DNV·GL

CLASS PROGRAMME

Type approval

DNVGL-CP-0231 Edition January 2018

Cyber security capabilities of control system components

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.

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

CHANGES – CURRENT

This is a new document.

CONTENTS

SECTION 1 GENERAL

1 Introduction

Components type approved in accordance with this class programme (CP) are certified to have cyber security capabilities in compliance with DNV GL standards or rules for classification.

2 Objective

The objective of this class programme is to describe the process and requirements for type approval of cyber security capabilities of software-based components to be installed on board classed ships and offshore installations.

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

3 Application

Type approval in accordance with this CP is voluntary unless otherwise stated in the applicable DNV GL standards and rules for classification.

This type approval is applicable for any software-based component on board ships and offshore installations, but is deemed as especially relevant for components used in the following applications:

— remote access to components (e.g. from on-shore or from other uncontrolled systems)
— integrated and inter-connected control and monitoring systems
— safety systems
— navigation systems
— systems supporting essential vessel services
— other systems subjected to requirements for redundancy and/or separation.

Approval of security capabilities in accordance with this CP should be applied as a part of the overall cyber security management framework on the vessel (see e.g. DNVGL-RP-0496, ISA/IEC 62443 series of standards or NIST cybersecurity framework).

4 Scope

This CP describes the type approval process, the requirements for security capabilities and the requirements for type testing.

5 Abbreviations

Table 1 Abbreviations

Abbreviation	*Definition*
ACL	Access control list
AES	Advanced encryption standard
AP	Access point
A/V	Anti virus
CD	Compact disc

Abbreviation	*Definition*
CP	Class programme
CRC	Cyclic redundancy check
DHCP	Dynamic host configuration protocol
DNS	Domain name system
DMZ	De-militarized zone
DoS	Denial of service
EDSA	Embedded device security assurance
EICAR	European Institute for Computer Antivirus Research
FR	Foundational requirement. See IEC 62443
FTP	File transfer protocol
HMI	Human machine interface
HTTP	Hypertext transfer protocol
IACS	Industrial automation and control system
ICMP	Internet control message protocol
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IP	Internet protocol
IPS	Intrusion prevention system
ISA	International Society of Automation
LAN	Local area network
MAC	Media access control
MFA	Multifactor authentication
MSTP	Multiple spanning tree protocol
N/A	Not applicable
NAC	Network access control
OS	Operating system
OWASP	Open web application security project
PDF	Portable document format
PKI	Public key infrastructure
PLC	Programmable logic controller
REDS	Removable external data source
RSA	RSA SecurID, formerly referred to as SecurID, is a mechanism developed by Security Dynamics (later RSA Security and now RSA)

Abbreviation	*Definition*
RSTP	Rapid spanning tree protocol
SFTP	SSH file transfer protocol
SL-C	Capability security level. See IEC 62443
SNMP	Simple network management protocol
SNTP	Simple network time protocol
SSH	Secure shell
TA	Type approval
TCP	Transmission control protocol
UDP	User datagram protocol
USB	Universal serial bus
VLAN	Virtual local area network

SECTION 2 TYPE APPROVAL PROCESS

1 Component types

Type approval in accordance with this CP provides independent assessment and certification of a component's cyber security capabilities. The CP may also be applied for type approval of a system when the system comprises a defined group of components.

Components to be type approved shall be categorized according to the types listed below. The table indicates relationship between the component types in this CP and components defined in the referenced standards ISA-62443-4-2 and IEC 61162-460.

Table 1 Component types

Component types in this CP	*Description*	*Component types in IEC 61162-460*	*Component types in ISA-62443-4-2*
Node	An end-device connected to the secure/controlled network, e.g. operator station, PLC, etc.	460-Node	— software application — embedded device — host device
Switch	A network infrastructure device used to interconnect nodes on the same secure/controlled network, e.g. a layer-2 switch.	460-Switch	— network device
Forwarder	A network infrastructure device used to interconnect secure/controlled networks, e.g. a layer-3 switch or a router.	460-Forwarder	— network device — software application — host device
Gateway	A network infrastructure device used for connecting secure/controlled network to insecure/uncontrolled networks, e.g. a router including firewall (including wireless gateway).	460-Gateway 460-Wireless Gateway	— network device — software application — host device
Border gateway	A network infrastructure device located on shore and used for remote access to the vessel where communication is routed via insecure/uncontrolled network(s) such as e.g. the Internet.	460-Gateway	— network device — software application — host device

2 Requirements and security levels

The security requirements in this CP are organized according to the seven foundational requirements (FRs) described in IEC 62443-1-1 (edition 1.0 2009-07) and IEC 62443-3-3 (edition 1.0 2013-08).

Table 2 IEC 62443 Foundational Requirements

Number	*Name*	*Requirements related to:*
FR1	Identification and authentication control	Identification and authentication of human users, software applications and hardware components.
FR2	Use control	Assignment and control of privileges and authorizations for the identified user, application or component.
FR3	System integrity	Protection of the integrity of components or systems.

Number	*Name*	*Requirements related to:*
FR4	Data confidentiality	Protection of data, applies to stored data and data transferred via communication channels.
FR5	Restricted data flow	Segmentation of the control system. Refer to the concept of zones and conduits in ISA/IEC 62443. Relevant capabilities are firewalling, unidirectional communication, DMZ, etc.
FR6	Timely response to events	Monitoring, recording and reporting of security incidents.
FR7	Resource availability	Availability of the component and its applications. Capabilities related to resilience, degradation, response and recovery in case of security incidents.

The CP intends to be aligned with ISA/IEC 62443 by including all requirements in ISA-62443-4-2 D4E1 (draft 4, edit 1, January 12, 2017). These requirements have been summarized as interpreted by DNV GL and amended as relevant to comply with any specific application requirements in DNV GL standards and rules for classification. The referenced standard is a necessary reading in order to understand the full content of the requirements. The CP also includes specific test methods for each requirement in ISA-62443-4-2, these test specifications are developed by DNV GL since this is not part of ISA-62443-4-2.

In addition, selected requirements and concepts from IEC 61162-460 (edition 1.0 2015-08) have been included in the CP. The main reason for this is to complement the CP with relevant and specific security requirements related to e.g. removable external data sources (REDS) and principles on communication to/from insecure/uncontrolled networks. The CP does not intend to be aligned with all content in IEC 61162-460.

Finally, supplementary security requirements have been developed by DNV GL as deemed necessary.

The requirements are differentiated in accordance with the four component capability security levels (SL-C) described in ISA-62443-4-2. The four security levels have commonly been defined to provide the following general protection capabilities (source: ISA-99 Meetings, Frankfurt, June 2015 (http://isa99.isa.org/ Public/ Meetings/Committee/201506-Frankfurt/ISA99-Protection-Levels.pdf).

Table 3 Security levels

Security level	*Capabilities*
1	Protection against casual or coincidental violation
2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
3	Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation
4	Protection against intentional violation using sophisticated means, extended resources, IACS specific skills, high motivation

The security requirements in Sec.3 are stated in tables of a common format as exemplified in Table 4.

The first row specifies for which component type the respective requirement applies. The rows below specify the capability requirements and corresponding test requirements for each security level.

The requirements are incremental unless otherwise noted. This means that if the component shall comply with e.g. requirements for security level 3, it shall also comply with requirements for security levels 1 and 2.

Table 4 Requirement format

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***NO***
1	Capability requirement for security level 1				
	Test requirement for security level 1				
2	Capability requirement for security level 2				
	Test requirement for security level 2				
3	Capability requirement for security level 3				
	Test requirement for security level 3				
4	Capability requirement for security level 4				
	Test requirement for security level 4				

3 Zones, conduits and controlled networks

Following the concept of zones and conduits described in IEC 62443-1-1, components integrated onboard should be selected according to the target security level (SL-T) which has been determined for the respective zone or conduit as a result of risk assessments such as described in ISA-62443-3-2 (draft 7, edit 1, May 22, 2017). See also DNVGL-RP-G108 for guidance on partitioning the system into zones and conduits.

Note that components which are not completely in compliance with all requirements at a given target security level may still be integrated into the system, but then appropriate compensating countermeasures should be applied and evaluated as part of the risk assessment process. These considerations are not in scope for this type approval program, but the certificate will include reference to a list of any findings or requirements which are not complied with at the applicable security level.

The CP adopts the concept of controlled and uncontrolled networks described in IEC 61162-460. The main purpose is to specifically address requirements to communication between onboard secure networks (controlled) and other networks onboard or onshore (e.g. remote access).

It is not in scope of this CP to determine whether given network segments are to be considered secure, nor does it intend to define an exact relationship between zones defined by IEC 62443 and controlled networks defined by IEC 61162.

A security zone is defined in IEC 62443-1-1 as a grouping of logical or physical assets that share common security requirements.

A controlled network is defined in IEC 61162-460 as any network that has been designed to operate such that authorities are satisfied by documented evidence that it does not pose any security risks to any connected network nodes.

4 Request for type approval

A formal request for type approval shall be submitted to the local DNV GL office by use of the form *Application for type approval of instrumentation and automation equipment* (form 86.02a.) The following specific information should be included in the application:

— Particulars of application shall specify that type approval is requested in accordance with this CP.
— Product listing shall identify each component for which type approval is requested. For each component, component type and security level shall be defined.
— Other information in form 86.02a shall be filled in as relevant.

After receipt of the request, DNV GL will provide a quotation for the requested service. Upon acceptance of the quotation, a contract will be established between the manufacturer and DNV GL local station.

5 Type approval certificate

The type approval certificate will state that the respective component(s) is found to comply with this document. Information will also be included in the certificate about the edition of the class programme which has been used. Upon renewal of the certificate, the component(s) will be required to comply with the current edition of the class programme.

Each component which has been type approved will be listed in the certificate, including component type, description, identification, reference to hardware approval (if relevant) and software versions.

6 Type approved software

This CP requires that any software which contains one or more of the required cyber security capabilities is identified with its name and version and listed in the certificate.

Furthermore, to enable efficient implementation and verification of the security capabilities when used in a project, the software shall be identified as follows:

1) For each type approved component, any software (e.g. firmware or operating system) which contains one or more required security capability shall be identified in the certificate with name and version. It shall be possible to view the version and revision of such software in an HMI (e.g. in a survey).

   Software versions (e.g. major and minor) are to be specified in the certificate. When a software version is updated during the period of certificate validity, DNV GL shall be informed and evaluate the need for document verification and/or type testing (the information shall describe the effect on the approved security capabilities). The type approval certificate shall be updated to reflect the new software version.

   Software revisions (e.g. bug fixes, patches, builds) are not required to be specified in the certificate provided that such revisions will not affect the functionality or configuration of approved security capabilities. This shall be documented and approved in the type approval process. It is also a condition that the manufacturer demonstrates adequate management of modifications.

2) For each type approved component, each configurable security capability shall be mapped towards the respective requirement in this CP and identified in a manufacturer-specific configuration file.

   This configuration file shall specify settings and instructions which must be implemented to achieve the approved capability at the approved security level. Default values should also be included. When the component is delivered in a project, the configuration shall be subject to established configuration management routines which will be audited during the type approval project.

   Verification or approval of the configuration file when the component is used in a project is not scope of this CP and will be subject to requirements in relevant class rules.

7 Documentation requirements

The following documentation shall be submitted for approval on a common and agreed electronic format (e.g. PDF) via email, CD, web file transfer service or via Veracity (https://my.dnvgl.com/):

Table 5 Documentation requirements

Object	*Document type*	*Additional description*	*Info*
Specification	Z100	For each component type: Product specification or manual, including description of the component's security capabilities.	FI

Object	*Document type*	*Additional description*	*Info*
Functional description	I020	For each component type: Narrative description of compliance with each required security requirement in this CP. The description shall include specific reference to chapter/paragraph where the capability is described in the product specification/manual.	AP
System block diagram (topology)	I030	Typical topology of the system in which the components are used.	FI
Test procedure	Z252	Test program for type testing where all required tests for the relevant component are described.	AP
Manual	Z160	If applicable, other relevant documentation as agreed in the type approval process. E.g. documentation related to configuration, parameterization, vessel application and system integration.	FI

8 Initial assessment

Requirement for initial type approval assessment may be exempted depending on whether similar quality control audit has been carried out for other certification services.

9 Hardware approval

Components to be type approved in accordance with this CP and which are part of/or support important or essential services onboard shall be hardware type approved as required by DNVGL-RU-SHIP-Pt.4 Ch.9 or DNVGL-OS-D202 (see also DNVGL-CG-0339.)

Exemption from such hardware approval applies for:

— Component type border gateway (unless otherwise stated in applicable DNV GL rules).
— Components which are MED-certified and compliant with IEC 60945.

10 Type testing

Type testing in accordance with this CP and approved test program shall be witnessed by DNV GL.

However, the component vendor may also engage DNV GL to conduct the type test in DNV GL test facilities. In such case, witnessing is not required. A signed test report shall be submitted for approval.

11 Validity of certificate

Validity of type approval certificates in accordance with this CP is two (2) years. Periodical assessment during the period of validity is not required for type approval certificates in accordance with this CP.

See DNVGL-CP-0338 for general conditions related to suspension or withdrawal of type approval certificates.

SECTION 3 SECURITY REQUIREMENTS

All requirements which refer to external standards shall be regarded as interpretations. The referenced standard shall be used to determine the full content, rationale and relevant guidance.

Where the requirements specify *alarm*, this shall be implemented in accordance with guidance in the referenced standard and in accordance with relevant principles such as IMO performance standard for bridge alert management (MSC.302(87) or DNVGL-RU-SHIP Pt.4 Ch.9/DNVGL-OS-D202.

1 Identification and authentication

This subsection includes requirements for capabilities related to identification and authentication of all users (human, software processes and devices).

1.1 User identification and authentication

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Requirement: ISA-62443-4-2 CR 1.1 Enforce identification and authentication on the interfaces that provide human user access.				
	Test: Verify that the device cannot be operated without being logged in with a specific user account. Verify that the normal user account used as always logged in (in e.g. manned control rooms) does not have administrative rights on the device, and the actions allowed for the given user account concern only the operation of the component and not administration.				
2, 3	Requirement: ISA-62443-4-2 CR 1.1 (1) Enforce unique identification and authentication of each human user.				
	Test: Verify that no publicly known - default - credentials can be used to authenticate to the device. Enumerate all usernames, if applicable, to verify that no shared accounts are used.				
4	Requirement: ISA-62443-4-2 CR 1.1 (1)(2) Enforce multifactor authentication of each human user.				
	Test: Verify that the different paths of authentication information cannot easily be tampered with.				

Guidance note:

Applicable for all requirements to identification and authentication of human users:

Where immediate operator interaction is needed, the component should allow for human users to directly access the component's operator interface without identification and authentication. In such case, access to such components should be controlled by other compensating measures (e.g. component located in continuously manned control room, physical access to room is restricted/ controlled, etc.) Such compensating measures are not scope of type approval.

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

1.2 Application or device identification and authentication

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2	Requirement: ISA-62443-4-2 CR 1.2 Identify and authenticate itself when interfacing other component(s).				
	Test: Use the method/protocol (e.g. SNMP, or LLDP for discovery, and 802.1X for authentication) specified by the vendor to retrieve and verify component type.				
3, 4	Requirement: ISA-62443-4-2 CR 1.2 (1) Uniquely identify and authenticate itself when interfacing other component(s).				
	Test: Use the method/protocol (e.g. SNMP, or LLDP for discovery, and 802.1X for authentication) specified by the vendor to retrieve and verify component type and its unique ID.				

1.3 Account management

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 1.3 Provide management of all accounts directly in component or support such management in a common system.				
	Test: Login using an existing account to the target device. Disable the account used using account management. Retry login with the now disabled account. It shall not be possible to login when the account is disabled.				

1.4 Identifier management

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 1.4 Provide management of identifiers by user, group, role or control system interface, either directly in the component or support integration into a common system providing such identifier management. See guidance note in Sec.3 [1.1].				
	Test: Verify that the component supports identification on an entity using a central identifier management solution or directly.				

1.5 Secure authenticator management

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1, 2	Requirement: ISA-62443-4-2 CR 1.5 Support secure management of authenticator content, e.g. passwords. See guidance note in Sec.3 [1.1].				
	Test: — default installation authenticator can be modified — periodic authenticator change can be set — authenticator content storage and transmission is protected.				
3, 4	Requirement: ISA-62443-4-2 CR 1.5 (1) Hardware-based authentication, e.g. use of smart-cards, is required. See guidance note in Sec.3 [1.1].				
	Test: Confirm that by removing the hardware authentication device it is not possible to operate the component.				

1.6 Wireless access

Security level	*Node* **NO**	*Switch* **NO**	*Forwarder* **NO**	*Gateway* **YES**	*Border gateway* **NO**
1	Requirement: ISA-62443-4-2 NDR 1.6 A wireless gateway shall have be able to identify and authenticate all wireless connections.				
	Test: Verify that human users must log in to access the wireless gateway. Use the method/protocol specified by the vendor to verify that an application or embedded device must identify and authenticate itself to access the wireless gateway.				
2, 3, 4	Requirement: ISA-62443-4-2 NCR 1.6 (1) Unique identification and authentication of wireless connections shall be provided.				
	Test: Verify that any wireless connection requires unique identification.				

1.7 Strength of passwords

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Requirement: ISA-62443-4-2 CR 1.7 For components using password-based authentication, it shall be possible to enforce configurable password strength, either supported by the component itself or from a common system. Passwords shall not be stated in product documentation.				
	Test: Alter the applied password settings using the supported central configuration system, and verify that it is effected in the device by attempting a password change outside the set limits and then with a valid password.				
3	Requirement: ISA-62443-4-2 CR 1.7 (1) Human users shall not be able to reuse passwords. The component shall also have the capability to enforce lifetime restrictions on passwords for human users.				
	Test: Verify that the system disallows changing the password to a previous one. Confirm by observation that the system has a possibility to configure password expiration.				
4	Requirement: ISA-62443-4-2 CR 1.7 (1)(2) Password lifetime restrictions shall apply for all users.				
	Test: Confirm by observation that the system has a possibility to configure password expiration for non-human users.				

1.8 Public key infrastructure (PKI) certificates

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2, 3, 4	Requirement: ISA-62443-4-2 CR 1.8 When public key infrastructure (PKI) is utilized, use of PKI shall be according to ISA-62443-3-3 SR 1.8.				
	Test: Verify that certificate expirations dates are acceptable.				

1.9 Strength of public key authentication

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1	Not applicable				
2	Requirement: ISA-62443-4-2 CR 1.9 When public key infrastructure is utilized, validation of PKI certificates shall follow the requirements stated in the referred standard.				
	Test: Verify certification validation, e.g. by using an invalid, revoked certificate.				
3, 4	Requirement: ISA-62443-4-2 CR 1.9 (1) It shall be possible to protect the private keys via hardware.				
	Test: Verify that any private keys cannot be tampered with during installation or in storage.				

1.10 Obscure authentication information

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR1.10 During the authentication process (e.g. entering password), the application or component shall have the capability to obscure the authentication information. Any feedback given during the authentication process shall not give information that can be exploited by unauthorized individuals (e.g. by stating the reason for unsuccessful login).				
	Test: Verify obfuscation by observing valid authentication, and a combination of providing invalid authentication information (e.g. an invalid username and then an invalid password in a next try, if username/password pair is used to authenticate). Observe that no information is disclosed that could be used to brute force credentials.				

1.11 Unsuccessful login attempts

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 1.11 During the authentication process, the application or component shall restrict the number of consecutive login attempts. Such restriction shall apply for any access attempt (by human or by software). The limit of allowable login attempts shall be configurable. When the limit is reached, access shall be blocked for a specified period of time. See guidance note in Sec.3 [1.1].				
	Test: Verify by observation that failed login attempts lead to lockout.				

1.12 System use notification

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 1.12 The capability of displaying a configurable system use notification shall be implemented for components for which local authentication is provided. This requirement may not be related to security, but facilitates the use of e.g. warning messages or other information which should be given to the user. Displayed information shall not reveal critical information about the unit, such as exactly what kind/type of component it is, but should warn any users of the implications of unauthorized logins.				
	Test: Observe that appropriate and sufficient information, e.g. banner, is displayed during or before a login attempt.				

1.13 Access via untrusted networks

Security level	*Node* **NO**	*Switch* **NO**	*Forwarder* **NO**	*Gateway* **YES**	*Border gateway* **YES**
1, 2	Requirement: ISA-62443-4-2 NDR 1.13 Any attempted access from insecure/uncontrolled networks shall be monitored and managed by the gateway.				
	Test: Attempt to login from the untrusted side, using the protocol/application supported by the device, and verify that it is possible to monitor both successful and unsuccessful login attempts.				
3, 4	Requirement: ISA-62443-4-2 CR1.13 (1) A gateway installed onboard for access from onboard public networks or remote access from outside the vessel shall have the capability to deny access unless specifically authorized by an assigned role onboard. See also DNVGL-RU-SHIP Pt.4 Ch.9/DNVGL-OS-D202 requiring that remote access shall not be possible without acceptance and acknowledgment by the responsible person onboard the vessel.				
	Test: Attempt to login from the untrusted side, using the protocol/application supported by the device, and verify that it is not possible without acknowledgement from the internal side.				

1.14 Strength of symmetric key authentication

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2	Requirement: ISA-62443-4-2 CR 1.14 When symmetric key authentication is used, validation of the shared secret shall follow the requirements stated in IEC 62443-4-2 CR 1.14. Note on algorithms: MD5, SHA-0, SHA-1, DES, 3DES shall not be used. Proprietary encryption algorithms shall not be used. An asymmetric encryption algorithm shall provide at least 2048-bit key length, with encryption strength at least as strong as RSA; a symmetric encryption algorithm shall provide at least 256-bit key length with an encryption strength at least as strong as AES.				
	Test: See OWASP www.owasp.org/index.php/Guide_to_Cryptography. Verify that any private keys or certificate import files stored on the file system cannot be imported without authentication/password.				
3, 4	Requirement: ISA-62443-4-2 CR 1.14 (1) ISO/IEC 19790 Level 3 security for symmetric key is required.				
	Test: It shall be possible to protect the private keys via hardware.				

2 Use control

This subsection includes requirements for capabilities related to controlling how an identified and authenticated user may use (e.g. access, read, write, control) the component. Assignment of users with privileges and enforcement of restrictions is central to these requirements.

2.1 Enforcement of authorization

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Requirement: ISA-62443-4-2 CR 2.1 The component shall enforce authorization for all human users based on assigned role and least privilege. See guidance note in Sec.3 [1.1].				
	Test: If user accounts with different privilege levels exist, select a high privilege user account, log in and browse the features provided by the device. Subsequently, log in using an account with a lower privilege, and verify that some of the features are blocked for this second user account - as defined in supporting documentation.				
2	Requirement: ISA-62443-4-2 CR 2.1 (1)(2) Enforce authorization for all users. The component shall enable an authorized role to define and modify the permissions for all human users.				
	Test: Verify by observation that an authorized role exists with the above capability.				
3	Requirement: ISA-62443-4-2 CR 2.1 (1)(2)(3) The component shall provide support for manual override by a supervisor (higher privilege) role. The ability to perform manual override shall expire after a predetermined time or following a specified sequence of events.				
	Test: Authentication mechanisms for the supervisor override shall be described in the component's documentation. The operations which can be manually overridden shall be defined in the component's documentation and verified in the type test.				
4	Requirement: ISA-62443-4-2 CR 2.1 (1)(2)(3)(4) The component shall allow for approval by two different roles for actions that can result in serious/safety-related impact of the controlled process.				
	Test: Any actions which require such dual approval shall be described in the system documentation. The functionality of such dual approval shall be demonstrated in the type test.				

2.2 Wireless usage

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 2.2 If the component supports wireless communication, it shall support appropriate authorization, monitoring, and usage restriction mechanisms. Unique identification and authentication of all users is required.				
	Test: — Confirm that there are no generic/shared user identifiers accepted by the component (e.g. by listing all the configured user identifications). — Confirm authentication strength and usage restriction provided by the device (e.g. verify advertised security settings by wireless scanning). — Conform monitoring and logging functions (e.g. verify by accessing the device's management interface).				

2.3 Portable and mobile devices

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 2.3 Any component which may support the use of portable and mobile devices shall have capabilities to prevent or restrict the use of such devices (e.g. mobile phones, REDS, etc.).				
	Test: Enable portable device restriction supported by the device. Connect a supported portable device (e.g. USB stick), and verify that no data can be transferred to/from it.				

2.4 Mobile code

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Requirement: ISA-62443-4-2 SAR/EDR/HDR/NDR 2.4 Any component (host) which utilizes mobile code (e.g. Java, PDF, VBScript, etc.) shall have the capability to authenticate, authorize, and restrict execution of the mobile code. Transfer of mobile code to/from the component shall also be possible to restrict.				
	Test: Enable blocking of mobile code. Verify that no mobile code copied to the device or accessed by the device via network connection can be executed. Verify Java, JavaScript, ActiveX and VBScript blocking as a minimum, if no other mobile code technologies are explicitly supported.				
3, 4	Requirement: ISA-62443-4-2 SAR/EDR 2.4 (1) The host shall be capable of verifying the integrity of the mobile code before execution.				
	Test: Enable blocking of mobile code. Verify that no mobile code ,copied to the device, or accessed by the device via a network connection,- can be executed. Verify Java, JavaScript, ActiveX, and VBScript blocking as a minimum, if no other mobile code technologies are explicitly supported.				

2.5 Session lock

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 2.5 The component shall have the capability to implement session lock (e.g. logout or lock HMI) upon user request or after a configurable time of inactivity. See guidance note in Sec.3 [1.1].				
	Test: Verify by observation that time-based session lock (if applicable) kicks in after the configured time.				

2.6 Remote session termination

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2, 3, 4	Requirement: ISA-62443-4-2 CR 2.6 Remote access to applications or components from outside of the trusted network shall be controlled such that the user initiating the remote session (i.e. on board) can at any time terminate the session. The onboard applications or components supporting such remote sessions shall also have the capability to automatically terminate the session after a configurable time period of inactivity. See also Sec.3 [8].				
	Test: — Verify that a remote session is torn down after the configured time period is elapsed. — Verify that the user can terminate an ongoing session. — Monitor the network traffic to verify that the relevant network connections are terminated.				

2.7 Concurrent session control

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Not applicable				
3, 4	Requirement: ISA-62443-4-2 CR 2.7 It shall be possible to configure maximum number of concurrent sessions per network interface. See also to DoS protection Sec.3 [7.1].				
	Test: If possible by network traffic simulation, generate the maximum number of valid network sessions to the device. Verify that an additional network session gets blocked.				

2.8 Audit information

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 2.8 It shall be possible to generate audit records of security related events as relevant for the functionality provided by the component.				
	Test: Verify that log entries are sufficiently verbose, and according to requirements both with respect to event types and content of records.				

2.9 Audit storage

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Requirement: ISA-62443-4-2 CR 2.9 The component shall have sufficient audit storage capacity, and shall be able to prevent failure when storage capacity is exceeded.				
	Test: Generate events until the specified storage capacity is exhausted, observe if the system remains functional.				
3, 4	Requirement: ISA-62443-4-2 CR 2.9 (1) An alarm shall be generated when a configurable storage threshold is reached.				
	Test: Generate events until the specified storage capacity threshold is reached, observe alarms.				

2.10 Audit processing

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 2.10 The component shall be able to detect failures in the generation/processing of audit records. The component shall respond in a safe and predictive manner upon failures in audit processing.				
	Test: Verify that product documentation describes response to audit processing failures. Verification by testing may be required depending on the described functionality.				

2.11 Timestamps

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Requirement: ISA-62443-4-2 CR 2.11 The component shall have the capability of timestamping security events.				
	Test: Simulate events to generate up to five (5) alarms, verify timestamps in the device's log.				
3	Requirement: ISA-62443-4-2 CR 2.11 (1) The time-stamping shall be synchronized with a system wide time source, e.g. via (S)NTP.				
	Test: Simulate a local time source and configure the device to use it. Verify that time is correctly synchronized with the local simulated time source.				
4	Requirement: ISA-62443-4-2 CR 2.11 (1)(2) Any alteration of the time synchronization mechanism shall be subject to authorization. Unauthorized alteration shall be logged as an event.				
	Test: Modify external time source configuration and observe event logging.				

2.12 Non-repudiation for user actions

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Not applicable				
3	Requirement: ISA-62443-4-2 CR 2.12 The component shall be able to determine if an action taken has been performed by a human user.				
	Test: Modify at least three different settings in the device's configuration, and review the corresponding log. Verify that the events were logged.				
4	Requirement: ISA- CR 2.12 (1) The component shall provide non-repudiation capabilities for all users.				
	Test: Modify at least three different settings (using different user accounts) in the device's configuration, and 62443-4-2 review the corresponding log. Verify that the events were logged including user identification.				

2.13 Unauthorized access to test interfaces

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2	Requirement: ISA-62443-4-2 EDR 2.13/HDR 2.13/NDR 2.13 Interfaces for diagnostics and testing shall be protected from unauthorized use.				
	Test: Identify such interfaces by document assessment. Test that such interfaces are subject to restricted use in accordance with requirements for identification, authentication and authorization.				
3, 4	Requirement: ISA-62443-4-2 EDR 2.13(1)/HDR 2.13(1)/NDR 2.13(1) Any use of such test interfaces shall be monitored and logged, see Sec.3 [2.8].				
	Test: Verify that monitoring information is logged as specified by the referenced requirements.				

2.14 REDS security, USB

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***NO***
1, 2, 3, 4	Requirement: The component shall only have REDS needed for necessary operation, maintenance and support. Usage of licensed dongles shall be documented, including the relevant procedures and protection measures for their usage. REDS connections without physical protection shall be limited to device class 08_{hex} (mass storage). All other REDS connection points such as human interface device (HID) ports for equipment necessary for operation shall be physically protected/blocked (e.g. for keyboards, mouse) or disabled (e.g. SD cards).				
	Test: — Verify restriction of access on unused REDS connection points. — Verify restriction of usage and protection measures for USB ports for keyboards, mice, licensed dongles, etc. — Verify limitation to device class 08_{hex} (mass storage) for other USB ports.				

2.15 REDS security, executables

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***NO***
1, 2, 3, 4	Requirement: IEC 61162-460 Sec.6.2.3.3 Automatic execution from REDS including auto-run is not accepted. Manual execution of programs shall be subjected to authentication, and limited to files verified in advance.				
	Test: It shall be demonstrated that auto-run is not possible and that manual execution of programs requires specific authentication.				

2.16 Limited access to underlying operating system

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: It shall not possible to open any interface that provides access to file systems or other OS functions unless restricted in accordance with requirements for identification, authentication and authorization (e.g. administrator).				
	Test: Verify that in a windowing system it is not possible to open any OS windows or other interfaces besides the designated user interface. (E.g. in Microsoft windows OSs WIN+E, WIN+R, right-click, etc.) Insert CD-ROM with autorun, insert USB with autorun, use short-keys (alt-F4), stickey-keys (keep shift depressed, or tap five (5) times) and break-keys (ctr-alt-del, ctrl-c). If open file, printer or help dialogs can be opened, try to abuse by right click to open explorer/cmd instances or cause software exceptions, forcing a drop to desktop.				

3 System integrity

This subsection includes requirements for capabilities related to protecting the integrity of the component, including its data and software.

3.1 Communication integrity

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Requirement: ISA-62443-4-2 CR 3.1 The device shall be capable of protecting the integrity of the data being transmitted/received.				
	Test: Verify that the data (payload) transmitted/received, via common or proprietary protocols, has integrity checking in the form of for example CRC protection.				
3, 4	Requirement: IEC 62443-4-2 CR 3.1 (1) Authentication of communicated data shall be supported (e.g. by cryptographic mechanisms).				
	Test: Verify by monitoring that the data transmitted/received is encrypted. Other mechanisms to authenticate the data shall be verified as per manufacturer documentation and test program.				

3.2 Malicious code protection

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 SAR 3.2/EDR 3.2/HDR 3.2/NDR 3.2 Malware protection shall be provided either as part of the component or by compensated controls (e.g. OS lock-down, REDS security measures, application and process whitelisting) implemented in the system and by security policies. The applicable protection mechanisms shall be supported by the device and they shall not interfere with control functions. Manufacturer documentation shall pinpoint the protection methods and required configuration options. Host devices shall support malware protection and report the version of such protection software.				
	Test: Evaluate threat vectors and compensating controls. Verify that no malicious code can be executed on the component, e.g. by using an EICAR sample and file transfer.				

3.3 Verification of security functions

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3	Requirement: ISA-62443-4-2 CR 3.3 The component shall have capabilities to support verification of the implemented security functions according to IEC 62443-3-3 SR3.3.				
	Test: The type test program shall include and describe verification of security functions according to the referenced standards.				
4	Requirement: ISA-62443-4-2 CR 3.3 (1) The component shall support automated verification of security functions during normal operation. This capability/functionality shall not compromise the intended operation of the component/system.				
	Test: Verify the operation of the implemented security functions according to vendor documentation, while the component is in normal operational mode.				

3.4 Software and information integrity

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2	Requirement: ISA-62443-4-2 CR 3.4 (1) The component shall have capability to perform/support and report integrity checks of software, configuration and other data. In addition, authenticity of software, configuration and other data shall be verified either by functions implemented in the component itself of by an integrated system.				
	Test: If the device supports (re-)configuration via configuration files, attempt to load a corrupted configuration file to the device and verify that configuration change is not possible via corrupted files. Other implemented integrity checks such as e.g. incompatible software versions or erroneous configuration shall be demonstrated according to product documentation.				
3, 4	Requirement: ISA-62443-4-2 CR 3.4 (1)(2) If the component itself performs the integrity check, it shall issue an alarm (via the method implemented by the component) upon detected violations.				
	Test: Verify that appropriate alarms are issued when a corrupted configuration is attempted to be loaded.				

3.5 Input validation

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 3.5 Input validation shall be implemented and applies for input from human users and from other components. Sufficient input-validation shall be implemented on the network interfaces of the device for the set of supported protocols. The device shall be able to handle malformed traffic on protocols and interfaces without getting in a non-responsive state.				
	Test: Demonstrate robustness according to e.g. ISASecure EDSA-310, and EDSA-401 through -406. See document EDSA-100-2.8, *EDSA-100 ISA Security compliance institute - Embedded device security assurance - ISA Secure certification scheme* Ver.2.8, December 2014. (http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification).				

3.6 Deterministic output

Security level	*Node* ***YES***	*Switch* ***NO***	*Forwarder* ***NO***	*Gateway* ***NO***	*Border gateway* ***NO***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 3.6 A node shall be capable of setting outputs which control a process to a predetermined safe state if normal operation cannot be continued.				
	Test: Monitor the output(s) of the device during abnormal states of the component and its interfaces. Component or system documentation shall describe the abnormal states and the corresponding fail-to-safe responses.				

3.7 Identification and handling of error conditions

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 3.7 The component shall be able to detect, identify and report (i.e. issue an alarm) failures and errors. The response shall be according to applicable fail-safe requirements in class rules. Error messages shall not aid exploitation of the component.				
	Test: Trigger alarms of all implemented severity levels and monitor them. Verify that no unnecessary and sensitive information is exposed in alarms transmitted by the device over a network connection.				

3.8 Session integrity

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2	Requirement: ISA-62443-4-2 CR 3.8 The component shall protect authenticity of communication sessions and validity of transmitted information.				
	Test: Demonstrate mechanisms described in the component/system documentation.				
3	Requirement: ISA-62443-4-2 CR 3.8 (1)(2) Session identifiers shall be unique for each session and invalidated upon logout or other termination of the session. Only system-generated identifiers shall recognized by the component.				
	Test: Verify that sessions are invalidated after logout.				
4	Requirement: ISA-62443-4-2 CR 3.8 (1)(2)(3) Random session identifiers shall be generated.				
	Test: Verify that no patterns from pseudo-random generation of session IDs is observable. See OWASP Testing guide v4, OTG-SESS-001, which is freely available on internet (https://www.owasp.org).				

3.9 Audit information integrity

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2, 3	Requirement: ISA-62443-4-2 CR 3.9 Audit information such as records, logs, reports, settings and tools shall be protected from unauthorized access.				
	Test: Access audit logs and tools supported by the device with a standard and a highest-privileged user account (if applicable) and verify that it is not possible to change or delete records.				
4	Requirement: ISA-62443-4-2 CR 3.9 (1) It shall be possible to store audits logs on write-once media.				
	Test: Verify by observation that a physical write-once media is utilized for storing logs.				

3.10 Updates

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Requirement: ISA-62443-4-2 EDR 3.10/HDR 3.10/NDR 3.10 It shall be possible to update/upgrade the component. Redundancy or other means to maintain essential vessel functions while performing the update shall be supported.				
	Test: Verify by document assessment that relevant information for updating the component is available (e.g. instructions, release notes). Demonstrate the ability to maintain the supported vessel function while updating the component.				
3, 4	Requirement: ISA-62443-4-2 EDR 3.10(1)/HDR 3.10(1)/NDR 3.10(1) Mechanisms shall be implemented in the component to ensure the update is authentic (i.e. source), free of errors and complete prior to installation. Firmware/software and configuration updates should only be possible via authenticated means. If REDS are to be used, compensating (e.g. physical) security measures shall be in place.				
	Test: Verify by document assessment that mechanisms such as signed patches and checksums are applied. It is not required that the component shall automatically reject e.g. unsigned updates, but the user shall in such case be notified and given the choice to abort or proceed with the update. If firmware or configuration is to be updated by REDS, such as USB devices, verify the compensating physical security measures are in place.				

3.11 Physical tampering

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2	Requirement: ISA-62443-4-2 EDR 3.11/HDR 3.11/NDR 3.11 The component shall be designed to detect and prevent physical tampering.				
	Test: Such properties shall be verified by physical inspection.				
3, 4	Requirement: ISA-62443-4-2 EDR 3.11(1)HDR 3.11(1)/NDR 3.11(1) Automatic detection and monitoring of physical tampering shall be implemented. The event shall be logged and reported to authorized personnel.				
	Test: Verify by document assessment the nature of physical tampering which will be detected, logged and reported. If possible and non-destructive, this capability shall be tested.				

3.12 Supplier roots of trust

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1	Not applicable				
2, 3, 4	Requirement: ISA-62443-4-2 EDR 3.12/HDR 3.12/NDR 3.12 The component shall possess mechanisms to validate hardware, software and data from product supplier(s).				
	Test: Root of trust hardware mechanisms shall be tested/demonstrated.				

3.13 Asset owner roots of trust

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1	Not applicable				
2, 3, 4	Requirement: ISA-62443-4-2 EDR 3.13/HDR 3.13/NDR 3.13 The component shall possess mechanisms to validate the origin, authenticity and integrity of software and data which will be implemented by the asset owner. Confidentiality of such data shall be protected. These mechanisms shall not rely on components outside of the component's security zone.				
	Test: Verify by inspection that the documented capabilities are implemented and sufficient.				

3.14 Integrity of boot process

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1	Requirement: ISA-62443-4-2 EDR 3.14/HDR 3.14/NDR 3.14 To prevent booting into an insecure or invalid state, the component shall ensure integrity of necessary software and data.				
	Test: Relevant mechanisms shall be described, subject to document assessment. If applicable, verify with invalid configuration or invalid firmware that integrity breach detection is implemented.				
2, 3, 4	Requirement: ISA-62443-4-2 EDR 3.14(1)/HDR 3.14(1)/NDR 3.14(1) Supplier roots of trust (see [3.12]) shall be verified prior to booting.				
	Test: Verify that it is not possible to tamper with the configuration or firmware through the booting process (e.g. manually interrupting it).				

3.15 Security following a reboot

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1, 2, 3, 4	Requirement: Login during reboot shall not possible or shall be secure.				
	Test: Verify that during the reboot procedure of the device under test all login attempts are either denied or handled in a secure way.				

3.16 No basic webserver vulnerabilities

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1, 2, 3, 4	Requirement: If the device has a webserver built-in, there shall be no known vulnerabilities present in it. As a minimum, a password protected login screen shall guard access to the webserver.				
	Test: Verify that in order to login to the device at least a basic username/password combination is requested on the default landing page. Test for basic, known vulnerabilities using a web application vulnerability scanner.				

3.17 Firmware change

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1, 2, 3, 4	Requirement: There shall be no possibility for an unauthenticated change of firmware, not even via replacement of physical media.				
	Test: Verify physical protection of firmware storage media. Verify that firmware update from removable storage or via a network interface requires authentication and can only be conducted in a secure manner (e.g. man-in-the-middle attacks).				

3.18 Firmware version

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: The component should run the latest firmware version from its vendor. A release note shall exist for each firmware version. If application of older firmware versions is expected to be necessary, e.g. due to system compatibility issues, sufficient vendor documentation has to be available to support implementation of appropriate compensating actions. The main principle is that the firmware installed in the device should not have a publicly known vulnerability. E.g. if a vendor advisory exists advising a newer firmware version, this shall be followed.				
	Test: Verify firmware version using a configuration interface supported by the device.				

4 Data confidentiality

This subsection includes requirements for capabilities related to protection of confidentiality, i.e. preventing unauthorized disclosure of information.

4.1 Confidentiality of information

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 4.1 The component shall be able to protect confidentiality of information and avoid exposing operational data to unauthorized parties. For example, if the device has SNMP capability, it shall not leak any security critical data via responding to SNMP requests.				
	Test: Verify that the device does not leak critical information via the supported services/protocols, e.g. the most common ones: via HTTP(S), SNMP, or NetBIOS. Connect to the device using the supported protocols, and enumerate any information that can be obtained without authentication.				

4.2 Purging of authentication information from end-of-life components

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2	Requirement: ISA-62443-4-2 CR 4.2 Upon decommissioning of the component, it shall be possible to purge all information which has been defined by policies as subject to authorization.				
	Test: Test factory default reset functionality, and verify that activating it clears all sensitive information from the device.				
3, 4	Requirement: ISA-62443-4-2 CR 4.2(1)(2) Specific mechanisms shall be implemented to ensure that volatile shared memory is confirmed purged to avoid unintended transfer of information.				
	Test: Verify that the contents of volatile storage are not available after its removal, or after the respective device is power-cycled.				

4.3 Cryptography

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 4.3 If the component utilizes encryption, the following requirements apply: — Algorithms: MD5, SHA-0, SHA-1, DES, 3DES should not be used. — Proprietary encryption algorithms shall not be used. — An asymmetric encryption algorithm shall provide at least 2048-bit key length, with encryption strength at least as strong as RSA; a symmetric encryption algorithm shall provide at least 256-bit key length with an encryption strength at least as strong as AES.				
	Test: Inspect traffic from/to the component and verify it is encrypted appropriately.				

5 Restricted data flow

This subsection includes requirements for capabilities related to control of data flow/communication to support segmentation of a system into zones and conduits.

5.1 Network segmentation

Security level	*Node* **NO**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 5.1 The component shall support provisioning of a segmented network. Network segmentation can be employed to improve performance and security of the overall network, by supporting multiple zones with varying requirements in a network.				
	Test: Demonstrate that a probe placed in one network segment cannot be reached from another (to be separated) segment. Depending on the technology used for segmentation, use a probe and connection initiator as appropriate.				

5.2 Firewall

Security level	*Node* **NO**	*Switch* **NO**	*Forwarder* **NO**	*Gateway* **YES**	*Border gateway* **YES**
1	Requirement: ISA-62443-4-2 NDR 5.2 The device providing boundary protection shall be capable of filtering and monitoring traffic.				
	Test: Verify that component has functionality to configure blocking and monitoring of a given network stream traversing it.				
2	Requirement: ISA-62443-4-2 NDR 5.2 (1) The component shall by default deny all network traffic crossing the zone boundary and permit only traffic by exception.				
	Test: Verify that direct connections to the protected network are disabled by default.				
3	Requirement: ISA-62443-4-2 NDR 5.2 (1)(2)(3) The component shall be able to work in an "island mode" where no traffic can cross the boundary. The component shall respond to failures in the boundary protection in a fail-safe manner, i.e. it shall revert to island mode.				
	Test: Verify firewalling capability by performing the following steps as a minimum: — Full scan of all TCP/UDP ports, including IP fragmentation scan. — ACL mapping by fire-walking from both insecure and secure zones. — Test tunneling from the secure side, using e.g. ICMP, DNS, SSH, or HTTP. If it is possible to configure the component with an invalid configuration (e.g. delete all ACL rules), verify that all connections through the device are denied in a failure state.				
4	Requirement: The component shall have state-of-the-art firewalling functions, such as stateful inspection, and deep packet inspection (DPI).				
	Test: Verify advanced firewalling capability at least testing with ICMP, or DNS, or HTTP tunneling.				

5.3 User content filtering

Security level	*Node* **NO**	*Switch* **NO**	*Forwarder* **NO**	*Gateway* **YES**	*Border gateway* **YES**
1, 2, 3, 4	Requirement: 62443-4-2 NCR 5.3 The gateway shall provide capabilities for identifying and blocking communication violating security policies, e.g. social media content, transfer of images, etc.				
	Test: Verify that sites violating security policies, e.g. common social media sites, can be blocked.				

5.4 DNS exfiltration

Security level	*Node* ***YES***	*Switch* ***NO***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: No hidden communications channel can be established on the device via DNS exfiltration, DNS servers are configured to disallow resolution of untrusted or external hosts.				
	Test: Verify that relaying DNS queries to arbitrary internet-based name-servers (to form an uncontrolled communication channel) is not possible. Quick-check: resolution of "exfilt-test.energysec.org" does not return a valid IP address (e.g. 10.0.0.9).				

5.5 Guarded DHCP service

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3	Requirement: If the device is running a DHCP server, the service shall be guarded, i.e. an unauthorized unit shall not get an IP address assigned automatically from the device.				
	Test: Verify that it is possible to configure and enforce a list of clients (e.g. by MAC address) that are allowed to gain IP access.				
4	Requirement: Rogue DHCP servers shall be detected.				
	Test: Simulate a rogue DHCP server (e.g. DHCP reply and advertisement) and verify that it is detected.				

5.6 Switch loop prevention

Security level	*Node* ***NO***	*Switch* ***YES***	*Forwarder* ***NO***	*Gateway* ***NO***	*Border gateway* ***NO***
1, 2, 3, 4	Requirement: IEC 61162-460 Sec.5.2.2 The switch shall have capabilities for preventing switching loop in all interfaces, for example RSTP, MSTP or other protocols.				
	Test: IEC 61162-460 Sec.10.6.2 Refer to verification and tests described in the referenced standard.				

6 Timely response to events

This subsection includes requirements for capabilities related to monitoring, recording and response to security related events.

6.1 Audit information accessibility

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2	Requirement: ISA-62443-4-2 CR 6.1 Audit records required by Sec.3 [2.8] shall be accessible on read-only basis, subject to authorization.				
	Test: Verify that manual read-only access to audit logs is available (and subject to authorization).				
3, 4	Requirement: ISA-62443-4-2 CR 6.1(1) It shall be possible to access audit records using an application programming interface (API) for analysis and other event management purposes.				
	Test: Demonstrate access to audit logs using the vendor's API. Verify that API access is not possible without using the appropriate credentials.				

6.2 Continuous monitoring

Security level	*Node* ***NO***	*Switch* ***NO***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1	Not applicable				
2, 3, 4	Requirement: ISA-62443-4-2 CR 6.2 It shall be possible to continuously monitor security mechanisms which are provided by a component. Such monitoring may be performed e.g. by a dedicated intrusion detection system (IDS) or intrusion prevention system (IPS).				
	Test: Manufacturer shall document and/or demonstrate that all implemented security mechanisms are continuously monitored or can be continuously monitored e.g. by event recording or dedicated devices.				

7 Resource availability

This subsection includes requirements for capabilities related to availability of the component.

7.1 Denial of service protection

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***NO***
1	Requirement: ISA-62443-4-2 CR 7.1 The application or component shall be able to cope with a DoS event. If normal operation is not possible, depending on the DoS situation, the component shall revert to a degraded mode where essential functions, safety functions and local control functions are maintained. Any effects shall comply with applicable fail-safe principles. The component shall stay functional and can be operated as expected by an operator under network stress situations. Warnings or alarms are issued correctly for the component that is subjected to high network loads. Maximum input and output bandwidth for a node shall be stated in manufacturer documentation.				
	Test: IEC 61162-460 Sec.10.5.2.2 To test DoS protection, at least load stress testing consisting of valid traffic shall be done. Valid traffic shall be generated: 1) at a rate less than the saturation rate threshold specified by the vendor (e.g., simulating normal but busy plant conditions) 2) up to the full auto-negotiated link rate (e.g., simulating an attack or malfunction). Saturation rate testing shall be executed for durations long enough for any saturation effects to manifest (e.g. at least tens of seconds, in some cases much longer). Stress testing shall use deterministic traffic generation, and target unicast, broadcast and multicast addresses if applicable. Traffic generation for stress testing shall cover the protocols supported by the device.				
2, 3, 4	Requirement: ISA-62443-4-2 CR 7.1(1) Means provided to ensure operation of the node in a DoS event shall be implemented and described in manufacturer documentation, e.g. rate limiting. DoS prevention methods in switch, forwarder and gateway shall be implemented and described in manufacturer documentation.				
	Test: IEC 61162-460 Sec.10.6.3.2, Sec.10.7.4.2, Sec.10.8.1 and Sec.10.12.3.7 Test network resilience with unicast, multicast and broadcast traffic addressing the protocols relevant in the network where the component is going to be typically deployed into. This test should cover at least the following layers: ethernet/data link layer, IPv4/network layer, and TCP, UDP/transport layer. If applicable, simulate other DoS conditions to verify that the implemented mitigation mechanisms are working.				

7.2 Resource management

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **NO**
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 7.2 The component shall have the capability to manage resources such that low-priority processes (e.g. network scans) are prevented from interfering with higher priority processes (e.g. control, monitoring, alarm functions).				
	Test: Manufacturer documentation shall describe specific mechanisms ensuring high-priority functions are not affected by security functions. Such resource management mechanisms shall be tested as part of other tests in this CP, e.g.: — malicious code protection — DoS protection — audit storage — switch loop prevention — backup. CPU consumption (by low priority processes) tolerance may be tested using software tools, e.g. in case of Unix-based OS stress-ng, or in MS Windows OS consume.exe, run as given user.				

7.3 Backup

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **NO**
1	Requirement: ISA-62443-4-2 NCR 7.3 The component shall support system level backup operations.				
	Test: Perform system backup (if possible in type test) and verify that backup can be restored.				
2	Requirement: ISA-62443-4-2 NCR 7.3 (1) Successful execution of the backup shall be verified without need for manual actions. An alarm shall be produced if faults have occurred including if the integrity of the backup is compromised. The component shall also be able to validate the backup before restore.				
	Test: Validation of backup information shall be tested.				
3, 4	Requirement: ISA-62443-4-2 NCR 7.3 (1)(2) It shall be possible to perform a local backup of the component.				
	Test: Restore local backup.				

7.4 Retainment of configuration

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **NO**
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 7.4 Upon restoration of power after a switch-off or power failure, the component shall start/boot, ready for the intended operation, without loss of any configuration (i.e. previous configuration shall be retained). Following other failures or disruptions, it may be accepted that the component reverts to a predetermined safe and secure state.				
	Test: Document the component's configuration settings, switch off the component, re-apply power to the component and verify that it starts completely and that configuration settings are maintained. See also electrical power supply failure test in DNVGL-CG-0339.				

7.5 Network and security configuration settings

Security level	*Node* **YES**	*Switch* **YES**	*Forwarder* **YES**	*Gateway* **YES**	*Border gateway* **YES**
1, 2	Requirement: ISA-62443-4-2 CR 7.6 The component shall be delivered with default network and security configuration settings in accordance with recommended manufacturer settings and in accordance with this Type Approval Programme. Modifications of the settings shall be in accordance with security policies and requirements in this CP.				
	Test: — Verify that the device's default configuration is per the recommendations by the vendor. — Verify configuration file required in Sec.2 [2.6].				
3, 4	Requirement: ISA-62443-4-2 CR 7.6(1) The component shall be able to generate a machine-readable report, or export its configuration to a file, with its current security settings.				
	Test: Export the machine-readable configuration report and import and read it by the vendor supplied processing tool, or a compatible analysis tool.				

7.6 Least functionality

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: ISA-62443-4-2 CR 7.7 Applications or components serving essential and important functions shall have capability to prevent installation, enabling or use of unnecessary or irrelevant functions, ports, protocols and/or services.				
	Test: Verify e.g. that no unnecessary UDP or TCP ports are open by scanning the device.				

7.7 Component inventory

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***NO***
1	Not applicable				
2, 3, 4	Requirement: ISA-62443-4-2 CR 7.8 It shall be possible to identify the component's hardware and software type and version. This includes version/revision of configurable elements. See also Sec.2 [2.6].				
	Test: Verify that the properties listed in the requirement are reported by/or visible on the component.				

8 Specific systems and applications

Security requirements in this subsection apply as relevant when components are designated for use in specific system applications such as remote support access, wireless topologies, monitoring stations in insecure areas, etc.

Any relevant requirements in the previous subsections apply.

The requirements adopt the concept of controlled/uncontrolled network defined in IEC 61162-460. This CP will not define an exact relationship between zones with specific target security levels (IEC 62443) and controlled networks (IEC 61162-460). However, for this type approval programme, a controlled network shall be regarded as a secure zone at a defined security level.

The requirements are based on IEC 61162-460, but do not intend to be aligned with all contents in this standard.

8.1 Network access control from (physically) insecure areas

Security level	*Node* ***NO***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***NO***	*Border gateway* ***NO***
1, 2, 3, 4	Requirement: IEC 61162-460 Sec.6.2.4.2 and IEC 61162-460 Sec.4.7 If the device, or connections to it, is intended to be installed (physically) outside of a protected area, it should provide the means to control network access (e.g. MAC-address based admission), and protect the network from unauthorized device connections				
	Test: IEC 61162-460 Sec.10.6.3.4 and IEC 61162-460 Sec.10.7.4.4 Verify by testing in accordance with referenced requirements.				

8.2 Direct communication to controlled network

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***YES***	*Border gateway* ***YES***
1, 2, 3, 4	Requirement: IEC 61162-460 Sec.6.3.2.3 Direct communication from an uncontrolled network to a component inside the controlled network is in principle not allowed. See [5.2] (firewall) for requirements to filtering and firewalling capabilities. Communication from uncontrolled to controlled networks shall be implemented through a gateway compliant with the requirements in this CP, in such case the direct communication shall be specifically permitted by the responsible role onboard the vessel. Such direct communication shall be subject to relevant requirements in this CP (i.e. identification and authentication, use control, integrity, confidentiality, etc.) Communication to onboard marine and other control systems shall happen via a jump-host in a DMZ onboard. Communication to a controlled network from another controlled network shall be implemented through a forwarder compliant with the requirements in this CP.				
	Test: Verify that, when relevant, manufacturer documentation describes communication mechanisms from outside to a controlled network. See also relevant tests for authentication and restriction/monitoring of data flow.				

8.3 Direct communication to uncontrolled network

Security level	*Node* ***YES***	*Switch* ***NO***	*Forwarder* ***NO***	*Gateway* ***YES***	*Border gateway* ***NO***
1	Requirement: IEC 61162-460 Sec.6.3.4 A node shall only be able to communicate to components outside of the controlled network through a gateway. When a connection to an uncontrolled network is realized, a permanent indication shall be activated. Indication of this connection shall be supported by the component, but not necessarily be provided by it. Communication shall always be opened from the ship side, by authorized members of the crew.				
	Test: IEC 61162-460 Sec.10.5.2.5 — Verify that, when relevant, manufacturer documentation describes communication mechanisms from a controlled network to uncontrolled networks. — Verify that a connection to an uncontrolled network is not possible until activation from a node in the controlled network. — Verify that a test-probe placed outside the controlled network can only be reached from the node via a gateway, by monitoring traffic at the probe, and on the uncontrolled side of the gateway attached to the device under test. — Verify that when a connection to an uncontrolled network is realized a permanent indication is activated.				
2	Requirement: Two-factor authentication shall be applied to enable communication (e.g. SMS). An intermediate jump-host shall be used on-board. All incoming connections shall land at the jump-host. Communication via the device shall be encrypted. File-transfers shall undergo a malware check.				
	Test: — Verify that it is not possible to access the controlled network evading the jump-host. — Verify that the active connection to the uncontrolled network is appropriately encrypted by monitoring the connection on the uncontrolled side of the associated gateway. — Verify that it is not possible to upload to a malicious file.				
3, 4	Requirement: Stronger two-factor authentication shall be implemented (e.g. smart-card based). Advanced user management and event-logging for compliance shall be implemented.				
	Test: Create a successful and an unsuccessful login, a verify that the sessions are logged.				

8.4 DMZ jump-host

Security level	*Node* **YES**	*Switch* **NO**	*Forwarder* **NO**	*Gateway* **YES**	*Border gateway* **YES**
1, 2	Requirement: A DMZ jump-host is an intermediate host deployed in a demilitarized zone, used to enable indirect remote access to a secure network. If the node is to assume to the role of a jump-host, the following requirements apply. Requirement: IEC 61162-460 Sec.6.3.5.2, Sec.6.3.5.3, and Sec.6.3.4 The jump-host shall be running a hardened operating system, and access to it shall be controlled and monitored. If the component provides application server functionality, it provides access to resources, e.g. data, shared between clients in controlled and uncontrolled networks. In addition to requirements in IEC 61162-460 Sec.6.3.5.2, if the component provides application server functionality it shall comply with the requirements for a node, cf. IEC 61162-460 Sec.6.3.4. If the component provides access to stored files that can be accessed from controlled and/or uncontrolled networks, trusted protocols shall be employed for the service.				
	Test: IEC 61162-460 Sec.10.8.5 and Sec.10.8.6 — Test if anti-virus solution is deployed and operational. If anti-virus software is intentionally not installed, verify compensating actions. — Verify that the application server is not acting as a gateway itself, i.e. does not route packets through itself. — Verify (e.g. by scanning) that no fundamentally insecure file sharing protocols are enabled on the device under test.				
3, 4	Requirement: — The jump-host shall be accessed via two-factor authentication. — Hardening of the jump-host shall include process/application whitelisting. — The jump-host shall not have outgoing Internet-access. — In addition, strict event logging shall be applied on the jump-host.				
	Test: Verify patch-level, application/process whitelisting, and blocked Internet-access.				

8.5 Wireless connections

Security level	*Node* **NO**	*Switch* **NO**	*Forwarder* **NO**	*Gateway* **YES**	*Border gateway* **NO**
1, 2, 3, 4	Requirement: IEC 61162-460 Sec.6.3.6 If the component supports wireless networking, it shall only operate as a client (i.e. not as an access point), without any traffic forwarding from/to any wireless network. A device shall not have any undocumented, or implicitly enabled e.g. bluetooth, ZigBee or other wireless connectivity.				
	Test: IEC 61162-460 Sec.10.9.2 — Verify using wireless scanning software that the device does not have undocumented connectivity. — Verify that access point and forwarding functions are not active.				

8.6 Wireless LAN and VLAN tunneling

Security level	*Node* ***YES***	*Switch* ***YES***	*Forwarder* ***YES***	*Gateway* ***NO***	*Border gateway* ***NO***
1, 2, 3, 4	Requirement: IEC 61162-460 Sec.6.2.1 Node, switch and forwarder shall not utilize VLAN (802.1Q, Q-in-Q) tunneling and should prevent VLAN hopping attacks. Node , switch, and forwarder shall not function as a wireless access point (AP). Wireless communication to components inside a controlled network shall consequently be implemented through a wireless gateway (AP) that is compliant with the requirements for a gateway in this CP.				
	Test: IEC 61162-460 Sec.10.5.2.1, Sec.10.6.3.1 and Sec.10.7.4.1 If VLAN is provided for node, switch or forwarder, check that VLAN tunneling is disabled and verify that VLAN hopping is prevented. Check that wireless LAN interface or wireless AP functions are not implemented or can be disabled.				

CHANGES – HISTORIC

There are currently no historical changes for this document.

About DNV GL

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations 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 and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our experts are dedicated to helping our customers make the world safer, smarter and greener.

SAFER, SMARTER, GREENER