SEANET MARINEPLANET

HO H.3307 Cyber Security Survey Time Table(Reference)

Date	Place	Time	Focused Items	Remark
Nov. 18th (Tue)	W/H	10:00	Pre-Audit Discussion / Documentation Review / Component Check Jacking System test	with Gusto & SEANET
	Breaktime			
	-	14:00	Visual check of Negligible risk system	with SEANET
	W/H	15:30	Integrated Navigation System (Including Remote Access)	with Wartsila & SEANET
	W/H	-	DNV Inspector's Audit Review	
Nov. 19th (Wed)	ECR	10:00	Pre-Audit Discussion / Documentation Review / Component Check	
	ECR	10:30	Integrated Automation System (Including Remote Access)	with ABB & SEANET
	Breaktime			
	W/H	14:00	Dynamic Positioning sysem (DNV TA acquired system)	with SEANET
	W/H	-	DNV Inspector's Audit Review	
Nov. 20th (Thu)	ECR	10:00	Pre-Audit Discussion / Documentation Review / Component Check	
	ECR	10:30	Thruster (DNV TA acquired system)	with Wartsila & SEANET
	ECR	-	DNV Inspector's Audit Review	
	Breaktime			
	-	-	Contingency time	

Note 1. Schedule can be changed due to test circumstance or participants request.

Note 2. November 20th (Thu.) afternoon will be contingency time for inspection follow-up.

Cyber Security Test Procedure For H3306s
Cadeler WTIV Project

< H.3306 / Integrated Navigation System (INS) >

Cyber Security Test Procedure
For Hanwha Ocean H3306s Cadeler
WTIV Project

< H.3307 / Integrated Navigation System (INS) >

CONTENTS

Contents

1. History

No.	Date (DD/MM/YYYY)	Revision	Description	Remarks
1	16-12-2024	A	First Issue	First Issue

2. Introduction

2.1. Background

Under the H.3306, SeaNet conducts the cybersecurity survey. This survey assesses the implementation of cybersecurity requirements within the target system. SeaNet's responsibilities include ensuring the security of design and implementation, operating system, and application software throughout the inspection process. SeaNet also verifies adherence to various cybersecurity standards, such as those related to account management for software applications

2.2. Scope

Survey Date	27/01/2025	Surveyor(s) name(s)	Dong Ho, Park
Test Location	Bridge		

2.3. Definitions

Owner : The entity responsible for possessing and managing the vessel

Yard : Hanwah Ocean, a shipyard where ships are constructed

Supplier : Wärtsilä, a company that supplies cyber-physical systems and components that are a part of the SuC

Integrator : SEANET, a company that is responsible for acquiring, installing, and integrating systems and components of the SuC

Class : DNV, a classification society that validates compliance with the standards for cyber security as denoted by the notation “Cyber Secure”

2.4. Applicable Specifications and Standards

2.4.1. Documents

Ref.	Title
HO01-CS-001	Cyber Security Design Philosophy

2.4.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2020)
IEC-62443-3-3	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
NIST SP 800-82	Guide to industrial Control System (ICS) Security

1. History

No.	Date (DD/MM/YYYY)	Revision	Description	Remarks
1	16-12-2024	A	First Issue	First Issue

2. Introduction

2.1. Background

Under the H.3306, SeaNet conducts the cybersecurity survey. This survey assesses the implementation of cybersecurity requirements within the target system. SeaNet's responsibilities include ensuring the security of design and implementation, operating system, and application software throughout the inspection process. SeaNet also verifies adherence to various cybersecurity standards, such as those related to account management for software applications

2.2. Scope

Survey Date		Surveyor(s) name(s)	
Test Location	Bridge		

2.3. Definitions

Owner :	The entity responsible for possessing and managing the vessel
Yard :	Hanwha Ocean, a shipyard where ships are constructed
Supplier :	Wärtsilä, a company that supplies cyber-physical systems and components that are a part of the SuC
Integrator :	SEANET, a company that is responsible for acquiring, installing, and integrating systems and components of the SuC
Class :	DNV, a classification society that validates compliance with the standards for cyber security as denoted by the notation “Cyber Secure”

2.4. Applicable Specifications and Standards

2.4.1. Documents

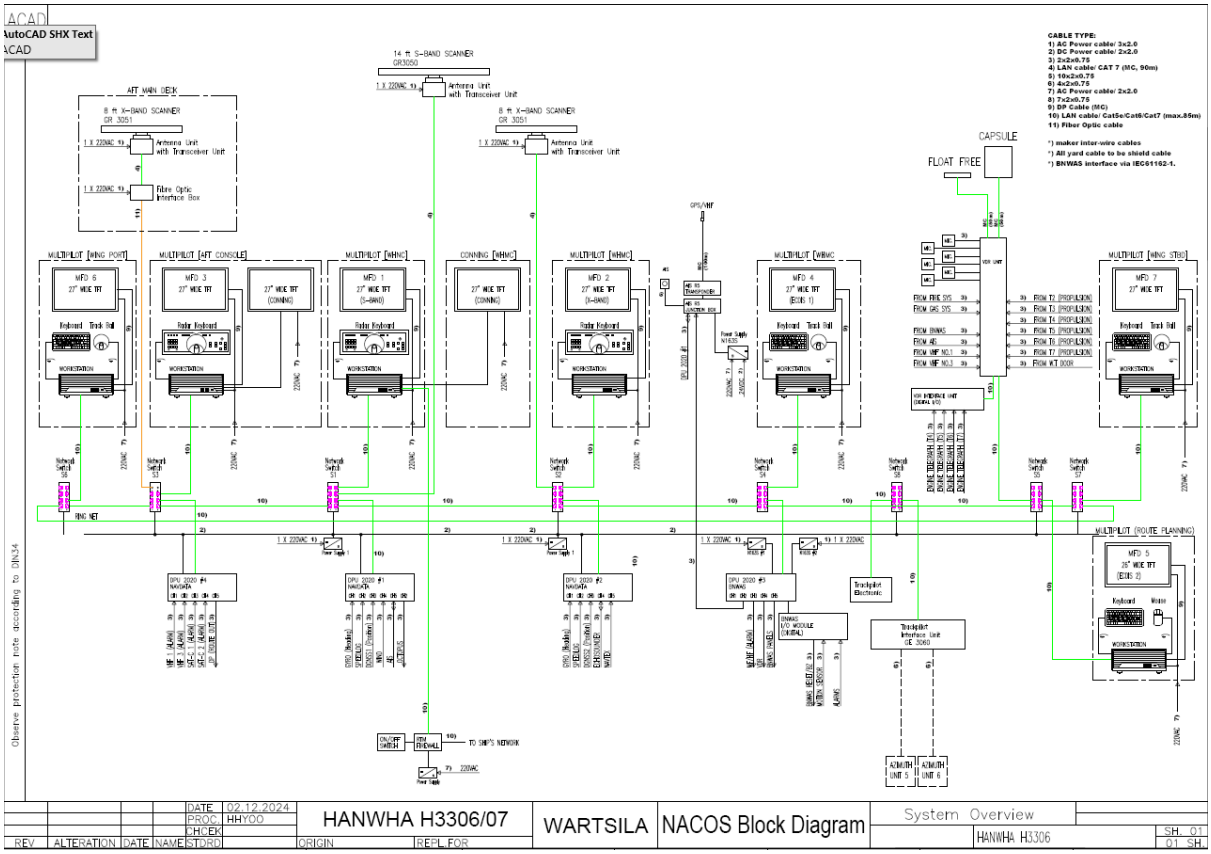
Ref.	Title
HO01-CS-001	Cyber Security Design Philosophy

2.4.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2020)
IEC-62443-3-3	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
NIST SP 800-82	Guide to industrial Control System (ICS) Security

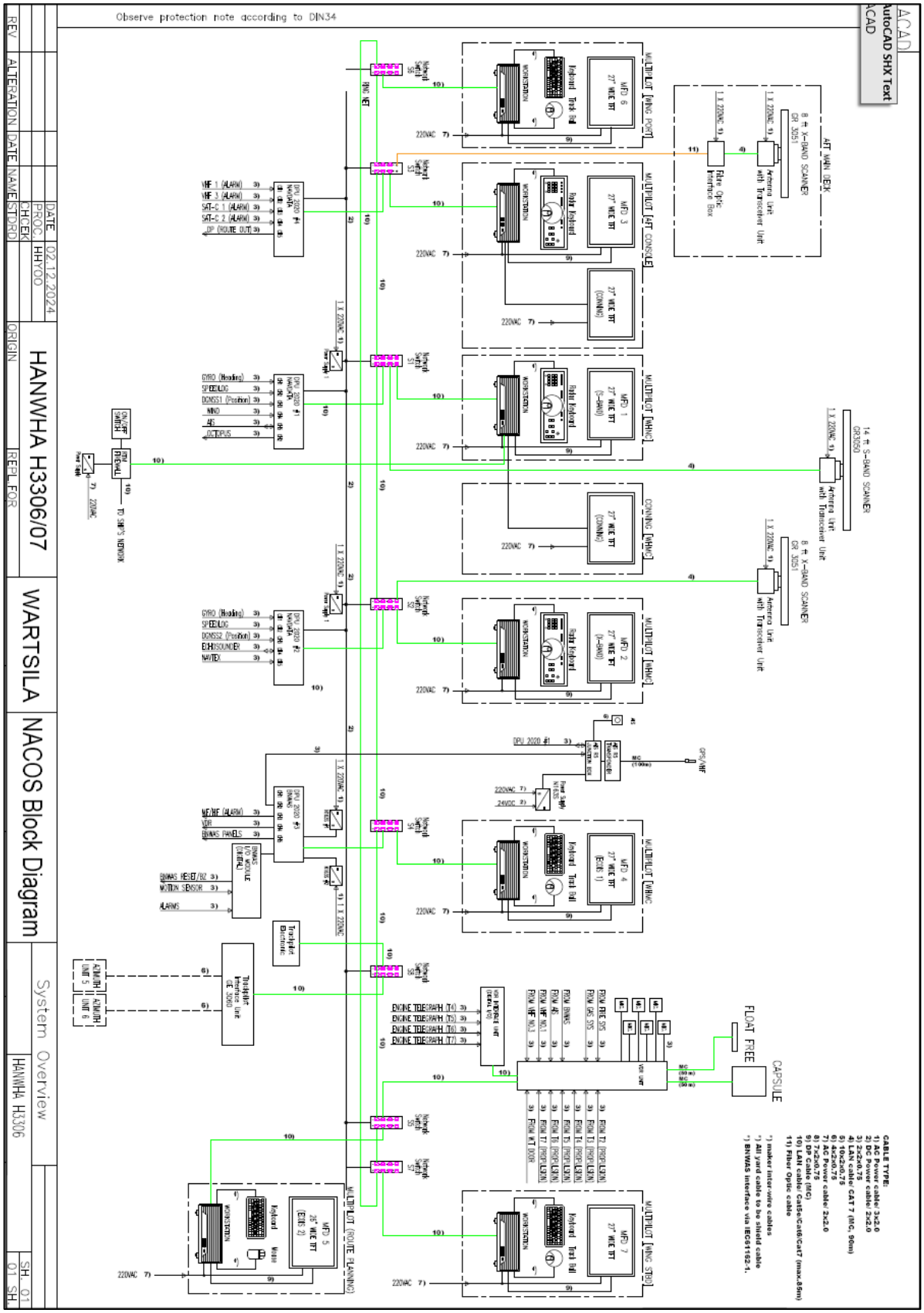
3. Test Circumstance

3.1. System Topology



3. Test Circumstance

3.1. System Topology



3.2. Target Devices

This cyber security survey is limited to equipment available in Supplier scope, at the time of the survey.

The list of equipment is described in the below table.

NO.	BRAND	MODEL	H/W TYPE	LOCATION	REMARKS
1	Adstec	RMT2200	Security	W/H	Remote Service
2	Moxa	EDS-408A	Network	W/H(7)	
3	Moxa	EDS-408A-MM-SC	Network	W/H(2)	Operation Panel
4	HP	HP 800 G6	PC	W/H(7)	MFD
5	Wartsila	IPRC 2	Embeded	Radar mast(2) AFT(1)	Radar operation
6	Wartsila	DPU 2020	Embeded	W/H(4)	Nav. Data Interface Nav. Data Interface Nav. Data Interface BNWAS Data Int
7	Wartsila	TPE20	Embeded	W/H	Positioning Monitoring

The list of test tools is described in the below table.

NO.	TOOL NAME	PURPOSE	REMARKS
1	Anti Malware Test File	Malware Protection Function Check	-
2	Wireshark	Packet Capture and Monitoring	Ver. 4.2.XX
3	Command Prompt	Ping Test	-
4	Advanced Port Scanner	Open Port Scan	Ver. 2.5.XX
5	IP Traffic Generator	DoS Test	-

3.3. Initial Condition

This survey is conducted in accordance with the DNV approved documentation.

To conduct the survey, followings should be fulfilled;

- Unauthorized modifications of security related software or configuration has not been done since the system was shipped, or has been applied as relevant.
- Temporary used accounts have been removed

3.4. Statement of Assurance

Professional survey procedures are completed, and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions are based on comparing the situations that existed during the survey with the established criteria.

3.2. Target Devices

This cyber security survey is limited to equipment available in Supplier scope, at the time of the survey.

The list of equipment is described in the below table.

NO.	BRAND	MODEL	H/W TYPE	LOCATION	REMARKS
1	Adstec	RMT2200	Security	W/H	Remote Service
2	Moxa	EDS-408A	Network	W/H(7)	
3	Moxa	EDS-408A-MM-SC	Network	W/H(2)	Operation Panel
4	HP	HP 800 G6	PC	W/H(7)	MFD
5	Wartsila	IPRC 2	Embeded	Radar mast(2) AFT(1)	Radar operation
6	Wartsila	DPU 2020	Embeded	W/H(4)	Nav. Data Interface Nav. Data Interface Nav. Data Interface BNWAS Data Int
7	Wartsila	TPE20	Embeded	W/H	Positioning Monitoring

The list of test tools is described in the below table.

NO.	TOOL NAME	PURPOSE	REMARKS
1	Anti Malware Test File	Malware Protection Function Check	-
2	Wireshark	Packet Capture and Monitoring	Ver. 4.2.XX
3	Command Prompt	Ping Test	-
4	Advanced Port Scanner	Open Port Scan	Ver. 2.5.XX
5	IP Traffic Generator	DoS Test	-

3.3. Initial Condition

This survey is conducted in accordance with the DNV approved documentation.

To conduct the survey, followings should be fulfilled;

- Unauthorized modifications of security related software or configuration has not been done since the system was shipped, or has been applied as relevant.
- Temporary used accounts have been removed

3.4. Statement of Assurance

Professional survey procedures are completed, and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions are based on comparing the situations that existed during the survey with the established criteria.

4. System Test

[Sample]

No	Task Description	Expected Result	Test Result
1	Verify availability of:	Expected result after following descriptions	Pass / Fail / N/A

4.1. TA Acquired System

4.1.1. System Configuration Verification

As the system has a Type Approval document, it is required to verify that the system is appropriately set as its approved status.

(Requirement(s) : Regarding Class Rule 5.2.4 Type approved systems)

Step No	Task Description	Expected Result	Result
1	Check that the asset inventory matches the TA.	Asset inventory matches the TA.	**N/A**
2	Check the system's configuration information to verify that the system is appropriately set.	Configuration is appropriately set.	**N/A**
Detailed Steps	4.1.1.1. The asset inventory of installed hardware and software should be identical to the Type Approval document, or its regarding information. Target assets are: N/A 4.1.1.2. The system's configuration should be identical with Type Approval document, or its regarding information.		
Comments & Actual Results	- Comments : - Actual Results :		

4. System Test

[Sample]

No	Task Description	Expected Result	Test Result
1	Verify availability of:	Expected result after following descriptions	Pass / Fail / N/A

4.1. TA Acquired System

4.1.1. System Configuration Verification

As the system has a Type Approval document, it is required to verify that the system is appropriately set as its approved status.

(Requirement(s) : Regarding Class Rule 5.2.4 Type approved systems)

Step No	Task Description	Expected Result	Result
1	Check that the asset inventory matches the TA.	Asset inventory matches the TA.	**N/A**
2	Check the system's configuration information to verify that the system is appropriately set.	Configuration is appropriately set.	**N/A**
Detailed Steps	4.1.1.1. The asset inventory of installed hardware and software should be identical to the Type Approval document, or its regarding information. Target assets are: N/A 4.1.1.2. The system's configuration should be identical with Type Approval document, or its regarding information.		
Comments & Actual Results	- Comments : - Actual Results :		

4.2. TA Non-Acquired System

4.2.1. Use Control for Portable and Mobile Devices

The system shall enforce usage restrictions of portable and mobile devices.
(Requirement(s) : 4.3.4 Use control for portable and mobile devices / IEC 62443-3-3 SR 2.3)

Step No	Task Description	Expected Result	Result
1	Connect portable and/or mobile devices to the system and check the system can control device usage. If the above step is failed, check that unused interfaces are blocked, and device connection is appropriately managed.	Portable and mobile device usage is safely configured.	**Pass**
Detailed Steps	4.2.1.1. Insert a USB/portable storage device and check if the INS system (MFD) can prevent the use of portable and mobile devices. There is an option in MFD Customizer for a toggle to allow or disallow the use of portable and mobile devices.		
Comments & Actual Results	- Comments : - Actual Results : Can't access any portable devices with operation level. Can identify the EICAR file and deleted by the system with service engineer level. Can't execute an .exe file. Checked if the system has whitelisted policies applied for executables. Password for service engineers are not shared with other parties.		

4.2. TA Non-Acquired System

4.2.1. Use Control for Portable and Mobile Devices

The system shall enforce usage restrictions of portable and mobile devices.
(Requirement(s) : 4.3.4 Use control for portable and mobile devices / IEC 62443-3-3 SR 2.3)

Step No	Task Description	Expected Result	Result
1	Connect portable and/or mobile devices to the system and check the system can control device usage. If the above step is failed, check that unused interfaces are blocked, and device connection is appropriately managed.	Portable and mobile device usage is safely configured.	
Detailed Steps	4.2.1.1. Insert a USB/portable storage device and check if the INS system (MFD) can prevent the use of portable and mobile devices. There is an option in MFD Customizer for a toggle to allow or disallow the use of portable and mobile devices.		
Comments & Actual Results	- Comments : - Actual Results :		

4.2.2. Auditable Events

The system shall generate audit records for various events which include sufficient information.

(Requirement(s): 4.3.9 Auditable events / IEC 62443-3-3 SR 2.8)

Step No	Task Description	Expected Result	Result
1	See various logs regarding application program, security, and system. Logs shall include timestamp, source, category, type, event ID and event result.	Various event logs can be checked	**Pass**
Detailed Steps	4.2.2.1. Check logs in NACOS Platinum Monitoring Network, MFD CAM (Central Alarm Management). Logs can also be checked on Windows Event Viewer. Check that logs can be saved on an external drive.		
Comments & Actual Results	- Comments : - Actual Results : Checked. Various event logs can be checked.		

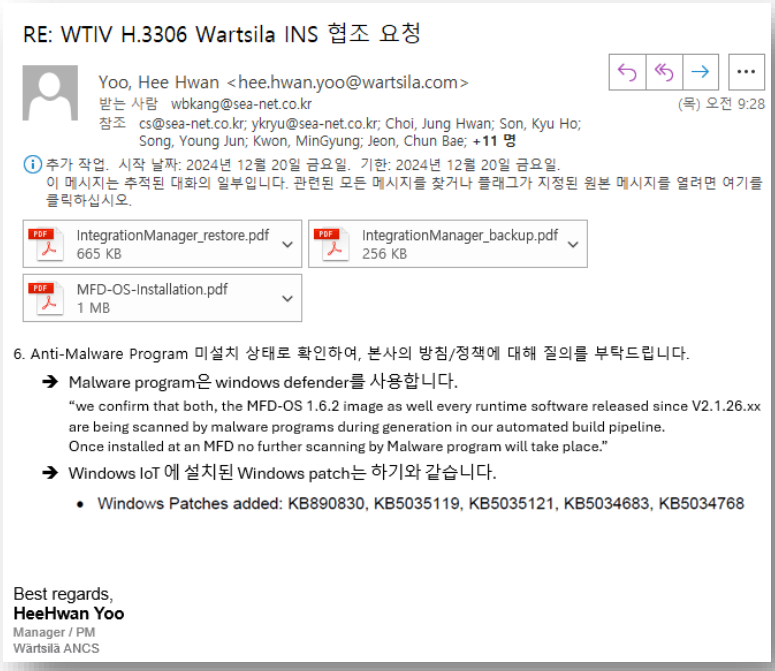
4.2.2. Auditable Events

The system shall generate audit records for various events which include sufficient information.
(Requirement(s): 4.3.9 Auditable events / IEC 62443-3-3 SR 2.8)

Step No	Task Description	Expected Result	Result
1	See various logs regarding application program, security, and system. Logs shall include timestamp, source, category, type, event ID and event result.	Various event logs can be checked	
Detailed Steps	4.2.2.1. Check logs in NACOS Platinum Monitoring Network, MFD CAM (Central Alarm Management). Logs can also be checked on Windows Event Viewer. Check that logs can be saved on an external drive.		
Comments & Actual Results	- Comments : - Actual Results :		

4.2.3. Malicious Code Protection

The system shall have a protection mechanism against malicious code or unauthorized software. The protection mechanism shall be kept updated.
(Requirement(s): 4.4.3 Malicious code protection / IEC 62443-3-3 SR 3.2)

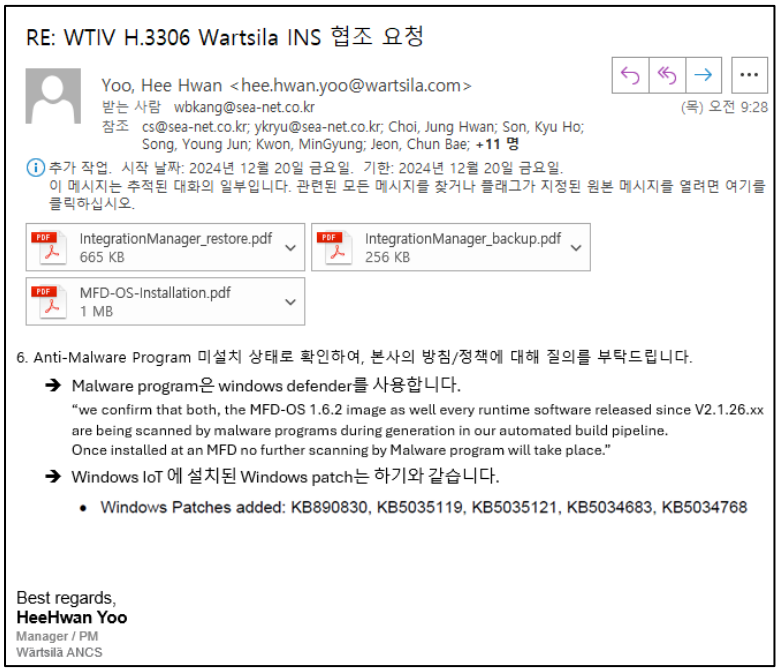
Step No	Task Description	Expected Result	Result
1	Check if the system's prevention mechanism against malicious code/program files is installed and running and the latest update is available. *If there is no anti-malware mechanism or it is insufficient, check if the attack surface is minimized. If it is confirmed that the attack surface is minimized so that internal/external attacks are appropriately controlled, this section is considered as pass.*	Anti-Malicious code/program is running.	**Pass**
Detailed Steps	4.2.3.1. No antivirus software is installed on the INS. In compliance with DNVGL-RU-SHIP 2020 Pt.6 Ch.5 Sec 21 Cyber Security regulations, the following information is used as compensating countermeasures: Integrated Navigation System (INS) is running on Wartsila's own operating system which is based off Windows IoT and is scanned for malware upon generation of OS image and before installation on vessel. 		
Comments & Actual Results	- Comments : - Actual Results : Refer to 4.2.1.		

4.2.3. Malicious Code Protection

The system shall have a protection mechanism against malicious code or unauthorized software. The protection mechanism shall be kept updated.
(Requirement(s): 4.4.3 Malicious code protection / IEC 62443-3-3 SR 3.2)

<table>
<tr><th>Step No</th><th>Task Description</th><th>Expected Result</th><th>Result</th></tr>
<tr><td>1</td><td>Check if the system's prevention mechanism against malicious code/program files is installed and running and the latest update is available.

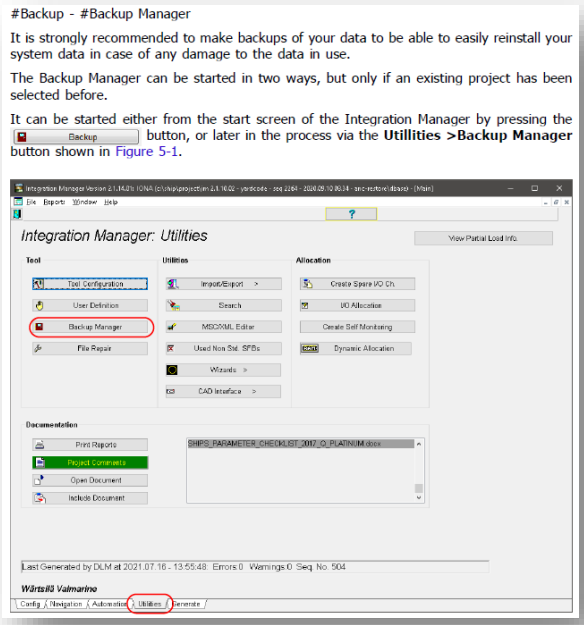
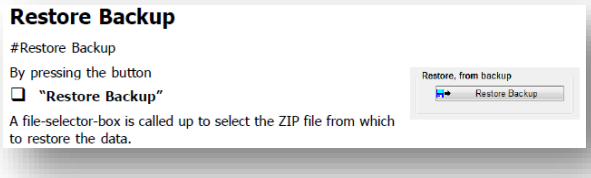
If there is no anti-malware mechanism or it is insufficient, check if the attack surface is minimized. If it is confirmed that the attack surface is minimized so that internal/external attacks are appropriately controlled, this section is considered as pass.</td><td>Anti-Malicious code/program is running.</td><td></td></tr>
<tr><td>Detailed Steps</td><td colspan="3">4.2.3.1. No antivirus software is installed on the INS.
In compliance with DNVGL-RU-SHIP 2020 Pt.6 Ch.5 Sec 21 Cyber Security regulations, the following information is used as compensating countermeasures:

Integrated Navigation System (INS) is running on Wartsila's own operating system which is based off Windows IoT and is scanned for malware upon generation of OS image and before installation on vessel.
 
</td></tr>
<tr><td>Comments & Actual Results</td><td colspan="3">- Comments :
- Actual Results :</td></tr>
</table>

4.2.4. Control System Backup & Restoration

The system shall be able to create a complete backup during normal operation, and restore from a cyber incident.

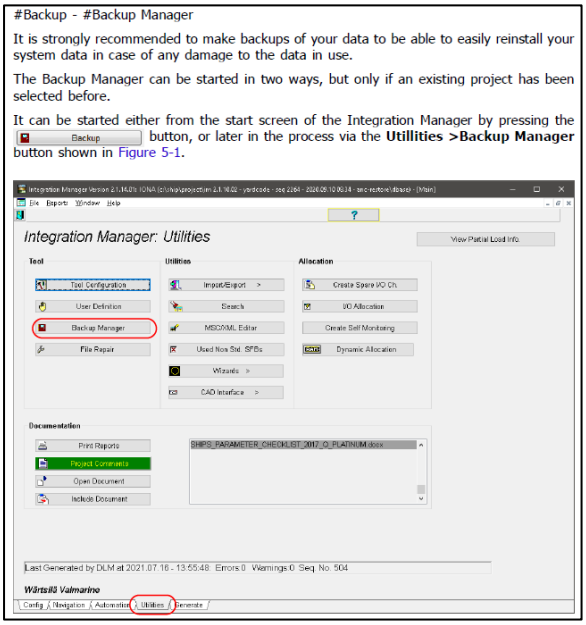
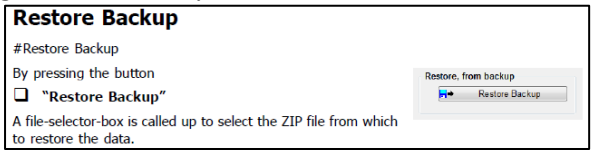
(Requirement(s): 4.8.4 Control system back-up / IEC 62443-3-3 SR 7.3
4.8.5 Control system recovery and reconstitution / IEC-62443-3-3 SR 7.4)

Step No	Task Description	Expected Result	Result
1	Check that the control system data can be saved after following certain procedure.	System data can be saved	**Pass**
2	Check that the control system data can be restored after following certain procedure, to recover from data loss.	System data can be restored	**Pass**
Detailed Steps	4.2.4.1. System configurations can be backed up using the Integration Manager tool.  4.2.4.2. The INS operates on a dedicated OS, Windows IoT, with a spare bootable USB provided to the vessel. In the event of OS issues, system configurations are backed up before the OS is reinstalled, allowing the configurations to be reapplied afterward. If the OS is functioning properly, the NACOS program can restore the backed-up configurations directly. 		
Comments & Actual Results	- Comments : - Actual Results : Checked that the system can backup and restore.		

4.2.4. Control System Backup & Restoration

The system shall be able to create a complete backup during normal operation, and restore from a cyber incident.

(Requirement(s): 4.8.4 Control system back-up / IEC 62443-3-3 SR 7.3
4.8.5 Control system recovery and reconstitution / IEC-62443-3-3 SR 7.4)

Step No	Task Description	Expected Result	Result
1	Check that the control system data can be saved after following certain procedure.	System data can be saved	
2	Check that the control system data can be restored after following certain procedure, to recover from data loss.	System data can be restored	
Detailed Steps	4.2.4.1. System configurations can be backed up using the Integration Manager tool.  #Backup - #Backup Manager It is strongly recommended to make backups of your data to be able to easily reinstall your system data in case of any damage to the data in use. The Backup Manager can be started in two ways, but only if an existing project has been selected before. It can be started either from the start screen of the Integration Manager by pressing the Backup button, or later in the process via the **Utillities >Backup Manager** button shown in Figure 5-1. Integration Manager: Utilities 4.2.4.2. The INS operates on a dedicated OS, Windows IoT, with a spare bootable USB provided to the vessel. In the event of OS issues, system configurations are backed up before the OS is reinstalled, allowing the configurations to be reapplied afterward. If the OS is functioning properly, the NACOS program can restore the backed-up configurations directly.  **Restore Backup** #Restore Backup By pressing the button ❑ **"Restore Backup"** A file-selector-box is called up to select the ZIP file from which to restore the data. Restore, from backup Restore Backup		
Comments & Actual Results	- Comments : - Actual Results :		

5. Integration Test

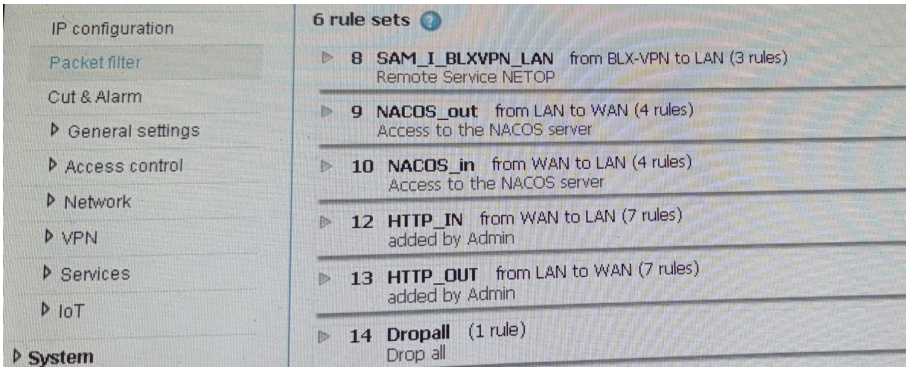
5.1. Network Segmentation & Zone Boundary Test

Requirement(s): 4.6.2 Network segmentation / IEC 62443-3-3 SR 5.1, 5.1 RE 1
4.6.3 Zone boundary protection / IEC-62443-3-3 SR 5.2, 5.2 RE 1

Test Prerequisite

1) Different network zones must be physically or logically separated.
2) Communication between different zones should be controlled and monitored.
   Communication should be controlled based on 'deny by default, allow by exception' principle.

5.1.1. Test Result

Step No	Task Description	Expected Result	Result
1	Check the zone boundary protection device's configuration; that network is well segmented and whitelisted, and data cannot be transferred to different zones without approval.	Zones are well segmented and unnecessary functions are disabled	**Pass**
2	Check that zone protecting device can stop communication manually.	Communication between zones can be stopped	**Pass**
Detailed Steps	5.1.1.1. The INS is divided into two zones: the internal INS network zone and the external network zone. The external network zone extends from the Big-LinX (BLX) VPN to the LAN. The BLX VPN is secure, and only authorized personnel can access it. The internal zone is only connected to the INS itself. Check Firewall rulesets  5.1.1.2. - The system allows for **manual** disconnection of network segments through configured isolation points, particularly at secure router and MOXA Switches.		
Comments & Actual Results	- Comments : - Actual Results : Checked in accordance with the information under "Detailed Steps".		

5. Integration Test

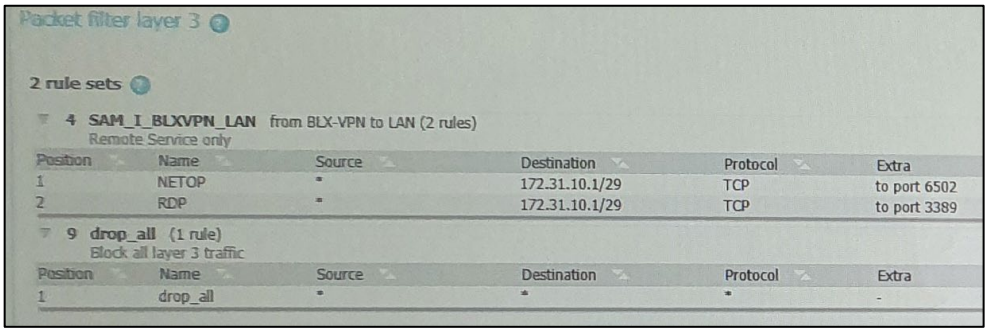
5.1. Network Segmentation & Zone Boundary Test

Requirement(s): 4.6.2 Network segmentation / IEC 62443-3-3 SR 5.1, 5.1 RE 1
4.6.3 Zone boundary protection / IEC-62443-3-3 SR 5.2, 5.2 RE 1

5.1.1. Test Prerequisite

1) Different network zones must be physically or logically separated.
2) Communication between different zones should be controlled and monitored.
Communication should be controlled based on 'deny by default, allow by exception' principle.

5.1.2. Test Result

Step No	Task Description	Expected Result	Result
1	Check the zone boundary protection device's configuration; that network is well segmented and whitelisted, and data cannot be transferred to different zones without approval.	Zones are well segmented and unnecessary functions are disabled	
2	Check that zone protecting device can stop communication manually.	Communication between zones can be stopped	
Detailed Steps	5.1.1.1. The INS is divided into two zones: the internal INS network zone and the external network zone. The external network zone extends from the Big-LinX (BLX) VPN to the LAN. The BLX VPN is secure, and only authorized personnel can access it. The internal zone is only connected to the INS itself. Check Firewall rulesets  5.1.1.2. The system allows for **manual** disconnection of network segments through configured isolation points, particularly at secure router and MOXA Switches.		
Comments & Actual Results	- Comments : - Actual Results :		

5.2. Denial of Service (DoS) Test

Requirement(s): 4.8.2 Denial of Service (DoS) Protection / IEC 62443-3-3 SR 7.1

5.2.1. Test Prerequisite

1) It should generate busier-than-normal traffic. (e.g., at least tens of seconds, in some cases much longer).
2) Check how the device protects the network when overloaded traffic is generated. It should be able to operate in a degraded mode.

System	Target Device	Maximum Network Load	Remark
INS	RMT2200 EDS-408A EDS-408A-MM-SC	1 Gbps	

5.2.2. Test Result

Step No	Task Description	Expected Result	Result
1	If the target system communicates with a trusted network, simulate DoS attack to target device and network, and verify that the system functions normally as it prevents DoS attack or detects DoS attack and restart automatically to be resilient from the attack.	The system works normally, or restart automatically to resilient	**Pass**
2	If the target system communicates with untrusted network, simulate DoS attack to the zone boundary protection device to verify that the network and the target device are operating normally.	The system works normally, or restart automatically to resilient	**Pass**
Detailed Steps	Conduct a network storming test on the INS zone boundary protection device and confirm that the system runs properly with no degradation.		
Comments & Actual Results	- Comments : - Actual Results : **Internal Network Storm:** ICMP Flooding – Alarm for network switch abnormal / System working as intended UDP Flooding – Alarm for network switch abnormal / System working as intended TCP SYN Flooding – no Alarms generated / System working as intended Broadcast – No alarm / System working as intended **External Network Storm (Source: WAN; Target: MFD 01)** For all protocols, Source sends packets to MFD 01, can be seen that router receives packets however are dropped before reaching MFD 01.		

5.2. Denial of Service (DoS) Test

Requirement(s): 4.8.2 Denial of Service (DoS) Protection / IEC 62443-3-3 SR 7.1

5.2.1. Test Prerequisite

1) It should generate busier-than-normal traffic. (e.g., at least tens of seconds, in some cases much longer).
2) Check how the device protects the network when overloaded traffic is generated. It should be able to operate in a degraded mode.

System	Target Device	Maximum Network Load	Remark
INS	RMT2200 EDS-408A EDS-408A-MM-SC	1 Gbps	

5.2.2. Test Result

Step No	Task Description	Expected Result	Result
1	If the target system communicates with a trusted network, simulate DoS attack to target device and network, and verify that the system functions normally as it prevents DoS attack or detects DoS attack and restart automatically to be resilient from the attack.	The system works normally, or restart automatically to resilient	
2	If the target system communicates with untrusted network, simulate DoS attack to the zone boundary protection device to verify that the network and the target device are operating normally.	The system works normally, or restart automatically to resilient	
Detailed Steps	Generate network overload using traffic generator tool. Check whether the system detects DoS attack and gives alarm, and runs well from DoS attack.		
Comments & Actual Results	- Comments : - Actual Results :		

5.3. Integration Test for Untrusted networks

5.3.1. User identification and Authentication

All human user access from untrusted networks shall use multifactor authentication.

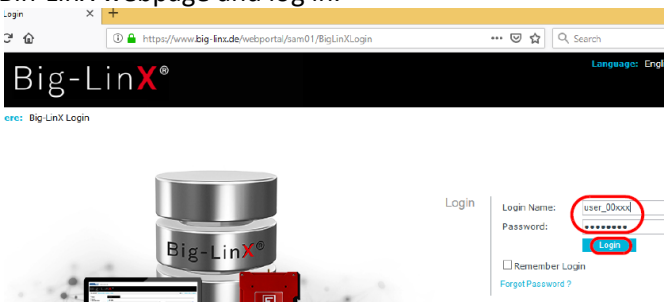
Requirement: 4.2.2 User identification and authentication / IEC 62443-3-3 SR 1.1 RE 2

Step No	Task Description	Expected Result	Result
1	Check that the system asks multifactor authentication for user access.	Multifactor authentication process should be activated.	**Pass**

Detailed Steps

5.3.1.1. The MFA Access of remote access is following;

1. Access the Bin-LinX webpage and log in.



2. Log in to the Virtual Machine (VM).

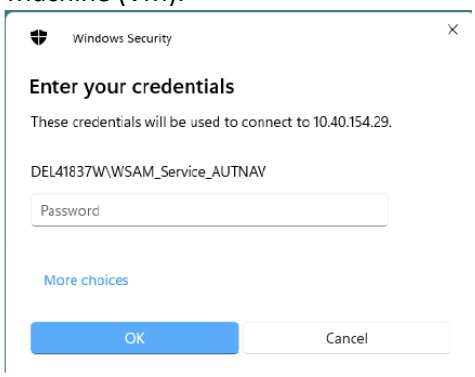


Fig. 4-10 Logon VM Machine

3. Use the VM to log in to Netop.

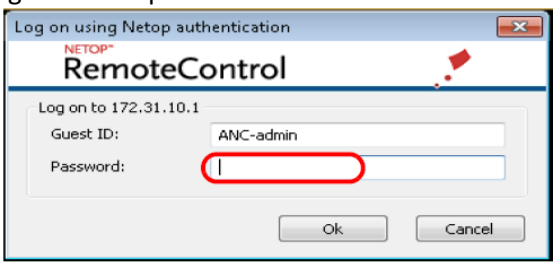


Fig. 4-14 Logon Remote MFD / PC over NETOP

4. On the vessel side, authorized crew approve the key switch on.

Comments & Actual Results

- Comments :
- Actual Results :

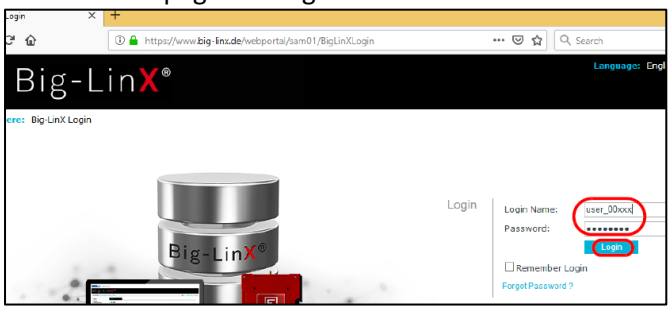
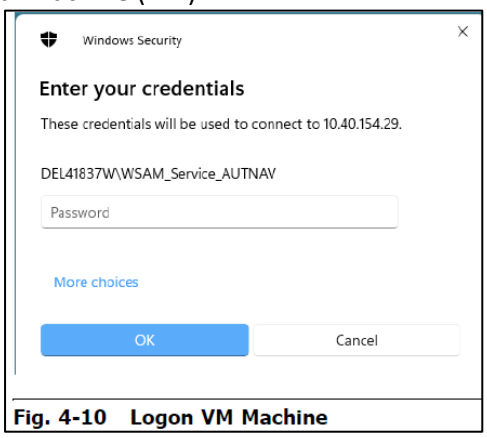
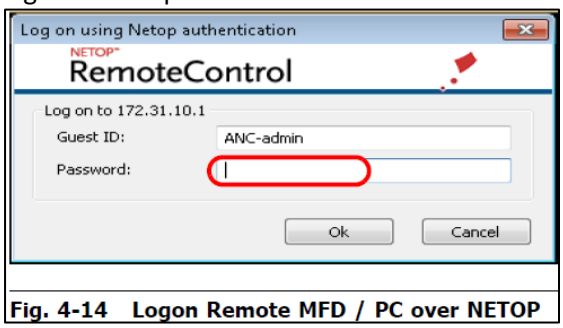
Checked in accordance with “Detailed Steps” provided above.

5.3. Integration Test for Untrusted networks

5.3.1. User identification and Authentication

All human user access from untrusted networks shall use multifactor authentication.

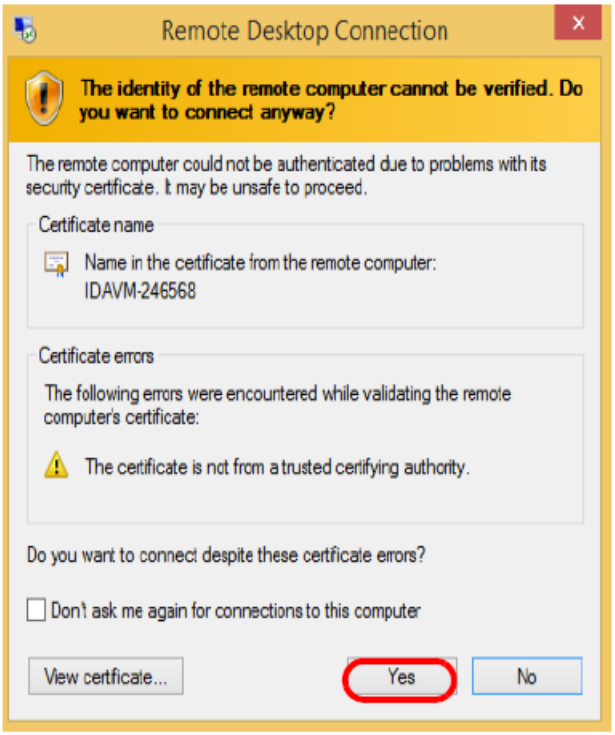
Requirement: 4.2.2 User identification and authentication / IEC 62443-3-3 SR 1.1 RE 2

Step No	Task Description	Expected Result	Result
1	Check that the system asks multifactor authentication for user access.	Multifactor authentication process should be activated.	
Detailed Steps	5.3.1.1. The MFA Access of remote access is following; 1. Access the Bin-LinX webpage and log in.  2. Log in to the Virtual Machine (VM).  **Fig. 4-10 Logon VM Machine** 3. Use the VM to log in to Netop.  **Fig. 4-14 Logon Remote MFD / PC over NETOP** 4. On the vessel side, authorized crew approve the key switch on.		
Comments & Actual Results	- Comments : - Actual Results :		

5.3.2. System Use Notification

The system shall display a configurable use notification message before user authentication when accessed from untrusted networks.

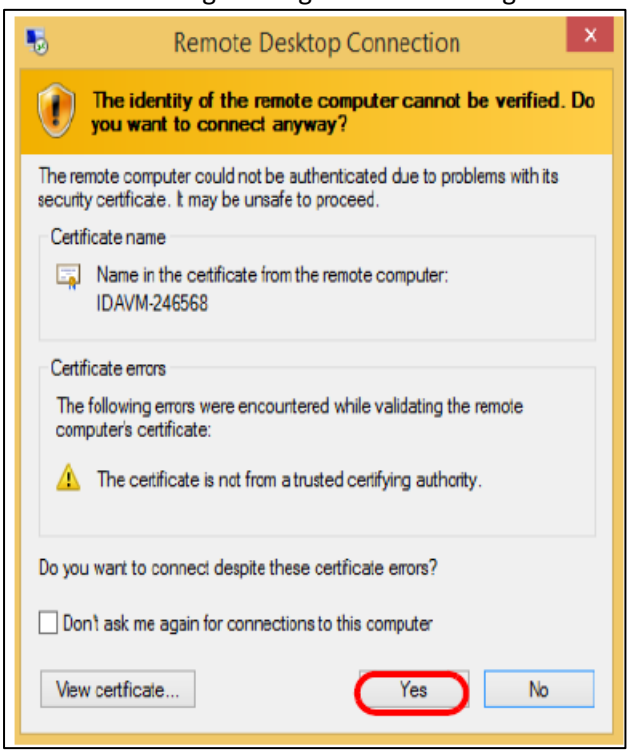
Requirement(s): 4.2.13 System user notification / IEC 62443-3-3 SR 1.12

Step No	Task Description	Expected Result	Result
1	Check the system shows a use notification message when accessing remotely.	Notification message should be shown.	**Pass**
Detailed Steps	5.3.2.1. When accessing the MFD via Big-LinX's virtual machine, a notification prompts the user with a warning message before creating a connection. 		
Comments & Actual Results	- Comments : - Actual Results : Checked in accordance with "Detailed Steps" provided above.		

5.3.2. System Use Notification

The system shall display a configurable use notification message before user authentication when accessed from untrusted networks.

Requirement(s): 4.2.13 System user notification / IEC 62443-3-3 SR 1.12

Step No	Task Description	Expected Result	Result
1	Check the system shows a use notification message when accessing remotely.	Notification message should be shown.	
Detailed Steps	5.3.2.1. When accessing the MFD via Big-LinX's virtual machine, a notification prompts the user with a warning message before creating a connection. 		
Comments & Actual Results	- Comments : - Actual Results :		

5.3.3. Access via untrusted networks

The system shall monitor and control all access methods from untrusted networks. It shall deny access requests via untrusted networks unless approved by an assigned crew member.

Requirement(s): 4.2.14 Access via untrusted networks / IEC 62443-3-3 SR 1.13
4.2.14 Access via untrusted networks / IEC 62443-3-3 SR 1.13 RE 1

Step No	Task Description	Expected Result	Result
1	Check whether the system monitors and controls remote access. This can be checked from logs.	The system shall monitor and control access.	**Pass**
2	Check whether the system deny access requests via untrusted networks, if the request is not approved.	The system can deny unapproved access request.	**Pass**

Detailed Steps

5.3.3.1. Wartsila headquarters replied regarding this requirement below.
Remote access logs are logged on Big-LinX platform

5.3.3.2. Wartsila headquarters replied regarding this requirement below.
The key switch, controlled by an authorized crew member, is the only way to start and stop the session. When remote access is necessary, the crew turns the key switch on. Otherwise, the switch remains off.

Comments & Actual Results

- Comments :
- Actual Results :

Checked in accordance with “Detailed Steps” provided above.

Note:
There were no indications shown on the MFD during the remote connection status. However, Windows Event Viewer was able to log the remote connection.

5.3.3. Access via untrusted networks

The system shall monitor and control all access methods from untrusted networks. It shall deny access requests via untrusted networks unless approved by an assigned crew member.

Requirement(s): 4.2.14 Access via untrusted networks / IEC 62443-3-3 SR 1.13

4.2.14 Access via untrusted networks / IEC 62443-3-3 SR 1.13 RE 1

Step No	Task Description	Expected Result	Result
1	Check whether the system monitors and controls remote access. This can be checked from logs.	The system shall monitor and control access.	
2	Check whether the system deny access requests via untrusted networks, if the request is not approved.	The system can deny unapproved access request.	
Detailed Steps	5.3.3.1. Wartsila headquarters replied regarding this requirement below. Remote access logs are logged on Big-LinX platform  5.3.3.2. Wartsila headquarters replied regarding this requirement below. The key switch, controlled by an authorized crew member, is the only way to start and stop the session. When remote access is necessary, the crew turns the key switch on. Otherwise, the switch remains off.		
Comments & Actual Results	- Comments : - Actual Results :		

5.3.4. Remote session termination

The system shall automatically terminate remote sessions after a configurable period of inactivity or upon manual termination by an assigned crew member. Termination shall not jeopardize vessel or crew safety.

Requirement(s): 4.3.7 Remote session termination / IEC 62443-3-3 SR 2.6

Step No	Task Description	Expected Result	Result
1	Check whether the system automatically terminate a remote session after certain time has passed, or by manually.	The remote access can be terminated either automatically or manually.	**Pass**

Detailed Steps

5.3.4.1. Wartsila headquarters replied regarding this requirement below.

Wartsila headquarters replied regarding this requirement below.
The key switch, controlled by an authorized crew member, is the only way to start and stop the session. When remote access is necessary, the crew turns the key switch on. Otherwise, the switch remains off.

RE: WTIV H.3306 Wartsila INS 협조 요청

회신 | 전체 회신 | 전달 | ...

YH Yoo, Hee Hwan <hee.hwan.yoo@wartsila.com>
받는 사람 wbkang@sea-net.co.kr
참조 cs@sea-net.co.kr; ykryu@sea-net.co.kr; Choi, Jung Hwan; Son, Kyu Ho; Song, Young Jun; Kwon, MinGyung; Jeon, Chun Bae; '서석진(SEOK JIN SEO)'; '권상아(SANG A Kwon)'; +9 명
2024-12-17 (화) 오후 4:01

추가 작업. 시작 날짜: 2024년 12월 17일 화요일. 기한: 2024년 12월 17일 화요일.
이 메시지는 추적된 대화의 일부입니다. 관련된 모든 메시지를 찾거나 플래그가 지정된 원본 메시지를 열려면 여기를 클릭하십시오.

7. Remote Access 접속을 본선 선박에서 거부하거나, 세션을 강제로 종료하는 방법이 키 박스 외에 다른 해결책이 있는지 여부를 알려주시길 바랍니다.
가령 원격 중, 선박에서 허용치 않은 원격 접속을 발견하여 접속을 거부하거나 세션을 강제 종료하는 기능이 있다면, 스크린샷과 함께 설명을 해주시면 좋겠습니다.
→ 하기 내용을 참고 바랍니다.
The key switch is the only way to stop the session. The second option is to turn off the router or disconnect the Ethernet cable between the router and the workstation.

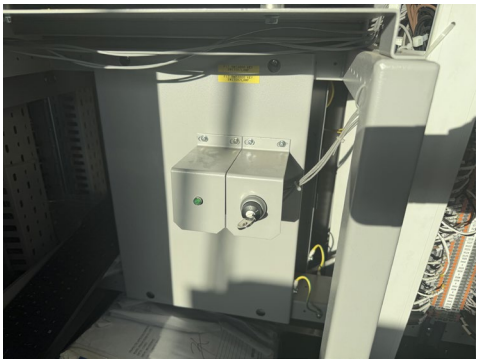
Best regards,
HeeHwan Yoo
Manager / PM
Wärtsilä ANCS

Mob +82 10 9302 9278
hee.hwan.yoo@wartsila.com

Comments & Actual Results

- Comments :
- Actual Results :

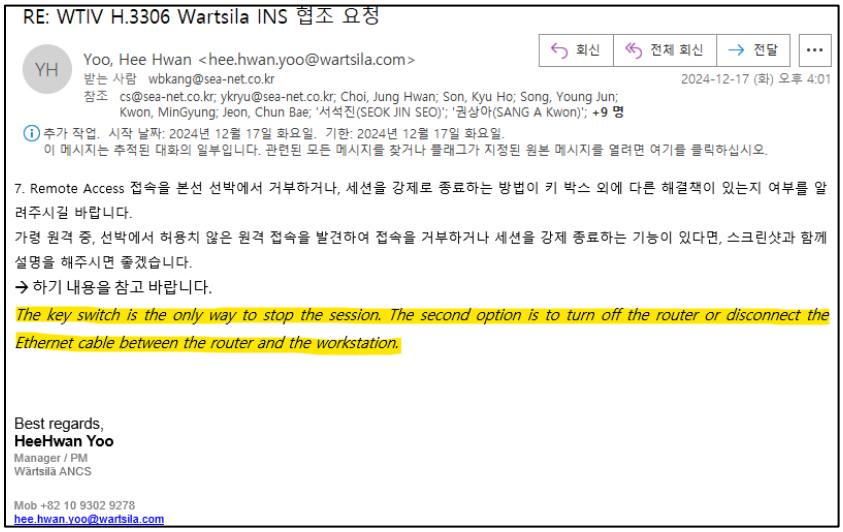
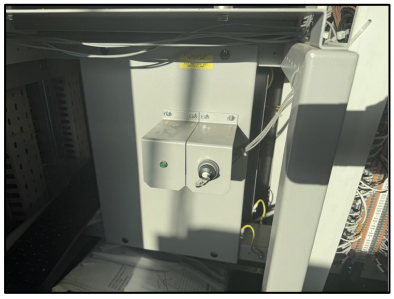
The remote session can be terminated by turning off the physical key for the remote connection.



5.3.4. Remote session termination

The system shall automatically terminate remote sessions after a configurable period of inactivity or upon manual termination by an assigned crew member. Termination shall not jeopardize vessel or crew safety.

Requirement(s): 4.3.7 Remote session termination / IEC 62443-3-3 SR 2.6

Step No	Task Description	Expected Result	Result
1	Check whether the system automatically terminate a remote session after certain time has passed, or by manually.	The remote access can be terminated either automatically or manually.	
Detailed Steps	5.3.4.1. Wartsila headquarters replied regarding this requirement below. Wartsila headquarters replied regarding this requirement below. The key switch, controlled by an authorized crew member, is the only way to start and stop the session. When remote access is necessary, the crew turns the key switch on. Otherwise, the switch remains off.  		
Comments & Actual Results	- Comments : - Actual Results :		

RE: WTIV H.3306 Wartsila INS 협조 요청

회신 | 전체 회신 | 전달 | ...

YH Yoo, Hee Hwan <hee.hwan.yoo@wartsila.com>
받는 사람 wbkang@sea-net.co.kr
참조 cs@sea-net.co.kr; ykryu@sea-net.co.kr; Choi, Jung Hwan; Son, Kyu Ho; Song, Young Jun; Kwon, MinGyung; Jeon, Chun Bae; '서석진(SEOK JIN SEO)'; '권상아(SANG A Kwon)'; +9 명
2024-12-17 (화) 오후 4:01

ⓘ 추가 작업. 시작 날짜: 2024년 12월 17일 화요일. 기한: 2024년 12월 17일 화요일.
이 메시지는 추적된 대화의 일부입니다. 관련된 모든 메시지를 찾거나 플래그가 지정된 원본 메시지를 열려면 여기를 클릭하십시오.

7. Remote Access 접속을 본선 선박에서 거부하거나, 세션을 강제로 종료하는 방법이 키 박스 외에 다른 해결책이 있는지 여부를 알려주시길 바랍니다.
가령 원격 중, 선박에서 허용치 않은 원격 접속을 발견하여 접속을 거부하거나 세션을 강제 종료하는 기능이 있다면, 스크린샷과 함께 설명을 해주시면 좋겠습니다.
→ 하기 내용을 참고 바랍니다.
The key switch is the only way to stop the session. The second option is to turn off the router or disconnect the Ethernet cable between the router and the workstation.

Best regards,
HeeHwan Yoo
Manager / PM
Wärtsilä ANCS

Mob +82 10 9302 9278
hee.hwan.yoo@wartsila.com

5.3.5. Communication integrity

The system shall protect the integrity of transmitted information.

Requirement(s): 4.4.2 Community integrity / IEC 62443-3-3 SR 3.1

Step No	Task Description	Expected Result	Result
1	Check the system may protect the information integrity.	There is an information integrity protection method.	**Pass**

Detailed Steps

5.3.5.1. Wartsila headquarters replied regarding this requirement below.
Communication via TLS/SSL protocol is encrypted method of remote access.

Comments & Actual Results

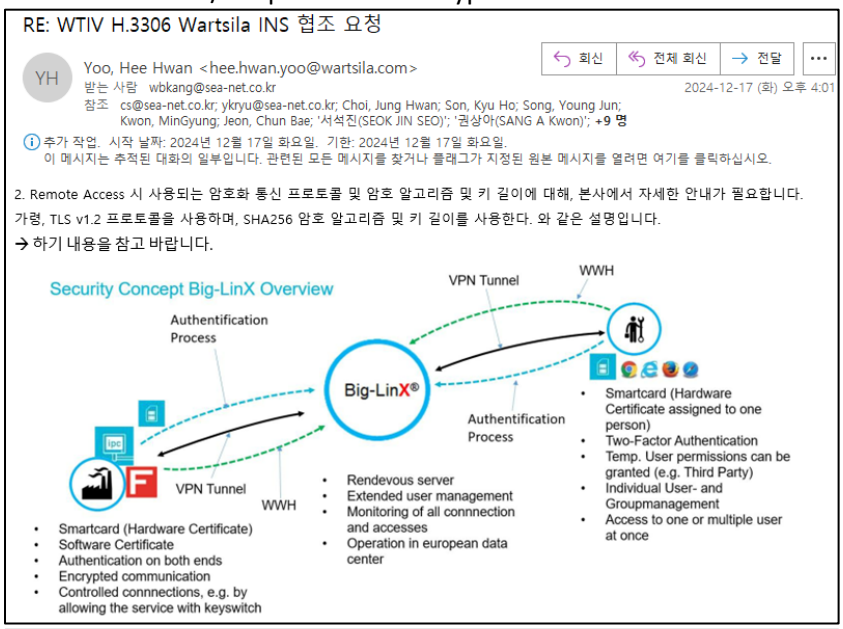
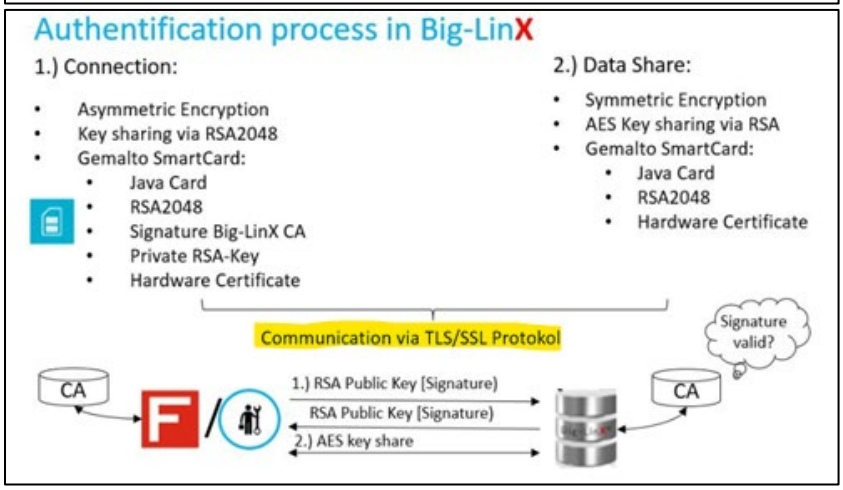
- Comments :
- Actual Results :

Refer to the manufacturer's information in the detailed step.

5.3.5. Communication integrity

The system shall protect the integrity of transmitted information.

Requirement(s): 4.4.2 Community integrity / IEC 62443-3-3 SR 3.1

Step No	Task Description	Expected Result	Result
1	Check the system may protect the information integrity.	There is an information integrity protection method.	
Detailed Steps	5.3.5.1. Wartsila headquarters replied regarding this requirement below. Communication via TLS/SSL protocol is encrypted method of remote access.  		
Comments & Actual Results	- Comments : - Actual Results :		

5.3.6. Session integrity

The system shall protect the integrity of sessions over untrusted networks by rejecting invalid session IDs. Session IDs shall be invalidated upon logout or session termination, and each session shall use a unique session ID. Unexpected session IDs shall be treated as invalid.

Requirement(s): 4.4.9 Session integrity / IEC 62443-3-3 SR 3.8
4.4.9 Session integrity / IEC 62443-3-3 SR 3.8 RE 1
4.4.9 Session integrity / IEC 62443-3-3 SR 3.8 RE 2

Step No	Task Description	Expected Result	Result
1	Check the system may protect the session integrity.	There is a session integrity protection method.	**Pass**
2	Check the system may invalidate session IDs upon user logout or other session termination.	After termination, the session IDs become invalid.	**Pass**
3	Check the system may generate a unique session ID for each session.	All session IDs are unique.	**Pass**
Detailed Steps	5.3.6. Wartsila headquarters replied regarding this requirement below. Communication via TLS/SSL protocol is encrypted method of remote access.		
Comments & Actual Results	- Comments : - Actual Results : See 5.3.5		

5.3.6. Session integrity

The system shall protect the integrity of sessions over untrusted networks by rejecting invalid session IDs. Session IDs shall be invalidated upon logout or session termination, and each session shall use a unique session ID. Unexpected session IDs shall be treated as invalid.

Requirement(s): 4.4.9 Session integrity / IEC 62443-3-3 SR 3.8
4.4.9 Session integrity / IEC 62443-3-3 SR 3.8 RE 1
4.4.9 Session integrity / IEC 62443-3-3 SR 3.8 RE 2

Step No	Task Description	Expected Result	Result
1	Check the system may protect the session integrity.	There is a session integrity protection method.	
2	Check the system may invalidate session IDs upon user logout or other session termination.	After termination, the session IDs become invalid.	
3	Check the system may generate a unique session ID for each session.	All session IDs are unique.	
Detailed Steps	5.3.6. Wartsila headquarters replied regarding this requirement below. Communication via TLS/SSL protocol is encrypted method of remote access.		
Comments & Actual Results	- Comments : - Actual Results :		

5.3.7. Information confidentiality

The system shall protect the confidentiality of information explicitly authorized for reading.

Requirement(s): 4.5.2 Information confidentiality / IEC 62443-3-3 SR 4.1

Step No	Task Description	Expected Result	Result
1	Check the system may protect the information confidentiality.	There is an information confidentiality protection method.	**Pass**
Detailed Steps	5.3.7.1 Wartsila headquarters replied regarding this requirement below. Communication via TLS/SSL protocol is encrypted method of remote access.		
Comments & Actual Results	- Comments : - Actual Results : See 5.3.5		

5.3.7. Information confidentiality

The system shall protect the confidentiality of information explicitly authorized for reading.

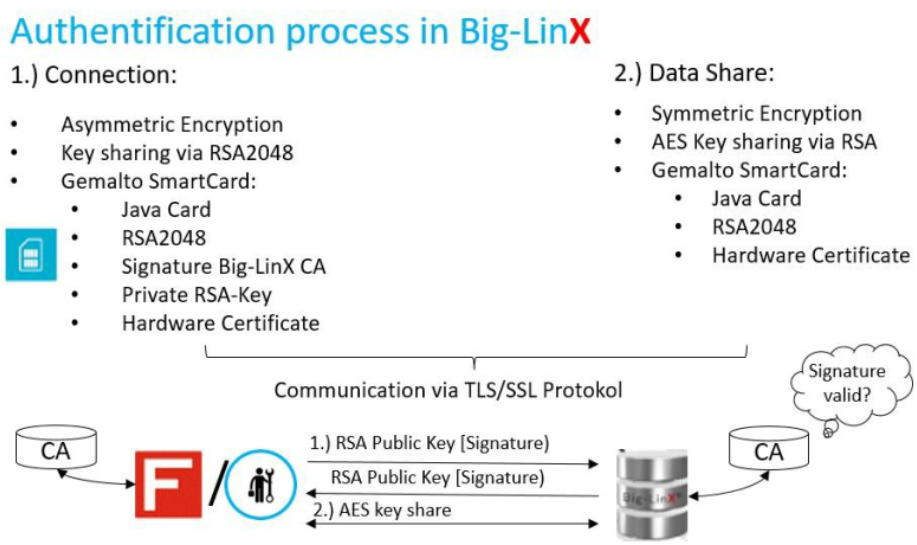
Requirement(s): 4.5.2 Information confidentiality / IEC 62443-3-3 SR 4.1

Step No	Task Description	Expected Result	Result
1	Check the system may protect the information confidentiality.	There is an information confidentiality protection method.	
Detailed Steps	5.3.7.1 Wartsila headquarters replied regarding this requirement below. Communication via TLS/SSL protocol is encrypted method of remote access.		
Comments & Actual Results	- Comments : - Actual Results :		

5.3.8. Use of cryptography

The system shall use cryptographic algorithms, key sizes, and key management mechanisms aligned with best practices for communication over untrusted networks.

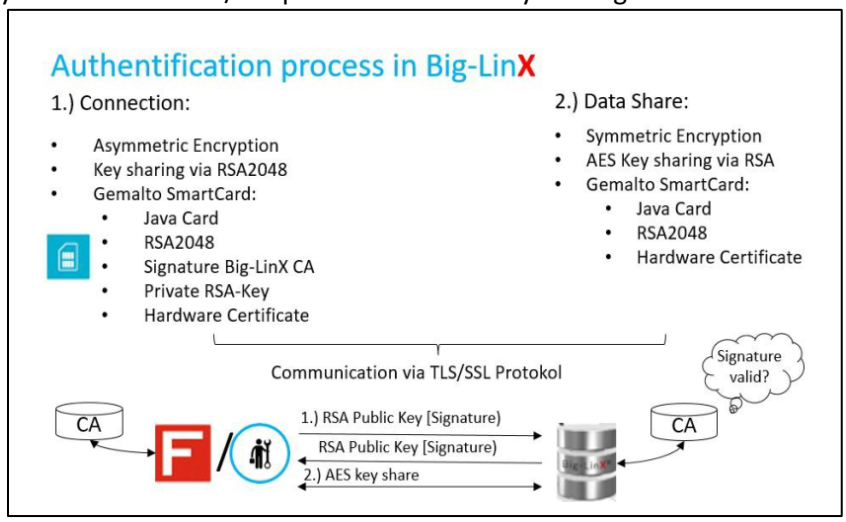
Requirement(s): 4.5.4 Use of cryptography / IEC 62443-3-3 SR 4.3

Step No	Task Description	Expected Result	Result
1	Check the system may use cryptographic algorithms.	There is a cryptographic algorithm used.	**Pass**
Detailed Steps	5.3.8.1. Wartsila headquarters replied regarding this requirement below. The system uses the TLS/SSL protocol and AES key sharing via RSA2048. 		
Comments & Actual Results	- Comments : - Actual Results : See 5.3.5		

5.3.8. Use of cryptography

The system shall use cryptographic algorithms, key sizes, and key management mechanisms aligned with best practices for communication over untrusted networks.

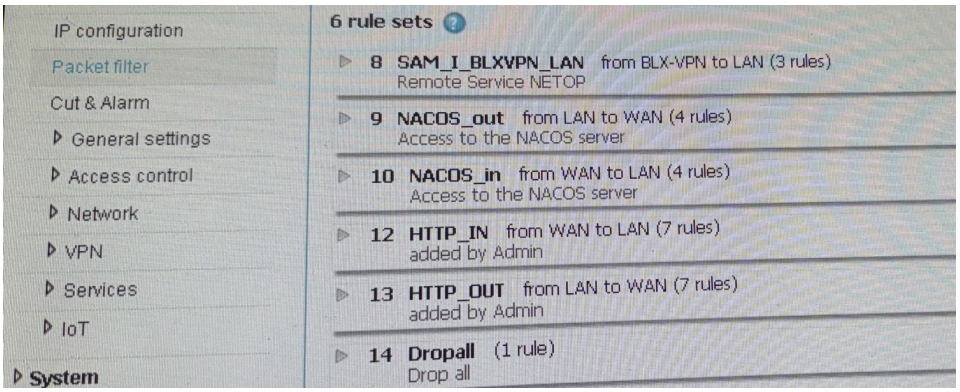
Requirement(s): 4.5.4 Use of cryptography / IEC 62443-3-3 SR 4.3

Step No	Task Description	Expected Result	Result
1	Check the system may use cryptographic algorithms.	There is a cryptographic algorithm used.	
Detailed Steps	5.3.8.1. Wartsila headquarters replied regarding this requirement below. The system uses the TLS/SSL protocol and AES key sharing via RSA2048. 		
Comments & Actual Results	- Comments : - Actual Results :		

5.3.9. Zone boundary protection

The system shall deny network traffic by default, allowing only traffic explicitly permitted through whitelisting.

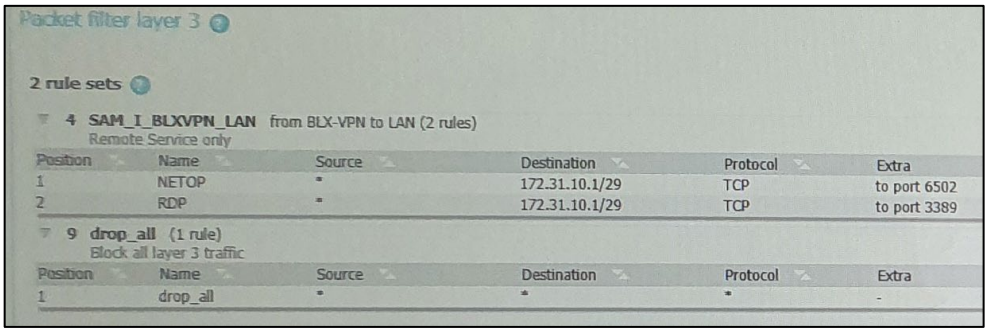
Requirement(s): 4.6.3 Zone boundary protection / IEC 62443-3-3 SR 5.2 RE 1

Step No	Task Description	Expected Result	Result
1	Check the system deny network traffic by default, and allow whitelisted traffics only.	Firewall rules are relevantly set.	**Pass**
Detailed Steps	5.3.9.1. Wartsila headquarters replied regarding this requirement below. Check firewall rule set 		
Comments & Actual Results	- Comments : - Actual Results : Refer 5.1.1		

5.3.9. Zone boundary protection

The system shall deny network traffic by default, allowing only traffic explicitly permitted through whitelisting.

Requirement(s): 4.6.3 Zone boundary protection / IEC 62443-3-3 SR 5.2 RE 1

Step No	Task Description	Expected Result	Result
1	Check the system deny network traffic by default, and allow whitelisted traffics only.	Firewall rules are relevantly set.	
Detailed Steps	5.3.9.1. Wartsila headquarters replied regarding this requirement below. Check firewall rule set 		
Comments & Actual Results	- Comments : - Actual Results :		

5.3.10. General purpose person-to-person communication restrictions

The system shall block person-to-person messages from users or systems external to the control system.

Requirement(s): 4.6.4 General purpose person-to-person communication restrictions / IEC 62443-3-3 SR 5.3

Step No	Task Description	Expected Result	Result
1	Check whether the system can block person-to-person messages from users or systems external to the control system.	Any unauthorized messages are blocked.	**Pass**
Detailed Steps	Human users access the system through INS OS PC. Therefore, check the list of software installed on the OS PC to verify that there is no messenger program.		
Comments & Actual Results	- Comments : - Actual Results : Checked that no person to person message service are running.		

5.3.10. General purpose person-to-person communication restrictions

The system shall block person-to-person messages from users or systems external to the control system.

Requirement(s): 4.6.4 General purpose person-to-person communication restrictions / IEC 62443-3-3 SR 5.3

Step No	Task Description	Expected Result	Result
1	Check whether the system can block person-to-person messages from users or systems external to the control system.	Any unauthorized messages are blocked.	
Detailed Steps	Human users access the system through INS OS PC. Therefore, check the list of software installed on the OS PC to verify that there is no messenger program.		
Comments & Actual Results	- Comments : - Actual Results :		

5.3.11. Least functionality

The system shall prohibit or restrict unnecessary functions and services, such as file transfer protocols and instant messaging.

Requirement(s): 4.8.8 Least functionality / IEC 62443-3-3 SR 7.7

Step No	Task Description	Expected Result	Result
1	Check whether there is no unnecessary functions or services running in the system.	No unnecessary functions are running.	**Pass**
Detailed Steps	Verify that all services are minimally permitted by checking software list and firewall rule.		
Comments & Actual Results	- Comments : - Actual Results : Checked that no unnecessary functions are running		

5.3.11. Least functionality

The system shall prohibit or restrict unnecessary functions and services, such as file transfer protocols and instant messaging.

Requirement(s): 4.8.8 Least functionality / IEC 62443-3-3 SR 7.7

Step No	Task Description	Expected Result	Result
1	Check whether there is no unnecessary functions or services running in the system.	No unnecessary functions are running.	
Detailed Steps	Verify that all services are minimally permitted by checking software list and firewall rule.		
Comments & Actual Results	- Comments : - Actual Results :		