Lloyd's Register

Lloyd's Register Type Approval System

Type Approval Requirements for components within Cyber Enabled Systems on board Ships

Procedure for Network and Network-related devices

September 2017

Lloyd's Register

Table of Contents

Foreword

This document details the requirements, within the LR's Type Approval framework, for LR Type Approval of Network and Network-related devices within Cyber Enabled Systems on board ships.

These requirements are to be read in conjunction with the Lloyd's Register Type Approval System Procedure TA14.

Failure to comply with these requirements may render the assessment process results unacceptable for the purposes of Lloyd's Register Type Approval.

The interpretation of this document is the sole responsibility, and at the discretion, of LR. Any uncertainty in the meaning of the specification is to be referred to the local LR office for clarification.

1. General Requirements

1.1 Introduction

1.1.1 This document applies to Lloyd's Register (hereinafter referred to as LR) Type Approval of Network and Network-related devices that are components of Cyber Enabled Systems on board ships, such as, but not limited to, those that fall under the scope of the LR Cyber Enabled Ships ShipRight procedure. This document applies to components within information technology (IT) and operational technology (OT) systems.

1.1.2 Network and Network related devices include but are not limited to:

- Repeaters
- Bridges
- Gateways
- Communication cables
- Routers
- Switches
- Hubs

1.1.3 Information technologies, as defined by NIST (National Institute of Standards and Technology), means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information

1.1.4 Operational technologies means hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events. They may also be referred to as Industrial Control Systems in the context of security.

1.1.5 Network and Network-related devices covered by this document are to comply with the requirements of the following:

a) LR Rules and Regulations for the Classification of Ships (hereinafter referred to as 'Rules for Ships', within which specific prescriptive requirements are established for Networks and Network-related devices and systems. See in particular Rules for Ships, Part 6, Chapter 1, 2.11

b) Other LR Rules and Regulations as appropriate.

c) The relevant requirements of LR Type Approval Test Specification No. 1, within which the environmental testing that is appropriate to equipment for installation in marine applications is specified.

1.1.6 Additional requirements pertaining to the type approval of components of Cyber Enabled Ship Systems are detailed in subsequent sections of this document.

1.1.7 If components with valid LR Type Approval Certificates are to be used within the systems referred to in 1.1.1, the additional requirements of this specification are to be complied with. In such cases the LR Type Approval Certificates will be amended accordingly.

1.1.8 Requirements within this specification are based on International Standards and Common Criteria as detailed in the Appendix and the terms used in this document have the meaning contained therein.

1.1.9 Where a Network or a Network-Node is intended to be part of an Ethernet Connection that includes Maritime Navigation and/or Radio communication system, then the requirements of IEC 61162-460 *Maritime Navigation and Radio communication equipment and systems — Digital interfaces Part 460: Multiple talkers and multiple listeners — Ethernet interconnection — Safety and security,* are to be further considered.

1.1.10 Where it is demonstrated that it is reasonably impracticable to comply with the requirements set out in this document, LR will give special consideration to alternative proposals.

1.2 Information to be submitted

1.2.1 Product Type and description (Target of Evaluation, TOE)

1.2.2 Detailed name of the product and extents of its configurations

1.2.3 Scope of Intended use (in particular specify if the Network or Network-related device or system is intended to be used within Maritime Navigation and Radio communication systems)

1.2.4 Detailed functional and technical description and architectural information

1.2.5 Product manuals, including hardware, software and maintenance

1.2.6 Functions within a system

1.2.7 The proposed Security Target (ST) or the Claimed Protection Profile (PP) chosen to evaluate the TOE

1.2.8 Details of the Common Criteria Testing Lab (CCTL) chosen to conduct the TOE evaluation

1.2.9 Where the Product has been already certified and included in the List of Certified Products, then the information required by 1.2.7 and 1.2.8 is to be replaced by:

a) Certification Report issued by a CCRA (Common Criteria Recognised Arrangement) member
b) Security Target or Protection Profile(s) as applicable

1.3 Design Review and Production Quality Assurance (PQA)

1.3.1 The submitted information together with an *Application Checklist* is to be forwarded to the local LR office that will provide a quotation for Type Approval on request.

1.3.2 A document review will be conducted to determine such facts as product acceptability, compliance with relevant standards and LR Rules, design review, adequacy of proposed Type Test programme and relevance of previous certification and reports.

1.3.3 Production Quality Assurance assessment (PQA) will be carried out by LR in accordance with the *LR Type Approval System Procedure, TA14*.

1.4 Cyber Security – context for Type Approval

1.4.1 The use of information technologies introduces additional risks to assets in terms of information and operational vulnerabilities. In general, Cyber Security is concerned with the protection of assets. Assets are entities that someone places value upon. Within the marine and shipping industry examples of

assets can be: contents of a file or a server, an operational system of classified facilities or information. Many assets are in the form of information that is stored, processed and transmitted by IT products to meet requirements laid down by owners of the information. Information owners may require that availability, dissemination and modification of any such information is strictly controlled and that the assets are protected from threats by countermeasures. Threat agents may include hackers, malicious users, non-malicious users (who sometimes make errors), computer processes and accidents.

1.4.2 Security-specific impairment commonly includes, but is not limited to: loss of asset confidentiality, loss of asset integrity and loss of asset availability. These are related to both information and operations.

1.4.3 The LR approach to cyber security is based on the premise that marine assets are subject to a Cyber Security Management System (CSMS) established by the Organisation. The definition of "Asset" is as given in ISO 15408-1. ("Organisation" refers to the beneficiaries of the CSMS and are Ship Owner/Operator, Shipyard, Ship's Systems manufacturers and maintenance suppliers).

1.4.4 Within such a CSMS, a number of countermeasures can be adopted to minimise, remove or mitigate the risks assessed to the assets as associated to the threats identified. Such countermeasures may consist of IT countermeasures (such as firewalls and smart cards) and non-IT countermeasures (such as guards and procedures). Identification of countermeasures only, however, does not complete the CSMS process.

1.4.5 The IT product evaluation is part of the IT countermeasures. In the IT product evaluation process, the sufficiency of the countermeasures is analysed through a construct called the Security Target (ST) that includes Security Objectives for the TOE (target of evaluation, i.e. the IT product) and Security Objectives for the Operational Environment. The Security Objectives of the TOE are detailed in the Security Functional Requirements (SFR). Reference is to be made to the ISO/IEC 15408-1, ISO/IEC 15408-2, and ISO/IEC 15408-3.

1.4.6 The ST furthermore provides a structured description of those activities that provide evidence of the correctness of the TOE (testing, examining various TOE design representations, and physical security of the TOE) in the form of Security Assurance Requirements (SARs). These SARs are formulated in a standardised language as described in the ISO/IEC 15408-3.

1.4.7 Packages and Protection Profiles (PP) are provided to facilitate writing of a Security Target. A Package can be either a set of SFR or a set of SAR. Whilst a ST describes a specific IT product, a PP is intended to describe an IT product type (e.g. network).

1.4.8 The LR approach to Type Approval of components for Cyber Enabled Systems on board ships includes consideration of evidence of a ST, a PP and assurance, based upon an evaluation (active investigation) of the product against the claimed ST and/or PP. A scale for rating assurance of the product can be claimed at the process start, called Evaluation Assurance Level (EAL), which is based on seven grades (EAL1 to EAL7). The level of assurance evaluated for the product is strictly connected to the level of risk that is assessed as associated to the threat to security (EAL1 when the threats to the security drive to low risk, EAL7 when the threats to the security drive to high risk).

1.4.9 The requirements contained in this document are intended to assess whether a product has a specified security level. This will be detailed as the outcome of the process in the LR Type Approval Certificate (together with other environmental capabilities details of the IT product as assessed against the LR Type Approval System – Technical Specification No. 1) and will include the ST, the PP and the EAL, as applicable. Such details will be the base for the target audience of the Certificate (Ship Owners/Operators, Shipyards and Systems Manufacturers) to identify if the product matches to the needs identified within the CSMS.

1.4.10 For the benefit of having a standardised language and an internationally recognised method, LR refers to the Common Criteria for Information Technology Security Evaluation (CC) (www.commoncriteriaportal.org) and to the ISO/IEC 15408 series that are harmonised with the Common Criteria. Within such an approach LR recognises the Common Methodology for Information Technology Security Evaluation (CEM), the Common Criteria Recognised Arrangement (CCRA) Members, the Certificate Authorising Scheme therein, and the licensed laboratories recognised by them.

1.4.11 For Network Devices, the Collaborative Protection Profile v.1.0 is considered as the PP reference that can be used, however Security Target, additional PPs or Packages can be considered as Conformance Claims to the TOE.

1.4.12 Successful completion of the product (TOE) evaluation by a licensed laboratory (list available on http://www.commoncriteriaportal.org/labs/) and final Certification issued by a CCRA Member (list available on http://www.commoncriteriaportal.org/ccra/members/) as specified in the Common Criteria Portal (http://www.commoncriteriaportal.org/) is a condition to successfully complete the LR Type Approval Certification specified in this set of requirements.

2. Network and Network-related devices requirements

2.1 Introduction

2.1.1 The following requirements are to be complied with for the approval of Network and Network-related devices in accordance with the LR Type Approval System Procedure and in conjunction with the latest LR Type Approval Test Specification No. 1.

2.1.2 Approval of Network and Network-related devices intended for installation and use in isolated enclosures may be based on upon agreed environmental performance tests. Network and Network-related devices intended for all other marine applications are to satisfy the requirements of Test Specification No. 1 category ENV2 as a minimum.

2.2 Quality Assurance System

2.2.1 The manufacturer shall have a quality management system satisfying the requirements of ISO 9001 by an accredited body.

2.3 Functional Requirements

2.3.1 General Functional Requirements

2.3.1.1 The Network and Network-related devices and systems are to comply with the requirements of LR Rules for Ships, Part 6, Chapter 1, 2.11 Data Communication links. Function and performance of such devices is to be demonstrated in accordance with the relevant requirements of LR Type Approval Test Specification No. 1. The testing is to be detailed in the test programme submitted.

2.3.1.2 Where Network and Network-related devices and systems are based on wireless technologies, then the requirements of LR Rules for Ships, Part 6, Chapter 1, 2.12 Additional requirements for wireless data communication links are to be complied with. Function and performance of such devices is to be demonstrated in accordance with the relevant requirements of LR Type Approval Test Specification No. 1, with particular reference to EMC testing. The testing is to be detailed in the test programme submitted.

2.3.2 Security Functional Requirements (SFR)

2.3.2.1 The Security Functional Requirements (SFR) define the rules by which the Network/Network-related Device/System governs access to and use of its resources, and thus information and services controlled by it. They are contained in the Security Target and/or Protection Profile and are expressed in classes, families and components.

2.3.2.2 The clear description of the Security Functional Requirements and key concepts is to be in accordance with IEC15408-2, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.

2.3.3 Security Assurance Requirements (SAR)

2.3.3.1 Security Assurance Requirements (SAR) are expressed in classes, families and components. A scale for rating assurance of the product is called Evaluation Assurance Level (EAL) and is based on seven grades (EAL1 to EAL7). The level of assurance required to the product is strictly connected to the level of risk that is assessed as associated to the threat to security (EAL1 when the threats to the security drive to low risk, EAL7 when the threats to the security drive to high risk).

2.3.3.2 The clear description of the Security Assurance Requirements and key concepts is to be in accordance with IEC15408-3, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security assurance components.

APPENDIX – Reference Documents

IMO MSC.1/Circ. 1526 Interim Guidelines on Maritime Cyber Risk Management

Lloyd's Register Rules for Ships

Lloyd's Register Type Approval System Procedure, TA14

Lloyd's Register Type Approval Test Specification No. 1

ISO/IEC 15408-1 Information technology – Security techniques - Evaluation criteria for IT security, Part 1: Introduction and general model

ISO/IEC 15408-2 Information technology – Security techniques - Evaluation criteria for IT security, Part 2: Security Functional components

ISO/IEC 15408-3 Information technology – Security techniques - Evaluation criteria for IT security, Part 1: Security Assurance components

ISO/IEC 18045 Information technology – Security techniques – Methodology for IT security evaluation

ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls

Common Criteria for Information Technology Security Evaluation (CC) issued by the Common Criteria Recognition Arrangement (CCRA)

Common Methodology for Information Technology Security Evaluation (CEM) issued by the Common Criteria Recognition Arrangement (CCRA)

ISO/IEC 17799 Information technology — Security techniques — Code of practice for information security management

ISO/IEC 19790 Information technology — Security techniques — Security requirements for cryptographic modules

ISO/IEC TR 19791 Information technology — Security techniques — Security assessment of operational systems

ISO/IEC 62443 series: Industrial communication networks — Network and system security

IEC 61162-460 Maritime navigation and radio communication equipment and systems — Digital interfaces Part 460: Multiple talkers and multiple listeners — Ethernet interconnection — Safety and security

Lloyd's Register Group Limited
Lloyd's Register Global Technology Centre
Southampton Boldrewood Innovation Campus
Burgess Road, Southampton, SO16 7QF