineering requirements, General requirements</td>
<td>Rules for Ships, Pt6, Ch1, 1 Control engineering requirements, General requirements</td>
<td>Rules for Ships, Pt6, Ch1, 1 Control engineering requirements, General requirements</td>
<td>Rules for Ships, Pt6, Ch1, 1 Control engineering requirements, General requirements</td>
<td></td>
</tr>
<tr>
<td>Rules for Ships, Pt6, Ch1, 2 Control engineering requirements, Essential features for control, alarm and safety systems</td>
<td>Rules for Ships, Pt6, Ch1, 2 Control engineering requirements, Essential features for control, alarm and safety systems</td>
<td>Rules for Ships, Pt6, Ch1, 2 Control engineering requirements, Essential features for control, alarm and safety systems</td>
<td>Rules for Ships, Pt6, Ch1, 2 Control engineering requirements, Essential features for control, alarm and safety systems</td>
<td></td>
</tr>
</tbody>
</table>

Data quality considerations (see 5.3) | ISO/IEC 25012 Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model
<table>
<thead>
<tr>
<th></th>
<th>AL2</th>
<th>AL3</th>
<th>AL4</th>
<th>AL5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software considerations</strong> <em>(see 5.6)</em></td>
<td>– Rules for Ships, Pt6, Ch1, 2.13 Control engineering requirements, Essential features for control, alarm and safety systems, Programmable electronic systems – Additional requirements for essential services and safety critical systems</td>
<td>– Rules for Ships, Pt6, Ch1, 2.13 Control engineering requirements, Essential features for control, alarm and safety systems, Programmable electronic systems – Additional requirements for essential services and safety critical systems</td>
<td>– Provisional Rules for Software to be used in Naval Ships</td>
<td>– Provisional Rules for Software to be used in Naval Ships</td>
</tr>
<tr>
<td><strong>Communication network considerations</strong> <em>(see 5.7)</em></td>
<td>– Rules for Ships, Pt6, Ch1, 2.11 Control engineering requirements, Essential features for control, alarm and safety systems, data communication links</td>
<td>– Rules for Ships, Pt6, Ch1, 2.11 Control engineering requirements, Essential features for control, alarm and safety systems, data communication links</td>
<td>– To be established on a project by project basis</td>
<td>– To be established on a project by project basis</td>
</tr>
<tr>
<td></td>
<td>– IEC 61162 Series, Maritime navigation and radiocommunication equipment and systems</td>
<td>– IEC 61162 Series, Maritime navigation and radiocommunication equipment and systems</td>
<td>– IEC 61162 Series, Maritime navigation and radiocommunication equipment and systems</td>
<td>– IEC 61162 Series, Maritime navigation and radiocommunication equipment and systems</td>
</tr>
<tr>
<td><strong>System integration considerations</strong> <em>(see 5.9)</em></td>
<td>– Rules for Ships, Pt6, Ch1, 2.14 Control engineering requirements, Essential features for control, alarm and safety systems, Programmable electronic systems – Additional requirements for integrated systems</td>
<td>– Rules for Ships, Pt6, Ch1, 2.14 Control engineering requirements, Essential features for control, alarm and safety systems, Programmable electronic systems – Additional requirements for integrated systems</td>
<td>– To be established on a project by project basis</td>
<td>– To be established on a project by project basis</td>
</tr>
<tr>
<td></td>
<td>– Rules for Ships, Pt7, Ch14, 1.8 Requirements for machinery and engineering systems of unconventional design, Integration</td>
<td>– Rules for Ships, Pt7, Ch14, 1.8 Requirements for machinery and engineering systems of unconventional design, Integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relevant rules, standards and guidance for Cyber SAFE, MAINTAIN and PERFORM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Configuration management considerations</strong> (see 5.10)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AL2</strong></td>
<td><strong>AL3</strong></td>
<td><strong>AL4</strong></td>
<td><strong>AL5</strong></td>
<td></td>
</tr>
<tr>
<td>— Rules for Ships, Pt6, Ch1, 1.4 Control engineering requirements, General Requirements, Alterations and Additions</td>
<td>— Rules for Ships, Pt6, Ch1, 1.4 Control engineering requirements, General Requirements, Alterations and Additions</td>
<td>— Rules for Ships, Pt6, Ch1, 1.4 Control engineering requirements, General Requirements, Alterations and Additions</td>
<td>— Rules for Ships, Pt6, Ch1, 1.4 Control engineering requirements, General Requirements, Alterations and Additions</td>
<td></td>
</tr>
</tbody>
</table>
For further information, contact your local Lloyd’s Register Group office.