DNV·GL

CLASS PROGRAMME

Type approval

DNVGL-CP-0231 Edition March 2020

Cyber security capabilities of systems and components

The content of this service document is the subject of intellectual property rights reserved by DNV GL AS ("DNV GL"). The user accepts that it is prohibited by anyone else but DNV GL and/or its licensees to offer and/or perform classification, certification and/or verification services, including the issuance of certificates and/or declarations of conformity, wholly or partly, on the basis of and/or pursuant to this document whether free of charge or chargeable, without DNV GL's prior written consent. DNV GL is not responsible for the consequences arising from any use of this document by others.

The electronic PDF version of this document, available at the DNV GL website dnvgl.com, is the official, binding version.

DNV GL AS

FOREWORD

DNV GL class programmes contain procedural and technical requirements including acceptance criteria for obtaining and retaining certificates for objects and organisations related to classification.

© DNV GL AS March 2020

Any comments may be sent by e-mail to *rules@dnvgl.com*

This service document has been prepared based on available knowledge, technology and/or information at the time of issuance of this document. The use of this document by others than DNV GL is at the user's sole risk. DNV GL does not accept any liability or responsibility for loss or damages resulting from any use of this document.

CHANGES – CURRENT

This document supersedes the February 2020 edition of DNVGL-CP-0231.

Changes in this document are highlighted in red colour. However, if the changes involve a whole chapter, section or subsection, normally only the title will be in red colour.

Changes March 2020

Only editorial corrections have been made in this edition.

Changes February 2020

Topic	*Reference*	*Description*
Alignment with class notation **Cyber secure**		Since the rules for class notation **Cyber secure**, DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21, were published July 2018, this revised edition of the TA programme is completely re-written to be aligned with the rules.
Security requirements	Sec.1 [3]	Security requirements are removed from this revised edition of the TA programme. The security requirements for type approval are instead stated in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21, or optionally for navigation and radiocommunication equipment in IEC 61162-460.
Components vs. systems	Sec.3 [1]	The first edition of this TA programme was based on individual components. This revised edition includes also systems and clarifies the difference between components and systems.
Documentation	Sec.3 [5]	Improved description of documentation to be submitted.

Editorial corrections

In addition to the above stated changes, editorial corrections may have been made.

CONTENTS

SECTION 1 GENERAL

1 Introduction

Recognising the increase in connectivity and integration as well as growing risks related to cyber incidents, it is crucial to address cyber security in the both design of cyber-physical systems as well as in operation of the vessel. DNV GL has therefore established class notation **Cyber secure** (see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21) addressing cyber security of vessels and their systems.

This class programme (CP) describes the procedure for DNV GL type approval (TA) of cyber security capabilities for systems and components to be installed on board ships and offshore installations.

2 Objective

The objective of this TA scheme is to offer an alternative to case-by-case design approval for systems or components intended for vessels with class notation **Cyber secure**.

3 Scope

The TA process described in this CP is specific for and limited to TA of cyber security capabilities and applies for routinely manufactured systems and components including the software supporting such security capabilities.

For a description of DNV GL type approval in general and further information on type approval of control systems and components, see DNVGL-CP-0338 *Type approval scheme* and DNVGL-CP-0203 *Electronic and programmable equipment and systems*.

4 Application

TA in accordance with this CP is voluntary unless specifically required by DNV GL rules for ships or DNV GL offshore standards. The scheme may be applied for any software-based system or component on board ships and offshore installations, but is deemed especially relevant for systems used in the following applications:

- remote access to OT-systems
- safety systems
- integrated and inter-connected control and monitoring systems
- systems supporting essential vessel services
- navigation and radiocommunication systems
- other systems subjected to requirements for integrity, confidentiality and availability.

5 Abbreviations

Table 1 Abbreviations

Abbreviation	*Description*
COTS	commercial off the shelf
CP	class programme
EDR	embedded device requirement
HDR	host device requirement

Abbreviation	*Description*
IT	information technology
NDR	network device requirement
OEM	original equipment manufacturer
OT	operational technology
SL	security level
SR	security requirement
SP	security profile
TA	type approval

SECTION 2 TYPE APPROVAL PROCESS

1 Request for type approval

A formal request for type approval should be submitted to the local DNV GL office. The following information should be included:

- high-level product information of the system or component to be type approved, including its intended application and identification of hardware, software and OEM
- desired security profile (SP), see Sec.3 [1]
- information about compliance with environmental requirements for hardware, see Sec.3 [6].

After receiving the request, DNV GL will provide a quotation for the type approval. Upon acceptance of the quotation by the manufacturer, a contract will be established between the manufacturer and DNV GL.

2 Initial type approval assessment

An initial TA survey may be required to confirm that the manufacturer has a production line and quality control for consistent production of the product(s) for which TA is requested. This initial TA assessment may be performed during the type test survey (see [4]) or be exempted if similar quality control audit has been previously carried out for other certification services.

3 Design assessment

For each system to be type approved, the manufacturer is required to submit the documents described in Table 1. Submittal should be on a common and agreed electronic format (e.g. PDF) via email, CD, web file transfer service or via Veracity (https://www.veracity.com/).

Table 1 Documentation requirements

Object	*Document type*	*Additional description*	*Info*
Vessel control and monitoring systems	I020 - Control system functional description	Description of security capabilities, see Sec.3 [5.2].	AP
	Z252 - Test procedure at manufacturer	Test procedure for type testing, see Sec.3 [5.3].	AP
	Z100 - Specification	Configuration, see Sec.3 [5.4].	AP
	Z100 - Specification	Asset inventory, see Sec.3 [5.5].	FI
	Z100 - Specification	Modification strategy, see Sec.3 [5.6].	AP
	I320 - Software change handling procedure	Change management procedure, see Sec.3 [5.7].	AP

Additional relevant documentation may be requested in the type approval process, e.g.:

- logical and physical topology drawings
- description of application functions and operational limitations
- information and instructions related to installation and integration
- information about product marking/labelling
- information about production quality assurance system, see [2].

DNV GL will verify the documentation for compliance with the applicable requirements.

4 Type testing

Type testing shall be witnessed by the Society and carried out in accordance with an approved test procedure, see Sec.3 [5.3]. The type testing may commence when the design assessment has been completed by DNV GL. A copy of the signed and marked-up test program may serve as official test report.

Type testing shall also include verification of the following:

- correctness of approved configuration, see Sec.3 [5.4]
- correctness of asset inventory, Sec.3 [5.5]
- product marking/labelling to include identification of manufacturer, type number/model number and serial number.

5 Issuance of certificate and validity period

When design assessment and type testing have been completed, DNV GL will issue TA certificate. The certificate will be available on www.approvalfinder.dnvgl.com and have a validity period of 2 years.

During the period of validity, major changes as defined in document *Modification strategy* (see Sec.3 [5.6]) are required to be informed to DNV GL and will be subject to assessment and possibly type testing. After approval of the modifications, the TA certificate will be updated to reflect the new version of the software.

SECTION 3 REQUIREMENTS

1 Security requirements

As noted in Sec.1 [2], the objective of this CP is to offer type approval of systems and components in accordance with DNV GL rules for class notation **Cyber secure** (DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21).

Class notation **Cyber secure** includes five selectable levels of risk reduction called security profiles (SP). The security profiles are incremental which means requirements for a selected SP include also requirements for all lower SPs (e.g. SP3 includes SP0, SP1, SP2 and SP3).

- SP0 applies for all **Cyber secure** class notation qualifiers. The requirements for SP0 constitute design principles and common security requirements. TA in accordance with SP0 is not relevant.
- SP1 applies for class notation **Cyber secure(Essential)**. The requirements for SP1 constitute security requirements based on IEC 62443 security level 1. SP1 may also be selected for systems included in class notation **Cyber secure(+)**.
- SP2 may be selected for systems included in class notation **Cyber secure(+)**. The requirements for SP2 constitute security requirements based on IEC 62443 security level 2.
- SP3 applies for class notation **Cyber secure(Advanced)**. The requirements constitute security requirements based on IEC 62443 security level 3. SP3 may also be selected for systems included in class notation **Cyber secure(+)**.
- SP4 may be selected for systems selected for class notation **Cyber secure(+)**. The requirements constitute security requirements based on IEC 62443 security level 4.

The requirements for security capabilities in SP1 to SP4 are based on, but not identical to, the requirements in IEC 62443 SL1 to SL4. The differences are reflected in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4]. For example; some requirements in IEC 62443 SL3 are not required by SP3 and some requirements in SP1 are higher than the corresponding IEC 62443 SL1.

For navigation and radiocommunication equipment, compliance with DNV GL security profiles may be achieved by applying IEC 61162-460 as an alternative standard. Full compliance with applicable clauses of IEC 61162-460 will be required. Any requirements additional to IEC 61162-460 are specifically identified in the rules, e.g. time synchronization in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.3.12] is not part of IEC 61162-460, but will be required for type approval. Note also that IEC 61162-460 requires compliance with relevant parts of other IEC 61162-standards (e.g. IEC 61162-450).

Guidance note:

Full compliance with IEC 61162-460 is only applicable for complete network. Components are type approved in accordance with applicable parts.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

Consequently, the company seeking TA should specify one of the following options for type approval:

1) TA in accordance with SP1
2) TA in accordance with SP2
3) TA in accordance with SP3
4) TA in accordance with SP4
5) TA in accordance with SP1-SP3, based on IEC 61162-460. Applicable only for navigation and radiocommunication equipment and compliant with all **Cyber secure** class notation qualifiers.

For options 1 to 4, the TA certificate will confirm compliance with the selected DNV GL security profile (SP). For option 5, the TA certificate will in addition confirm compliance with IEC 61162-460.

Guidance note:

This TA scheme is limited to verification of technical security capabilities of systems and components. Hence, requirements related to policies and procedures as required by class notation **Cyber secure** is not part of this type approval. Similarly, verification of a manufacturer's software development process as described in IEC 62443-4-1 (CCSC 4 in IEC 62443-4-2) is not included in this TA scheme. A separate approval of manufacturer (AoM) may be offered covering verification of work processes for software development in accordance with DNVGL-CP-0507.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

2 System type approval

This TA scheme is mainly intended for type approval of a system which, in the context of this CP, is defined as one or more interconnected components serving a defined maritime application or process.

It is generally required that all components in the system have the required security capabilities. However, some requirements may not be applicable, e.g.:

- If public key infrastructure (PKI) is not used in the system, this will be omitted, see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.2.9].
- Remote session termination is obviously only relevant for components supporting such functionality, see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.3.7].
- Authentication of control room operators will not be required for workstations located in continuously manned/restricted areas, see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.2.2].

Note that relevant requirements in IEC 62443-4-2 will also apply for type approval if such capabilities are needed to meet the requirements in DNV GL rules for class notation **Cyber secure**. E.g. the capability to support updates and upgrades in accordance with IEC 62443-4-2 HDR 3.10 will apply to meet requirements for cyber security management system in DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [3].

In the event that certain components in a system cannot comply with a requirement, compensating countermeasures should be proposed by the company seeking TA. Such equivalent solutions will be evaluated and, if accepted, stated in the TA certificate. An example could be information persistence (see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4.5.3]), it may be acceptable that a component does not have the capability to purge stored information if this is compensated by procedural measures. Such compensating countermeasures are generally not acceptable for navigation and radiocommunication equipment to be type approved in accordance with IEC 61162-460 (see option 5 in [1]).

3 Component type approval

Type approval in accordance with this CP may also be done for a 'generic' component which on its own does not serve a defined maritime application or process.

It is generally required that the component complies with all applicable requirements. Compensating countermeasures which need to be implemented when the component is integrated into a system are normally not acceptable.

4 Security updates

The company supplying products type approved in accordance with this CP should ensure that security vulnerabilities are identified, remediated and mitigated by qualifiying and offering security patches to their customers.

Such modifications shall be described in the modification strategy, see [5.6], and performed in accordance with the change management procedure, see [5.7]. Only information about patches classified as 'major' and patches that change security capabilities must be submitted to DNV GL. See also Sec.2 [5].

5 Documentation requirements

5.1 General

The following subsections describe purpose and required content of the documentation to be submitted for design assessment.

The documents shall be controlled in the suppliers document management system and shall be identified with name, document number and revision.

5.2 Description of security capabilities

This document shall serve two objectives:

1) The product supplier shall demonstrate control of the required security capabilities for the type approved system or component.
2) DNV GL shall be able to verify compliance with required security capabilities.

The compliance description shall describe with narrative text how each applicable requirement is complied with. It shall not be necessary to read other documentation such as OEM manuals or web pages to verify compliance with the requirements. The document shall be structured according to the requirements in DNV GL rules for class notation **Cyber secure** (see DNVGL-RU-SHIP Pt.6 Ch.5 Sec.21 [4]). This means the document shall contain one dedicated chapter or section for each requirement. Each chapter shall describe the security mechanisms in the various components in the system as follows:

- Narrative text describing how the required capability is implemented and achieved for the system as a whole. Differences in capabilities for the various components shall be identified and described.
- For each unique component type, identification of the software in which the security capability resides (this shall correspond with the software listed in asset inventory, see [5.5]).
- If applicable, reference to further detailed information about the security mechanism, e.g. in public OEM manuals or websites.
- In case a requirement is deemed not applicable, this shall be described and justified.
- In case a requirement is deemed not relevant for any component(s) in the system, this shall be described and justified.
- In case any component cannot comply with a requirement, the risk derived from this non-compliance shall be documented. The proposed compensating countermeasure(s) shall be described, and the risk mitigation based on the countermeasure(s) shall be documented.

5.3 Test procedure

Testing of security capabilities shall follow an approved test procedure and be witnessed by DNV GL surveyor. The surveyor may request additional testing if deemed necessary to verify compliance with the requirements.

The test procedure shall describe:

- how to test each required security capability (including necessary test setup, initial condition, acceptance criteria)
- demonstrate that the asset inventory represents the tested system/component
- demonstrate that type approved configuration file(s) represent correct settings.

For TA of systems, the following principles apply:

- repeated testing of identical components is generally not required
- testing of individual component capabilities may be partly or fully replaced by testing of system-wide functionality such as central logging of security events or unified account management

- in case compensating countermeasures have been approved, the test procedure shall include validation of such compensating countermeasure(s).

5.4 Configuration

A listing of all configurable parameters/settings needed to achieve the required security capabilities shall be submitted. The list may be individual per component or common for all components in the system.

The type approved configuration shall be subject to change management, i.e. the document shall be revised upon changes to the product, see [5.6] and [5.7] below.

When the type approved system or component is delivered to DNV GL classed vessels, the actual configuration of the delivered product is subject to verification against the contents of the configuration file.

5.5 Asset inventory

A register of the inventory for each system shall be submitted for information. The register shall include the information listed below per component. See also requirement in IEC 62443-3-3 SR 7.8.

- specifications hardware, including firmware as relevant
- specifications of system software (e.g. operating system)
- specifications application software(s)
- specifications of interfaces, supported data protocols and communication protocols
- name and version of configuration file(s), see [5.4].

When the type approved system or component is delivered to DNV GL classed vessels, the contents of the asset inventory is subject to verification against the delivered product.

The asset inventory shall be subject to change management, i.e. it shall be revised upon changes to the product, see [5.6] and [5.7] below.

5.6 Modification strategy

It is expected that modifications (e.g. updates and patching of COTS and other third-party software) will be done during the validity of the TA certificate. See also requirements to facilitate updates and patching in IEC 62443-4-2 EDR/HDR/NDR 3.10.

The modification strategy shall serve two main purposes (see guidance below for example):

- categorise type of modification according to the anticipated impact it may have on security capabilities
- define relationship between type of modification and assignment of new software version/revision.

Based on the modification strategy, the TA certificate will include a list of the software names/versions which are covered by the type approval, e.g. 'software: name, ver.2.4.z'.

During the validity of the TA certificate, major modifications shall be informed to DNV GL. The modification will be evaluated against applicable requirements and additional type testing may be required. The TA certificate will then be updated with new information and/or updated identifier in the software version.

Guidance note:

Example of modification categorisation:

Minor modifications, not affecting security capabilities, e.g.

- configuration/parameterisation changes such as adjusting a timer, adding a human user, changing time for session lock, etc.
- installation of qualified vendor security updates or patches
- design modifications not affecting security capabilities of other required functions.

Major modifications - potentially affecting security capabilities, e.g:

- design modifications resulting in change of inherent software code affecting security capabilities
- installation or upgrade of new software versions, e.g. operating systems and application programs
- identification of fault or malfunction which compromises security capabilities (e.g. known vulnerability, published vendor advisory). May require modification of delivered systems.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

Guidance note:

Example of relationship between type of modification and version/revision of 'software version x.y.z':

- Identifier 'x' is updated due to major modifications, e.g. main design changes
- Identifier 'y' is updated due to major modifications, e.g. upgrade of application software
- Identifier 'z' is updated due to minor modifications, e.g. security updates or patching.

---e-n-d---o-f---g-u-i-d-a-n-c-e---n-o-t-e---

5.7 Change management procedure

The company requesting TA is required to operate a quality management system where change management is adequately covered.

The procedure for change management shall at least describe the work processes listed in Table 1 below including how these activities are logged/documented, i.e. in a change log. It is required that all types of modifications (i.e. major and minor as described in [5.6]) are performed in accordance with the change management procedure. For vessels with class notation **Cyber secure**, change logs are subject to audit.

Table 1 Change management activities

Activity	*Description*
motive	describe reason for modification
category	determine type of modification in accordance with modification strategy
design	describe and perform required design activities, including update of related documentation
versioning	ensure correct update of software version/revision in accordance with modification strategy
implications	analyze possible impact of the modification
authorization	ensure required acceptance within the supplier organization and by the customer
implementation	describe and perform required implementation activities
verification	establish procedures and carry out activities related to testing, acceptance criteria, witnessing by other stakeholders, reporting

6 Hardware requirements

Hardware components in maritime automation and control systems shall be suitable for operation in maritime environments according to the location in which they will be installed. This normally requires that hardware shall be type approved in accordance with DNVGL-CP-0203. See also test specification DNVGL-CG-0339 and IEC 60945 (for navigation and radiocommunication equipment).

Hardware components serving non-important services (see DNVGL-RU-SHIP Pt.4 Ch.8 Sec.13) may be exempted from the mandatory 'hardware TA' scheme. However, it will be required that such components cannot upon any failure affect other essential or important systems or components onboard (e.g. compliance with requirements for electromagnetic emission in IEC 60945 may be required).

CHANGES – HISTORIC

January 2018 edition

There are currently no historic changes for this document

About DNV GL
DNV GL is a global quality assurance and risk management company. Driven by our purpose of safeguarding life, property and the environment, we enable our customers to advance the safety and sustainability of their business. We provide classification, technical assurance, software and independent expert advisory services to the maritime, oil & gas, power and renewables industries. We also provide certification, supply chain and data management services to customers across a wide range of industries. Operating in more than 100 countries, our experts are dedicated to helping customers make the world safer, smarter and greener.

SAFER, SMARTER, GREENER