RUSSIAN MARITIME REGISTER OF SHIPPING

CIRCULAR LETTER	**No. 315-12-1630c**	dated 16.09.2021

Re:

amendments to the Rules for Technical Supervision during Construction of Ships and Manufacture of Materials and Products for Ships, 2021, ND No. 2-020101-139-E

Item(s) of supervision:

cyber safety equipment

Entry-into-force date:
01.11.2021

~~Cancels / amends / adds Circular Letter No.~~ ~~dated~~

Number of pages: 1 + 12

Appendices:

Appendix 1: information on amendments introduced by the Circular Letter

Appendix 2: text of amendments to Part IV "Technical Supervision during Manufacture of Products"

Director General Konstantin G. Palnikov

Text of CL:

We hereby inform that the Rules for Technical Supervision during Construction of Ships and Manufacture of Materials and Products for Ships shall be amended as specified in the Appendices to the Circular Letter.

It is necessary to do the following:

1. Bring the content of the Circular Letter to the notice of the RS surveyors, interested organizations and persons in the area of the RS Branch Offices' activity.
2. Apply the provisions of the Circular Letter when performing technical supervision during manufacture of equipment/products requested on or after 01.11.2021.

List of the amended and/or introduced paras/chapters/sections:

Part IV: Section 18

Person in charge:	Andrey V. Kunavin	315	+7 (812) 380-19-92

"Thesis" System No. 21-200636

Appendix 1 to Circular Letter
No. 315-12-1630c dated 16.09.2021

Information on amendments introduced by the Circular Letter
(for inclusion in the Revision History to the RS Publication)

Nos.	Amended paras/chapters/ sections	Information on amendments	Number and date of the Circular Letter	Entry-into-force date
1	Part IV	New Section 18 has been introduced	315-12-1630c of 16.09.20221	01.11.2021

Appendix 2 to Circular Letter
No. 315-12-1630c dated 16.09.2021

RULES FOR TECHNICAL SUPERVISION DURING CONSTRUCTION OF SHIPS AND MANUFACTURE OF MATERIALS AND PRODUCTS FOR SHIPS, 2021,

ND No. 2-020101-139-E

PART IV. TECHNICAL SUPERVISION DURING MANUFACTURE OF PRODUCTS

New Section 18 is introduced reading as follows:

"18 CYBER SAFETY EQUIPMENT AND SYSTEMS

18.1 TERMS AND DEFINITIONS

18.1.1 The following definitions and abbreviations are used for the purposes of this Section.

460-Switch is a network infrastructure device used to interconnect nodes on a 460-Network and which satisfies the safety and security requirements as specified in this Section.

460-Forwarder is a network infrastructure device that can safely exchange data streams between a 460-Network and other controlled networks including other 460-Networks.

460-Network is a network which consists of only 460-Nodes, 460-Switches, 460-Forwarder, 460-Gateway and 460-Wireless gateway as well as 450-Nodes.

450-Node is a device compliant with IEC 61162-450 and which satisfies additional requirements specified in this Section.

460-Node is a device compliant with the requirement of a 450-Node and which satisfies the safety and security requirements as specified in this Section.

460-Gateway is a network infrastructure device that connects protected (controlled) 460-Networks and uncontrolled networks and which satisfies the safety and security requirements as specified in this Section.

18.2 GENERAL

18.2.1 The provisions of this Section apply in technical supervision for equipment listed in sections 15140000 and 05410000 of the Nomenclature of Items of the Register Technical Supervision.

18.2.2 The Section establishes the procedure, scope and methods of technical supervision during manufacture of the abovementioned items of technical supervision at the firm (manufacturer).

18.3.3 General provisions for the organization of technical supervision are set out in Part I "General Regulations for Technical Supervision", and those concerning technical documentation – in Part II "Technical Documentation" and in 1.4 of this Part.

18.3 TECHNICAL DOCUMENTATION

18.3.1 The extent of technical documentation to be submitted to the Register depending on the code of the Nomenclature is specified in Appendix 1.

18.3.2 The codes of technical documentation applied in the Section are shown in Table 18.3.2-1.

Table 18.3.2-1

Code	Name	Description
D1	general arrangement plan	a document specifying the product structure, interaction of its components and describing the product operation principle
D2	functional block diagram	a document specifying the basic functional components of the product, their purpose and interconnections
T1	technical description	a document containing a description of device and operation principle of the product being developed, as well as a substantiation of technical solutions accepted for its development
T2	test program and test procedure	a document containing technical data to be checked during the product testing, as well as the sequence and procedure of their control
T3	failure mode and effects analysis (FMEA)	failure mode and effect analysis representing structured approach to potential failures that may occur during the operation of the product (installation)
T4	list of MAC addresses	list shall contain the information on MAC addresses of each cyber safety equipment for navigation and radio communication systems
I1 [XXX][1]	Certificate of Compliance	Document certifying that this type of equipment complies with the specified standard(s)
I2	explosion-proof certificate	a document verifying that this type of equipment complies with the particular standard for explosion protection and is specially intended for the use in the explosive environment
[1] in brackets XXX shall be replaced by the standard(s) the compliance with which shall be confirmed by the certificate		

18.3.3 Where necessary, RS may require to submit additional technical documentation including the reliability information.

18.3.4 When reviewing the technical documentation, it is necessary to identify the compliance of the design and performance characteristics of the products with the requirements of the relevant RS normative documents, including shipboard service conditions.

18.4 SCOPE AND PROCEDURE OF SURVEY

18.4.1 Prior to tests of electrical equipment, the following shall be available at the firm (manufacturer):

.1 the Register approved technical documentation on the equipment testing;

.2 the Register approved test program;

.3 documents (certificates, test reports, etc.) of competent bodies, which confirm satisfactory results of special types of tests if provided by the test program;

.4 testing equipment specified in the program with pertinent documents confirming equipment parameters, certificates of testing laboratory;

.5 documents of competent bodies confirming compliance of the measurement instruments with the specified tolerance.

18.4.2 In surveying, the surveyor shall satisfy himself that tests are carried out in consistency with the Register approved program following the test procedures set forth in this Section or other equivalent procedures approved by the Register.

18.4.3 Upon completion of the mechanical and environmental tests, any types of special tests and checks following which mechanical damages of individual components are likely to occur as well as when the normal operation during any tests is disturbed, the equipment shall be subjected to detailed examination and the possibility of further tests shall be determined.

18.4.4 The surveyor can reject survey or tests performance if an item is inadequately prepared for tests, and also when defects effecting the safety of survey or test performance are revealed.

18.4.5 If a product has failed to pass a certain kind of tests and, as the result, its design has been changed or improved, the tests shall be repeated in accordance with the test program. The scope of these tests shall be agreed with the Register.

18.4.6 The scope and types of tests of the automation equipment during the manufacture thereof are given in Appendix 1.

18.4.7 When the test results are satisfactory, the certificate of the appropriate form shall be issued in accordance with Part I "General Regulations for Technical Supervision".

18.4.8 When the term of validity is expired, the Type Approval Certificate (CTO) is renewed on request of the manufacturer in accordance with 6.8, Part I "General Regulations for Technical Supervision".

18.4.9 In case of changes to the design of automation equipment resulting in the changes working process, load to the product components, service life or other essential parameters of the product, or changes in software and earlier declared technical parameters of material or product, for endorsement or renewal of CTO the products shall be tested according to the RS-approved program taking into consideration the changes made.

18.5 INSTRUCTIONS ON TESTS AND CHECKS PERFORMANCE

18.5.1 The tests and checks shall be carried out on common specimens in sequence to be specified in test programs.

18.5.2 For automatic equipment irrespective of the sequence specified and need not be on the specimens being subjected to other types of tests, the following tests may be performed:

.1 for exposure to salt mist;

.2 for fungus resistance.

18.5.3 Tests and checks of cyber safety equipment for navigation and radio communication equipment shall be performed by the testing laboratory.

18.5.4 Testing laboratories listed in 18.5.3 shall have at least the following equipment:

.1 network protocol analyser;

.2 simulator arrangement capable of:

transmitting and receiving IEC 61162-450:2018-compliant data and data not compliant thereof;

generating invalid data;

supporting the Ethernet interface;

providing SNMP and syslog client-server data;

monitoring network configuration and status information over SNMP;

monitoring network configuration and status information over syslog;

providing ICMP packets;

providing network load from 0 % to 100 % using IEC 61162-450:2018-compliant data and data not compliant with IEC 61162-450:2018 (for example TCP/IP, UDP/IP);

providing IEC 61162-450:2018-compliant data,

providing IEC 61162-450:2018-compliant data to multiple networks including VLANs and subnets.

.3 simulator arrangement for security testing capable of:

providing client-server connection;

providing DoS attack packet generation.

18.6 DESCRIPTION OF TESTS AND CHECKS

18.6.1 Tests and checks of the cyber safety equipment of control and automation systems.

18.6.1.1 Cyber safety equipment for control and automation systems shall meet the requirements of standards IEC 62443-4-1:2018 and IEC 62443-4-2:2019. The compliance of the equipment with the listed standards shall be confirmed by the Certificate of Compliance issued by a competent body recognized by national authority on accreditation for assessment of compliance with the specified standards.

18.6.1.2 In addition to 18.6.1.1, the products shall be tested and checked following the procedures specified in Section 2 of this Part. The list of tests is set in Appendix 1. Identification of tests and checks meets codes specified in Table 12.6 of Section 12 herein.

18.6.2 Tests and checks of cyber safety equipment for radio and navigation equipment.

18.6.2.1 Tests and checks of 450-Node.

.1 confirm that no connection to external networks or REDS can be established in normal operation;

.2 confirm that syslog is implemented in compliance with the requirements of 4.3.3.2 of standard IEC 61162-450:2018;

.3 confirm by inspection of the manufacturer's documentation that the data output from a node is documented;

.4 if other ONF services are stipulated than it is described in standard IEC 61162-450:2018 confirm by inspection of the firm's (manufacturer's) documentation that they include necessary protocol parameters, for instance for IP addresses and port numbers.

18.6.2.2 Tests and checks of 460-Node.

18.6.2.2.1 Network traffic management.

.1 confirm by analytical evaluation of documented evidence that the 460-Node does not create non-IEC 61162-450:2018-compliant traffic;

.2 refer to the firm's (manufacturer's) documentation and confirm by inspection of documented evidence that the maximum transmission rate for all supported services is specified, and confirm by analytical evaluation of documented evidence that all IEC 61162-450:2018 compliant data meet their maximum transmission rate;

.3 confirm by analytical evaluation that a device meets its equipment performance requirements with a loss rate of packets up to 0,1 % for a time period of 10 min;

.4 confirm by inspection of documented evidence that the firm (manufacturer) has specified device behaviour when the maximum input data rate has been exceeded;

.5 confirm by inspection of documented evidence by the firm (manufacturer) of the 460-Node that it discards all other received data except data it supports;

.6 If provided, refer to the manufacturer's (firm's) documentation and confirm that the maximum transmission rate for all supported VLAN services is specified. The firm (manufacturer) shall provide documented evidence that all IEC 61162-450 compliant data in each VLAN meet their maximum transmission rate;

.7 If VLAN is provided, confirm by inspection of documented evidence that the 460-Node supports VLAN IEEE 802.1Q.

18.6.2.2.2 Security check in general.

.1 confirm by inspection of the firm’s (manufacturer's) documentation that EUT does not use any wireless LAN interface or Wireless AP functions;

.2 confirm that there is no VLAN tunnelling protocol in use if VLAN is provided.

18.6.2.2.3 Check of denial of service behavior.

.1 confirm by inspection of the firm’s (manufacturer's) documentation that the maximum operational input bandwidth is declared by the manufacturer;

.2 check and confirm that simulation arrangements create traffics up to maximum that is declared by the firm (manufacturer). Confirm by observation that the EUT meets its performance requirements;

.3 check by the following procedure: use simulation arrangements to create traffics of 200 % of the maximum (according to the documentation) that is declared by the firm (manufacturer) for a period of at least 10 min. After 10 min, return to the 100 % traffic (according to the documentation). Confirm that the 460-Node behaves during and after the change in traffic as described by the firm's (manufacturer's) documentation;

.4 confirm by inspection of the firm's (manufacturer's) documentation that the maximum operational output bandwidth is declared by the firm (manufacturer);

.5 confirm that the EUT does not exceed the declared maximum operational output bandwidth.

18.6.2.2.4 Check of security for REDS.

.1 confirm by inspection of the documented evidence that the number of connection points for REDS (USB ports, disc drives, etc.) are limited to the absolute minimum required for the operation of the system and its lifetime maintenance and support. Confirm by observation that any other connection points are blocked from easy access;

.2 for USB based connection points for REDS, attach one by one a keyboard or mouse device to the port and confirm that the EUT both refuses to recognize the attached device and refuses to perform any functionality with the attached device;

.3 for USB based ports for other purposes than data sources, confirm that they are blocked from easy access by a user;

.4 if the EUT provides manual execution of any type of files from REDS, confirm that manual execution is only possible for files which have been verified by digital signatures or special keys;

.5 use the manufacturer's documentation about non-executable files which can be used by EUT. Confirm that all non-executable files are verified as described in the manufacturer's documentation before use by the EUT.

18.6.2.2.5 Check of access control to configuration setup.

.1 confirm according to the firm's (manufacturer's) documentation that the access to make changes in the configuration of the EUT is subject to user authentication;

.2 confirm that the user authentication before changing device settings is based on at least an 8 character long password, RSA keys, or another appropriate method;

.3 confirm that passwords are not accepted unless they have at least three of the four available character types: lowercase, uppercase, number, special character;

.4 confirm that the operator's manual includes guidance on the use of strong passwords, if appropriate.

18.6.2.2.6 Check of direct access to uncontrolled network.

The following tests are applicable if the device provides direct connection to exchange the information with other equipment connected to the uncontrolled network.

.1 confirm that the manufacturing default settings of the EUT enable no direct connections with uncontrolled networks;

.2 for each configured direct data exchange, confirm that as precondition for activation the direct connection the VPN has been established from a 460-Gateway and that only the operator of the 460-Node can activate the direct connection. This check shall be carried out for each configured direct data exchange;

.3 for each direct data exchange, confirm that:

there is a permanent indication when direct connection is active;

a caution is created when the direct connection is activated;

if provided, the caution is replaced by a warning after pre-defined time period;

the caution and warning are removed after closing of the direct connection;

.4 confirm that the encryption algorithm used for VPN is specified in the manufacturer's documentation. The secure encryption algorithm shall use either asymmetric or symmetric algorithms. An asymmetric encryption algorithm shall provide at least 2 048-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.

18.6.2.2.7 Redundancy.

For devices deemed critical according to the firm's (manufacturer's) documentation refer to the firm's (manufacturer's) documentation and confirm by inspection of the documented evidence which means are provided for redundancy capability of the EUT.

18.6.2.2.8 Check of monitoring function.

Confirm by observation that monitoring information to syslog is provided by the EUT periodically each 30 min and not more often than once per minute of configuration information.

18.6.2.3 Tests and checks of 460-Switch.

18.6.2.3.1 Check of resource allocation.

.1 confirm by inspection of the manufacturer's (firm's) documentation that a means is provided to configure a stream or a network flow that is identified by the combination of the interface identifier, the MAC address or IP address, protocol number and port number;

.2 confirm by inspection of the manufacturer's (firm's) documentation that means are provided to allocate a network resource for all registered streams;

.3 to perform this check it is necessary to register all incoming and outgoing traffic, to use simulation arrangements to create both registered and non-registered traffic, to confirm by analytical evaluation that only incoming and outgoing traffic goes through and all non-registered traffic is blocked;

.4 confirm by inspection of the manufacturer's (firm's) documentation that means are provided for limiting the total amount of traffic for each interface to a 450-Node and 460-Node using the resource allocation;

.5 use a simulation arrangement to interface two 460-Nodes to the EUT and set the nodes to communicate with each other using the set maximum traffic (according to settings). Confirm by analytical allocation that all traffic passes the EUT. Then increase the traffic by 50 % over the set maximum traffic for a period of 10 min. Confirm by analytical allocation that excessive traffic is blocked;

.6 if a VLAN is provided, confirm by inspection of the firm's (manufacturer's) documentation that a means is provided to configure virtual networks (VLAN) for each interface;

.7 confirm by inspection of the firm's (manufacturer's) documentation that, if VLAN is provided, the VLAN protocol IEEE 802.1Q is supported;

.8 confirm by inspection of documentation that that the EUT has means to filter multicast traffic by IGMP snooping;

.9 in order to confirm by observation the filtration of multicasting network traffic it is necessary to use a simulation arrangement to interface the EUT in parallel or one by one to a 460-Switch, a 460-Forwarder, a 460-Node and a 450-Node. Set a multicasting group in the EUT for filtering network traffic by IGMP snooping. Confirm by observation that the EUT sends IGMP membership queries for this multicast group.

18.6.2.3.2 Check of loop prevention.

.1 confirm by the documented evidence that the EUT provides a loop prevention mechanism;

.2 if an RSTP is provided, confirm by inspection of the firm's (manufacturer's) documentation that the RSTP protocol version IEEE 802.1D-2004 is supported;

.3 for check it is necessary to set three 460-Switches for loop topology connect with at least one 460-Node at each switch, for example using unicast. Confirm by analytical evaluation that the switch does not duplicate data at switches;

.4 for check it is necessary to set three 460-Switches for loop topology connect with at least one 460-Node per switch for example using unicast. Disconnect any cable between each neighbouring 460-Switch and confirm that the data is reachable among 460-Nodes within 5 s. Repeat the check by unplugging each cable in turn between the switches.

18.6.2.3.3 Check of security on general.

.1 confirm by inspection of the firm's (manufacturer's) documentation that the EUT does not use any wireless LAN interface or wireless AP functions;

.2 confirm by analytical evaluation that there is no VLAN tunnelling protocol in use if VLAN is provided.

18.6.2.3.4 Check of denial of service behavior.

Confirm by inspection of the firm's (manufacturer's) documentation that the EUT provides the ICMP and IGMP DoS prevention.

18.6.2.3.5 Check of access control to configuration setup.

.1 confirm by inspection of the firm's (manufacturer's) documentation that the access to make changes in the configuration of the EUT is subject to user authentication;

.2 confirm by analytical evaluation that the user authentication before changing device settings is based on at least a 8 character long password, RSA keys, or another appropriate method;

.3 confirm by observation that passwords are not accepted unless they have at least three of the four available character types: lowercase, uppercase, number, special character;

.4 confirm by inspection of the firm's (manufacturer's) documentation that the operator's manual includes guidance on the use of strong passwords, if appropriate.

18.6.2.3.6 Check of access control for network.

.1 confirm by inspection of the firm's (manufacturer's) documentation that means are provided to permit or deny a flow based on the IP address, protocol number and port number for each physical port;

.2 confirm by analytical evaluation that means are provided to permit or deny a device based on the MAC address for each physical port. If the EUT supports installation in a secure area, confirm that the means are configurable to either enable or disable authorization by the MAC address.

18.6.2.3.7 Check of additional security issues.

.1 confirm by analytical evaluation that the EUT continues normal operation with the previous configuration when power is reapplied after a switch off or power failure;

.2 confirm by analytical evaluation that means are provided in the system management function to revert to the previous stored configuration;

.3 confirm by inspection of the documented evidence that guidance is given to install the EUT in a physically protected location.

18.6.2.3.8 Check of monitoring function.

.1 confirm by observation that the following monitoring information is provided by the EUT: interface information, list of neighbouring MAC addresses per interface, the change of neighbouring MAC address;

.2 confirm by observation that the network configuration information is sent by the EUT as a response to the SNMP query from the network monitoring function. Confirm that the information is reported at least either by syslog (unconditional sending) or by SNMP-Traps (if requested so by the Network monitoring function) whenever some changes in the configuration occur, such as changes of a neighbour MAC address. Confirm that the configuration information using syslog is never reported more often than once per minute;

.3 confirm by observation that the interface input and output link utilization in percent (average over 5 min) is sent by the EUT as a response to the SNMP query from the network monitoring function. Confirm that the information is reported at least either by syslog (unconditional sending) or by SNMP-Traps (if requested so by network monitoring function) whenever significant changes (traffic is more than predefined limit in a 0 % to 100 % scale of network capacity) have been made. Confirm that the information using syslog is never reported more often than once per 3 s.

18.6.2.4 Tests and checks of 460-Forwarder.

18.6.2.4.1 Check of traffic separation.

.1 confirm by inspection of the firm's (manufacturer's) documentation that means are provided to transmit all or a subset of the traffic between a 460-Network and controlled networks or other 460-Networks;

.2 confirm by analytical evaluation the possibility to limit the maximum traffic flow between a 460-Network and controlled networks (or other 460-Networks). Follow instructions given by the firm (manufacturer);

.3 if VLAN capability is provided, confirm by inspection of the firm's (manufacturer's) documentation that means are provided to configure transmitting/disconnecting between a 460-Network and controlled networks or other 460-Networks with VLAN at the EUT;

.4 if VLAN capability is provided, confirm by inspection of the firm's (manufacturer's) documentation that the 460-Forwarder implements the VLAN protocol IEEE 802.1Q;

.5 confirm by inspection of the firm's (manufacturer's) that the EUT has means to filter multicast traffic by IGMP snooping;

.6 in order to confirm by observation the filtration of multicasting network traffic it is necessary to use a simulation arrangement to interface the EUT in parallel or one by one to a 460-Switch, a 460-Forwarder, a 460-Node and a 450-Node. Set a multicasting group in the EUT for filtering network traffic by IGMP snooping. Confirm by observation that the EUT sends IGMP membership queries for this multicast group.

18.6.2.4.2 Check of resource allocation.

.1 to perform this check it is necessary to register all incoming and outgoing traffic, to use simulation arrangements to create both registered and non-registered traffic, to confirm by analytical evaluation that only incoming and outgoing traffic goes through and all non-registered traffic is blocked;

.2 confirm by inspection of the manufacturer's (firm's) documentation that means are provided for limiting the total amount of traffic for each interface to a 450-Node and 460-Node using the resource allocation;

.3 use a simulation arrangement to interface two 460-Nodes to the EUT and set the nodes to communicate with each other using the set maximum traffic (according to settings). Confirm by analytical allocation that all traffic passes the EUT. Then increase the traffic by 50 % over the set maximum traffic for a period of 10 min. Confirm by analytical allocation that excessive traffic is blocked;

.4 Confirm by inspection of the manufacturer's (firm's) documentation that a means is provided to configure a stream or a network flow that is identified by the combination of interface identifier, the IP address, protocol number and port number for each physical port. Confirm by observation that means are provided to allocate a network resource for all registered streams;

.5 If VLAN capability is provided, confirm by analytical evaluation that means are provided for limiting the total amount of traffic for each VLAN to controlled networks or 460-Networks for a given value using resource allocation.

18.6.2.4.3 Check of traffic prioritization.

.1 check shall be carried out according to the following procedure:

use a simulation arrangement to set three different types of traffic with different priorities that include the lowest priority;

set the traffic limit to be enough only for the highest priority traffic;

increase the traffic with the lowest priority until data loss occurs.

The check is deemed passed if the loss rate of the highest priority traffic is lowest and that of lowest priority is the highest.

.2 for checking it is necessary to create for each port an increased traffic higher than 50 % of physical capacity of the line or higher than the set maximum input data rate set for the port for 30 s and return to below 50 % of physical capacity of the line and below the set maximum input data rate set for the port. Confirm by analytical evaluation that there was a drop in lower priority traffic until the traffic was below 50 % of physical capacity of the line and below the set maximum input data rate set for the port;

.3 during checking of each port confirm by analytical evaluation that the highest priority traffic continues lossless until the amount of traffic transferred in the last 30 s is higher than the set maximum input data rate set for the port, after which also a part of highest priority traffic may be dropped;

.4 confirm by analytical evaluation that the use of dropping is reported either by syslog for each period of 30 s during which the dropping has been used or as response to SNMP-Trap method.

18.6.2.4.4 Check of general requirements for security.

.1 confirm by inspection of the manufacturer's (firm's) documentation that the EUT does not use any wireless LAN interface or wireless AP functions;

.2 confirm by analytical evaluation that there is no VLAN tunnelling protocol in use if VLAN is provided.

18.6.2.4.5 Check of denial of service behavior.

Confirm by inspection of the manufacturer's (firm's) documentation that the EUT provides ICMP and IGMP DoS prevention.

18.6.2.4.6 Check of access control to configuration setup.

.1 confirm by inspection of the manufacturer's (firm's) documentation that the access to make changes in the configuration of the EUT is subject to user authentication;

.2 confirm by analytical evaluation that the user authentication before changing device settings is based on at least a 8 character long password, RSA keys, or another appropriate method;

.3 confirm that passwords are not accepted unless they have at least three of the four available character types: lowercase, uppercase, number, special character;

.4 confirm that the operator's manual includes guidance on the use of strong passwords, if appropriate.

18.6.2.4.7 Check of access control for network.

.1 confirm by inspection of the manufacturer's (firm's) documentation that means are provided to permit or deny a flow based on the IP address, protocol number and port number for each physical port;

.2 confirm by analytical evaluation that means are provided to permit or deny a device based on the MAC address for each physical port. If the EUT supports installation in a secure area, confirm by analytical evaluation that the means are configurable to either enable or disable authorization by the MAC address.

18.6.2.4.8 Check of additional security.

.1 confirm by observation that the EUT continues normal operation with the previous configuration when power is reapplied after switch off or input power interruption;

.2 confirm by analytical evaluation that, after changes have been made to the EUT configuration, means are provided in the system management function to revert to the previous stored configuration;

.3 confirm by inspection of the manufacturer's (firm's) documentation that guidance is given to install the EUT in a location with restricted physical access.

18.6.2.4.9 Check of monitoring function.

.1 confirm by observation that the following monitoring information is provided by the EUT: interface information, list of neighbouring MAC addresses per interface, the change of neighbouring MAC address;

.2 confirm by observation that the network configuration information is sent by the EUT as a response to the SNMP query from the network monitoring function. If VLAN is provided, confirm by observation that the current VLAN configuration information is sent as a response to the SNMP query. Confirm by analytical evaluation that the information is reported at least either by syslog (unconditional sending) or by SNMP-Traps (if requested so by Network monitoring function) whenever some changes in the configuration occur, such as changes of the neighbouring MAC address. Confirm by observation that the configuration information using syslog is never reported more often than once per minute;

.3 confirm by observation that the interface input and output link utilization in percent (average over 5 min) is sent by the EUT as a response to the SNMP query from the network monitoring function. Confirm by observation that the information is reported at least either by syslog (unconditional sending) or by SNMP-Traps (if requested so by the network monitoring function) whenever significant changes (traffic is more than predefined limit in a 0 % to 100 % scale of network capacity) have been made. Confirm by observation that the information using syslog is never reported more often than once per 3 s.

18.6.2.5 Tests and checks of 460-Gateway.

18.6.2.5.1 Check of denial of service behavior.

Confirm by inspection of documented evidence that the EUT provides ICMP and IGMP DoS prevention.

18.6.2.5.2 Check of access control to configuration setup.

.1 confirm by inspection of the manufacturer's (firm’s) documentation that according to the manufacturer's documentation the access to make changes in the configuration of the EUT is subject to user authentication;

.2 confirm that the user authentication before changing device settings is based on at least a 8 character long password, RSA keys, or another appropriate method;

.3 confirm that passwords are not accepted unless they have at least three of the four available character types: lowercase, uppercase, number, special character;

.4 confirm that the operator's manual includes guidance on the use of strong passwords, if appropriate.

18.6.2.5.3 Check of communication security.

.1 confirm by inspection of the manufacturer's (firm’s) documentation that a direct connection between uncontrolled networks and a 460-Network can only be enabled from a 460-Gateway;

.2 it is necessary by means of a simulation arrangement to establish a VPN connection originating at the EUT between 460-Network and uncontrolled network. Confirm by analytical evaluation that VPN is provided over the connection;

.3 confirm by inspection of the documented evidence that the encryption algorithm used for VPN. The encryption algorithm can be both asymmetric and symmetric and it meets the requirement of encryption strength as follows:

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;

.4 confirm by inspection of the documented evidence that the delivery of certificates is based on a chain of trust or that the private keys/certificates are exchanged in secure manual way or using a combination of manual methods and messages.

18.6.2.5.4 Check of firewall.

.1 confirm by analytical evaluation that all direct connections to the 460-Network are disabled in the manufacturer's (firm’s) default configuration;

.2 for check, in accordance with the manufacturer's (firm’s) documentation, it is necessary to set an EUT between 460-Networks and uncontrolled networks. Then, use the network scanner with port scanning function to scan the range of all addresses in 460-Network, DMZ and uncontrolled network. By means of a software to capture packets operating in "mixed" mode it is necessary to check that the device do not pass the following packets through the EUT and vice versa:

UDP and TCP port scanning in the range of 1 to 65535 for all internal address range of 460-Network;

UDP and TCP port scanning in the range of 1 to 65535 for all internal address range of DMS (if available);

UDP and TCP port scanning in the range of 1 to 65535 for all internal address ranges of uncontrolled networks.

.3 confirm by observation that the EUT registers traffic as an external/internal firewall rule which consists of source and destination IP address, protocol and port number;

.4 confirm by observation that the EUT provides a means to list all direct connections for the last 12 months;

.5 confirm by analytical evaluation that the EUT provides means to list activated direct connections between 460-Networks and uncontrolled networks with status information for each of these connections including: source IP address, destination IP address, starting time and end time of the connection, protocol, and port number;

.6 confirm by analytical evaluation that means provided to allow direct connection with a 460-Node from an uncontrolled network can only be activated by an operation on the 460-Network side of the firewall. Confirm by inspection of the manufacturer's (firm’s) documentation that this cannot be activated from uncontrolled networks. Confirm that means are provided to ensure that the operation can only be performed after obtaining permission, for instance from the bridge officers;

.7 confirm by observation that the EUT terminates all direct connection automatically after a predefined time not exceeding 4 h unless there is user intervention to extend the time;

.8 confirm by observation that the EUT terminates all direct connection automatically after the connection is idle for a pre-defined time not exceeding 10 min;

.9 if direct connection between 460-Networks and an uncontrolled network is provided, either confirm that the activated state is indicated or confirm that the activated state generates a caution.

18.6.2.5.5 Check of application server.

.1 confirm by inspection of the manufacturer's (firm's) documentation that an application server provides means to authenticate clients connected over uncontrolled networks, for example by password;

.2 confirm by analytical evaluation that Layer 3 forwarding or routing is disabled (i.e. no routing of packets is allowed);

.3 verify compliance with 460-Node requirements in accordance with 18.6.2.2;

.4 confirm by inspection of the manufacturer's (firm's) documentation that means for protection from malware are described as appropriate to the computer platform.

18.6.2.5.6 Check of interoperable access to file storage of DMZ.

.1 confirm by observation that a file can be downloaded and uploaded between the DMZ and uncontrolled networks if provided;

.2 confirm by observation that a file can be downloaded and uploaded between the DMZ and 460-Networks if provided;

.3 if access to the file storage within the DMZ is provided, confirm by inspection of the manufacturer's (firm’s) documentation that a protocol is provided, such as SMB or SFTP;

.4 confirm by inspection of the documented evidence that the EUT access to file storage and related data traffic of DMZ satisfies the requirements for ONF, NF as specified in IEC 61162-450 if applicable.

18.6.2.5.7 Check of additional security.

.1 confirm by observation that the EUT continues normal operation with the previous configuration when power is reapplied after switch off or input power interruption;

.2 confirm by analytical evaluation that, after changes have been made to the EUT configuration, means are provided in the system management function to revert to the previous stored configuration;

.3 confirm by inspection of the manufacturer's (firm's) documentation that guidance is given to install the EUT in a location with restricted physical access.

APPENDIX 1

TECHNICAL DOCUMENTATION TO BE SUBMITTED TO RS AND TESTS TO BE PERFORMED

Table 1

Code of item of technical supervision	Item of technical supervision	In case of CTO issuing	
		List of documentation	List of tests
15140000	**Cyber safety**		
15141000	Cyber safety equipment for control and automation systems	D1, D2, T1, T2, I1 [IEC 62443-4-1:2018, IEC 62443-4-2:2019], I2[1]	12.6.1 — 12.6.16
05410000	**Cyber safety equipment for radio and navigation equipment**		
05411000	450-Node	D1, D2, T1, T2, I1 [IEC 61162-450:2018]	IEC 60945:2002, 18.6.2.1
05412000	460-Node	D1, D2, T1, T2, I1 [IEC 61162-450:2018]	IEC 60945:2002, 18.6.2.2
05413000	460-Switch	D1, D2, T1, T2, I1 [IEC 61162-450:2018]	IEC 60945:2002, 18.6.2.3
05414000	460-Forwarder	D1, D2, T1, T2, I1 [IEC 61162-450:2018]	IEC 60945:2002, 18.6.2.4
05415000	460-Gateway	D1, D2, T1, T2, I1 [IEC 61162-450:2018]	IEC 60945:2002, 18.6.2.5

[1] for the equipment to be installed in the explosive area.

".