Cyber Security Test Procedure For S525s Project (115,000 DWT Class Oil/Product Tanker)

< S527 / Main Engine >

Cyber Security Test Procedure For S525s Project (115,000 DWT Class Oil/Product Tanker)

< S560 / Main Engine >

CONTENTS

CONTENTS

1. History

No.	Date (DD/MM/YYYY)	Revision	Description	Remarks
1	00/00/2024	A	First Issue	First Issue

2. Introduction

2.1. Scope

Survey Date	11/09/2024	Surveyor(s) name(s)	Simen, Vike Lande
Test Location	ECR		

2.2. Definitions

Owner : The entity responsible for possessing and managing the vessel

Yard : HD Hyundai Mipo (HMD), a shipyard where ships are constructed

Supplier : MAN-ES, 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”

2.3. Applicable Specifications and Standards

2.3.1. Documents

Ref.	Title
4A000E020	Cyber Security Management Plan

2.3.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2021)
DNV-CG-0325	Cyber Secure (Edition July 2021)
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	00/00/2025	A	First Issue	First Issue

2. Introduction

2.1. Scope

Survey Date	00/00/2025	Surveyor(s) name(s)	
Test Location			

2.2. Definitions

Owner : The entity responsible for possessing and managing the vessel

Yard : HD Hyundai Mipo (HMD), a shipyard where ships are constructed

Supplier : MAN-ES, 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”

2.3. Applicable Specifications and Standards

2.3.1. Documents

Ref.	Title
4A000E020	Cyber Security Management Plan

2.3.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2021)
DNV-CG-0325	Cyber Secure (Edition July 2021)
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. Background

Under the S525s 115,000 DWT Class Oil/Product Tanker Project, 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.

4. Perimeter and Approach

4.1. Perimeter

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.	SYSTEM	H/W TYPE	BRAND	MODEL	DESCRIPTION
1	Router	Router	Phoenix Contact	mGuard rs4000	VPN Router
2	Switch	Switch	Phoenix Contact	FL Switch 2316	Managed Switch
3	PC	PC	MAN	Standard Industrial PC	EMS-MOP PC
4	Panel PC	Panel PC	MAN	Integrated PC	ECS-MOP B PC
5	Panel PC	Panel PC	MAN	Integrated PC	ERCS-MOP PC

4.2. Approach

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

4.3. 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 as they exist at the time of the survey with the established criteria.

3. Background

Under the S525s 115,000 DWT Class Oil/Product Tanker Project, 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.

4. Perimeter and Approach

4.1. Perimeter

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.	SYSTEM	H/W TYPE	BRAND	MODEL	DESCRIPTION
1	Router	Router	Phoenix Contact	mGuard rs4000	VPN Router
2	Switch	Switch	Phoenix Contact	FL Switch 2316	Managed Switch
3	PC	PC	MAN	Standard Industrial PC	EMS-MOP PC
4	Panel PC	Panel PC	MAN	Integrated PC	ECS-MOP B PC
5	Panel PC	Panel PC	MAN	Integrated PC	ERCS-MOP PC

4.2. Approach

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

4.3. 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 as they exist at the time of the survey with the established criteria.

5. System Test

[Sample]

No	Category	Control Objective	Findings	Test Status
1	Documentation	Verify availability of:		Pass / Fail / N/A

- **Based on the mutual discussion between the Class and the Supplier, M/E control and EMS system is excluded from the test procedure document.**
- **The Supplier conducted test with the Class on July 3rd, 2024. The result would be delivered by the supplier to the Class directly, and the Class would review and approve it accordingly.**

6. Integration Test

- **Based on the mutual discussion between the Class and the Supplier, M/E control and EMS system is excluded from the test procedure document.**
- **The Supplier conducted test with the Class on July 3rd, 2024. The result would be delivered by the supplier to the Class directly, and the Class would review and approve it accordingly.**

5. System Test

[Sample]

No	Category	Control Objective	Findings	Test Status
1	Documentation	Verify availability of:		Pass / Fail / N/A

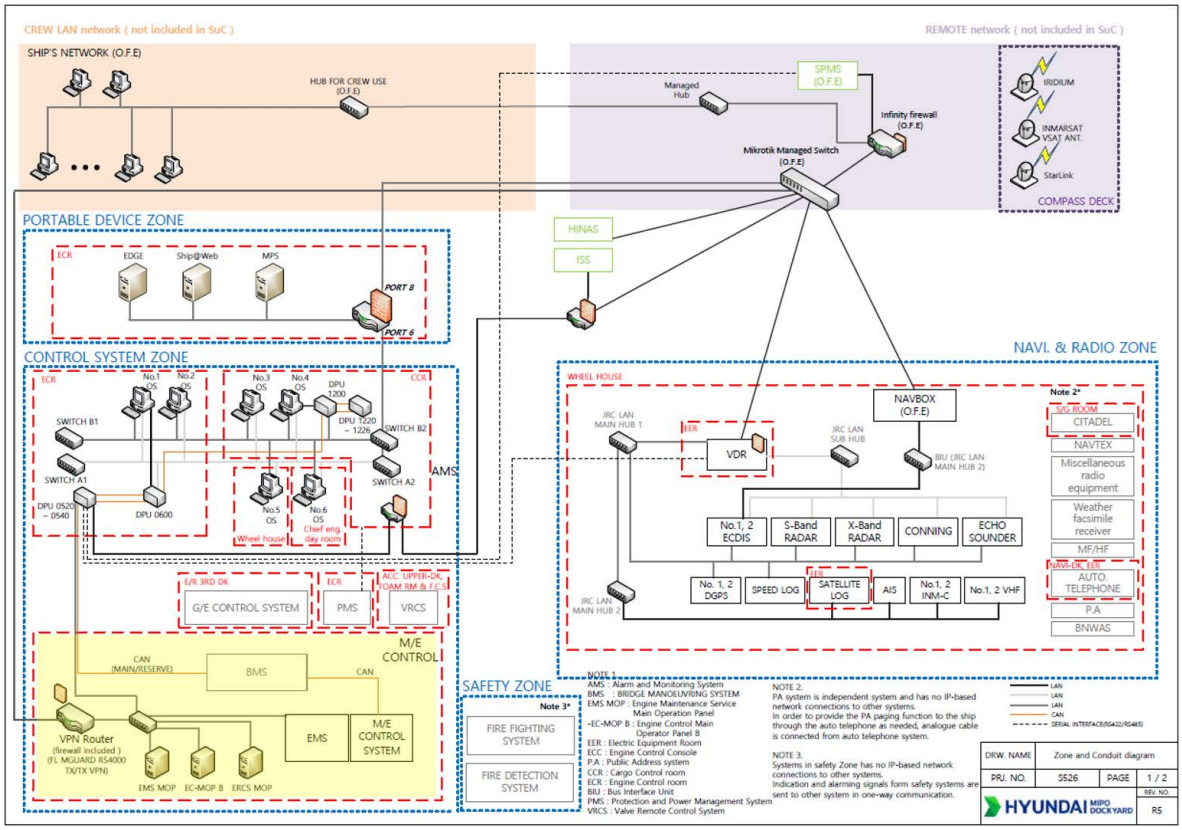
- **Based on the mutual discussion between the Class and the Supplier, M/E control and EMS system is excluded from the test procedure document.**
- **The Supplier conducted test with the Class on July 3rd, 2024. The result would be delivered by the supplier to the Class directly, and the Class would review and approve it accordingly.**

6. Integration Test

- **Based on the mutual discussion between the Class and the Supplier, M/E control and EMS system is excluded from the test procedure document.**
- **The Supplier conducted test with the Class on July 3rd, 2024. The result would be delivered by the supplier to the Class directly, and the Class would review and approve it accordingly.**

7. Appendix

7.1. Zone and Conduit Diagram

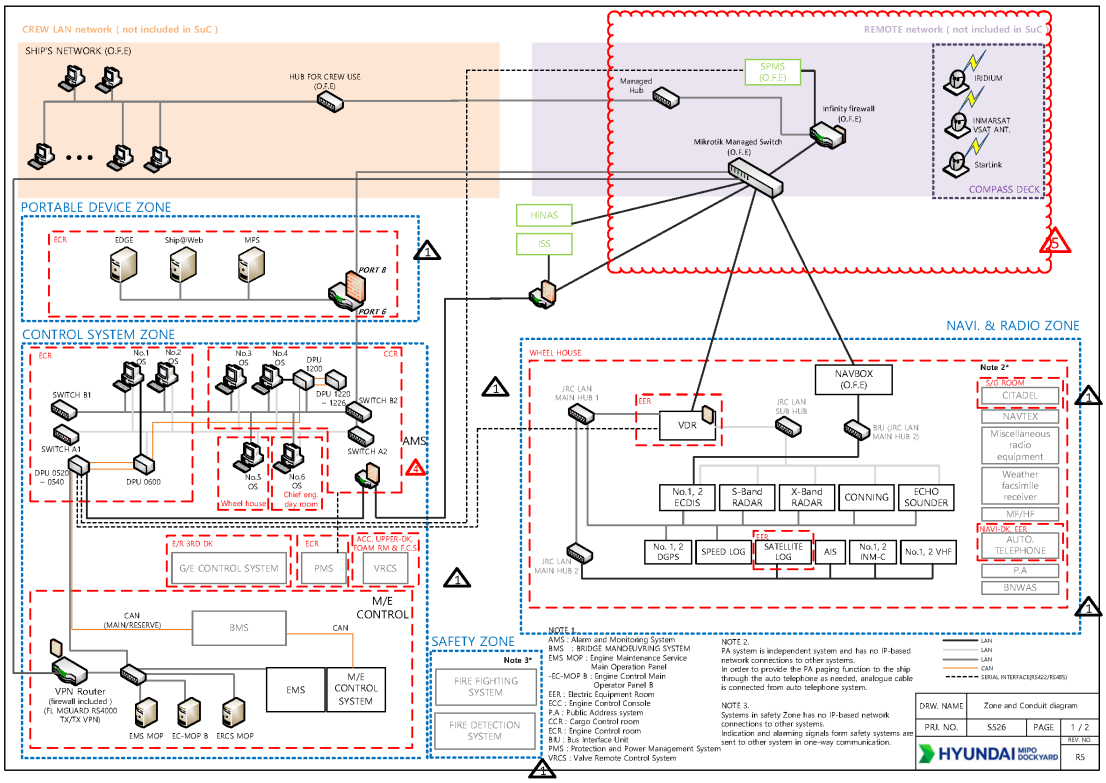


7.2. Device Information

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
1	VPN Router	Router	Phoenix contact	mGuard rs4000	-	-	-	ECR
2	Managed Switch	Switch	Phoenix contact	FL Switch 2316	-	-	-	ECR
3	EMS-MOP PC	PC	MAN	Standard Industrial PC	-	-	-	ECR
4	ECS-MOP B PC	Panel PC	MAN	Integrated PC	-	-	-	ECR
5	ERCS-MOP PC	Panel PC	MAN	Integrated PC	-	-	-	ECR

7. Appendix

7.1. Zone and Conduit Diagram



7.2. Device Information

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
1	VPN Router	Router	Phoenix contact	mGuard rs4000	-	-	-	ECR
2	Managed Switch	Switch	Phoenix contact	FL Switch 2316	-	-	-	ECR
3	EMS-MOP PC	PC	MAN	Standard Industrial PC	-	-	-	ECR
4	ECS-MOP B PC	Panel PC	MAN	Integrated PC	-	-	-	ECR
5	ERCS-MOP PC	Panel PC	MAN	Integrated PC	-	-	-	ECR

Cyber Security Test Procedure For S525s Project (115,000 DWT Class Oil/Product Tanker)

< S527 / Alarm & Monitoring System & Bridge Maneuvering System>

Cyber Security Test Procedure For S525s Project (115,000 DWT Class Oil/Product Tanker)

< S560 / Alarm & Monitoring System & Bridge Maneuvering System>

CONTENTS

CONTENTS

1. History

No.	Date (DD/MM/YYYY)	Revision	Description	Remarks
1	00/00/2024	A	First Issue	First Issue

2. Introduction

2.1. Scope

Survey Date	12/09/2024	Surveyor(s) name(s)	Simen, Vike Lande
Test Location	NaviDK, EER, CCR, ECR		

2.2. Definitions

Owner : The entity responsible for possessing and managing the vessel

Yard : HD Hyundai Mipo (HMD), a shipyard where ships are constructed

Supplier : Kongsberg, 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”

2.3. Applicable Specifications and Standards

2.3.1. Documents

Ref.	Title
4A000E020	Cyber Security Management Plan
TAA000033K	Type Approval Certificate

2.3.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2021)
DNV-CG-0325	Cyber Secure (Edition July 2021)
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	00/00/2025	A	First Issue	First Issue

2. Introduction

2.1. Scope

Survey Date	00/00/2025	Surveyor(s) name(s)	
Test Location	NaviDK, EER, CCR, ECR		

2.2. Definitions

Owner : The entity responsible for possessing and managing the vessel

Yard : HD Hyundai Mipo (HMD), a shipyard where ships are constructed

Supplier : Kongsberg, 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”

2.3. Applicable Specifications and Standards

2.3.1. Documents

Ref.	Title
4A000E020	Cyber Security Management Plan
TAA000033K	Type Approval Certificate

2.3.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2021)
DNV-CG-0325	Cyber Secure (Edition July 2021)
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. Background

Under the S525s 115,000 DWT Class Oil/Product Tanker Project, 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.

4. Perimeter and Approach

4.1. Perimeter

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.	SYSTEM	H/W TYPE	BRAND	MODEL	DESCRIPTION
1	AMS	Workstation	Lenovo	MC340	No.1 Operator Station
2	AMS	Workstation	Lenovo	MC340	No.2 Operator Station
3	AMS	Workstation	Lenovo	MC340	No.3 Operator Station
4	AMS	Workstation	Lenovo	MC340	No.4 Operator Station
5	AMS	Workstation	Lenovo	MC340	No.5 Operator Station
6	AMS	Workstation	Lenovo	MC340	No.6 Operator Station
7	AMS	Workstation	Lenovo	MC340	No.7 Operator Station
8	AMS	Switch	Moxa	EDS-408A	No.1 OS Switch
9	AMS	Switch	Moxa	EDS-408A	No.2 OS Switch
10	AMS	Switch	Moxa	EDS-408A	No.3 OS Switch
11	AMS	Switch	Moxa	EDS-408A	No.4 OS Switch
12	AMS	HMI	KM	MPS	7" Touch Panel PC
13	AMS	Server	Lenovo	MC340	Ship@Web Server
14	AMS	Router	Cisco	C891-24X/K9	K-GSN Router
15	BMS	Workstation	KM	CP-12	Workstation(W/H)
16	BMS	Workstation	KM	CP-12	Workstation(ECR)

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

NO.	BRAND	MODEL	VERSION	DESCRIPTION
1	EICAR	Anti Malware Test File	-	Malware Protection Function Check
2	Wireshark	Wireshark	4.2.XX	Packet Capture and Monitoring
3	Windows	Command Prompt	-	Ping Test
4	Famatech	Advanced Port Scanner	2.5.XX	Open Port Scan
5	Kongsberg	IP Traffic Generator	-	DoS Test

4.2. Approach

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

4.3. 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. Background

Under the S525s 115,000 DWT Class Oil/Product Tanker Project, 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.

4. Perimeter and Approach

4.1. Perimeter

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.	SYSTEM	H/W TYPE	BRAND	MODEL	DESCRIPTION
1	AMS	Workstation	Lenovo	MC340	No.1 Operator Station
2	AMS	Workstation	Lenovo	MC340	No.2 Operator Station
3	AMS	Workstation	Lenovo	MC340	No.3 Operator Station
4	AMS	Workstation	Lenovo	MC340	No.4 Operator Station
5	AMS	Workstation	Lenovo	MC340	No.5 Operator Station
6	AMS	Workstation	Lenovo	MC340	No.6 Operator Station
7	AMS	Workstation	Lenovo	MC340	No.7 Operator Station
8	AMS	Switch	Moxa	EDS-408A	No.1 OS Switch
9	AMS	Switch	Moxa	EDS-408A	No.2 OS Switch
10	AMS	Switch	Moxa	EDS-408A	No.3 OS Switch
11	AMS	Switch	Moxa	EDS-408A	No.4 OS Switch
12	AMS	HMI	KM	MPS	7" Touch Panel PC
13	AMS	Server	Lenovo	MC340	Ship@Web Server
14	AMS	Router	Cisco	C891-24X/K9	K-GSN Router
15	BMS	Workstation	KM	CP-12	Workstation(W/H)
16	BMS	Workstation	KM	CP-12	Workstation(ECR)

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

NO.	BRAND	MODEL	VERSION	DESCRIPTION
1	EICAR	Anti Malware Test File	-	Malware Protection Function Check
2	Wireshark	Wireshark	4.2.XX	Packet Capture and Monitoring
3	Windows	Command Prompt	-	Ping Test
4	Famatech	Advanced Port Scanner	2.5.XX	Open Port Scan
5	Kongsberg	IP Traffic Generator	-	DoS Test

4.2. Approach

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

4.3. 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.

5. System Test

[Sample]

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

5.1. General Test

5.1.1. AMS

5.1.1.1. 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) : 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.	**Pass**
2	Check the system's configuration information to verify that the system is appropriately set.	Configuration is appropriately set.	**Pass**
Detailed Steps	5.1.1.1.1. The asset inventory of installed hardware and software should be identical to the Type Approval document, or its regarding information. Target assets are: Workstation, Switch, MPS 5.1.1.1.2. The system's configuration should be identical with Type Approval document, or its regarding information. For instance, its software version would be higher than 12.16.ZZ.		
Comments & Actual Results	Comments: - SW: 1.16.108 - HW: OK Actual Results: - The TA matched the actual set up of the AMS system and C600 hardware list that was submitted in the CSMP.		

5. System Test

[Sample]

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

5.1. General Test

5.1.1. AMS

5.1.1.1. 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) : 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.	
2	Check the system's configuration information to verify that the system is appropriately set.	Configuration is appropriately set.	
Detailed Steps	5.1.1.1.1. The asset inventory of installed hardware and software should be identical to the Type Approval document, or its regarding information. Target assets are: Workstation, Switch, MPS 5.1.1.1.2. The system's configuration should be identical with Type Approval document, or its regarding information. For instance, its software version would be higher than 12.16.ZZ.		
Comments & Actual Results			

5.1.2. BMS

5.1.2.1. 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	Check that unused ports are blocked, and device connection is appropriately managed.	Any unused ports are blocked	**Pass**
2	Connect portable and/or mobile devices to the system and check the system can control device usage.	Portable and mobile device usage is controlled	**Pass**
Detailed Steps	5.1.2.1.1. All the devices' unused ports should be blocked. This can be checked by visual inspection. Logical block can be accepted, and this can be checked when MPS's running is verified from Task Manager. 5.1.2.1.2. When the user tries to connect portable and/or mobile devices to CP-12 without scanning from MPS, the system would block the devices or programs' running. This can be checked by running/copying files from unscanned USB stick.		
Comments & Actual Results	Comments: - MPS Actual Results: All ports are logically blocked and the MPS driver could be seen running in the background through the task manager. When a USB was inserted into the system, it would not auto-run nor would it run any files in the USB as it did not have a valid key. Files in a USB/portable device can only be run once validated by the MPS.		

5.1.2. BMS

5.1.2.1. 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	Check that unused ports are blocked, and device connection is appropriately managed.	Any unused ports are blocked	
2	Connect portable and/or mobile devices to the system and check the system can control device usage.	Portable and mobile device usage is controlled	
Detailed Steps	5.1.2.1.1. All the devices' unused ports should be blocked. This can be checked by visual inspection. Logical block can be accepted, and this can be checked when MPS's running is verified from Task Manager. 5.1.2.1.2. When the user tries to connect portable and/or mobile devices to CP-12 without scanning from MPS, the system would block the devices or programs' running. This can be checked by running/copying files from unscanned USB stick.		
Comments & Actual Results			

5.1.2.2. 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	5.1.2.2.1 The event logs and system logs can be checked from CP-12's Windows Event Viewer. The logs contain information including timestamp, source, and event result.		
Comments & Actual Results	Comments: - Win log Actual Results: - Events were checked on windows event viewer.		

5.1.2.2. 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	5.1.2.2.1 The event logs and system logs can be checked from CP-12's Windows Event Viewer. The logs contain information including timestamp, source, and event result.		
Comments & Actual Results			

5.1.2.3. 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	Try inserting and running malicious code/program files from the system, and check that the system blocks malicious code/programs.	Malicious code/program is not running	**Pass**
Detailed Steps	5.1.2.3.1. When the user tries to connect portable and/or mobile devices containing EICAR malware test program to CP-12 without scanning from MPS, the system would block the devices' running. This can be checked by running/copying files from unscanned USB stick.		
Comments & Actual Results	Comments: - MPS Actual Results: The MPS prevents running files in invalid USB stick (USBs without a valid key). It was not possible to run, copy, or move files from the USB stick to the local system. Files in a USB stick can only be run once validated by the MPS.		

5.1.2.3. 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	Try inserting and running malicious code/program files from the system, and check that the system blocks malicious code/programs.	Malicious code/program is not running	
Detailed Steps	5.1.2.3.1. When the user tries to connect portable and/or mobile devices containing EICAR malware test program to CP-12 without scanning from MPS, the system would block the devices' running. This can be checked by running/copying files from unscanned USB stick.		
Comments & Actual Results			

5.1.2.4. Use of Cryptography

When cryptography is required, the system shall use appropriate methods for transmit the information.

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

Step No	Task Description	Expected Result	Result
1	Check that when the system uses data cryptography, its algorithm and key are appropriately set based on best practices and recommendations.	Cryptography mechanism is appropriately set	**N/A**
Detailed Steps	5.1.2.4.1. N/A, as the system is integrated with AMS with CAN communication.		
Comments & Actual Results	Comments: Actual Results: As the BMS communicates with the AMS via CAN transmission, this test can be dismissed. The BMS and AMS use a L2C (LAN to CAN) converter to convert LAN data to CAN format.		

5.1.2.4. Use of Cryptography

When cryptography is required, the system shall use appropriate methods for transmit the information.

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

Step No	Task Description	Expected Result	Result
1	Check that when the system uses data cryptography, its algorithm and key are appropriately set based on best practices and recommendations.	Cryptography mechanism is appropriately set	**N/A**
Detailed Steps	5.1.2.4.1. N/A, as the system is integrated with AMS with CAN communication.		
Comments & Actual Results			

5.1.2.5. 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	5.1.2.5.1 The system data can be backed up in an image form by KM engineer after following certain process. 5.1.2.5.2. The system data can be restored from backup data image by KM engineer after following certain process.		
Comments & Actual Results	Comments: - Backup possible - OK Actual Results: Kongsberg engineers explained that BMS's backup and restoration can be done by AMS, as AMS controls BMS.		

5.1.2.5. 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	5.1.2.5.1 The system data can be backed up in an image form by KM engineer after following certain process. 5.1.2.5.2. The system data can be restored from backup data image by KM engineer after following certain process.		
Comments & Actual Results			

5.1.3. Remote Cabinet

5.1.3.1. 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	Check that unused ports are blocked, and device connection is appropriately managed.	Any unused ports are blocked	**Pass**
2	Connect portable and/or mobile devices to the system and check the system can control device usage.	Portable and mobile device usage is controlled	**Pass**
Detailed Steps	5.1.3.1.1. All the devices' unused ports should be blocked. As this is done logically, this can be checked by connecting laptop to any unused ports, or by KM Engineer's explanation. 5.1.3.1.2. When the user tries to connect portable and/or mobile devices to server without scanning from MPS, the system would block the devices or programs' running.		
Comments & Actual Results	Comments: - Covered by TA - Located in ECR Actual Results: Devices regarding Remote Access are type approved. It was also checked that the devices are located in a restricted area(ECR).		

5.1.3. Remote Cabinet

5.1.3.1. 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	Check that unused ports are blocked, and device connection is appropriately managed.	Any unused ports are blocked	
2	Connect portable and/or mobile devices to the system and check the system can control device usage.	Portable and mobile device usage is controlled	
Detailed Steps	5.1.3.1.1. All the devices' unused ports should be blocked. As this is done logically, this can be checked by connecting laptop to any unused ports, or by KM Engineer's explanation. 5.1.3.1.2. When the user tries to connect portable and/or mobile devices to server without scanning from MPS, the system would block the devices or programs' running.		
Comments & Actual Results			

5.1.3.2. 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	**N/A**
Detailed Steps	5.1.3.2.1 N/A, as the event logs and system logs are stored in onshore server.		
Comments & Actual Results	Comments: - Not tested Actual Results: It was not possible to test this task, as logs are stored onshore.		

5.1.3.2. 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	**N/A**
Detailed Steps	5.1.3.2.1 N/A, as the event logs and system logs are stored in onshore server.		
Comments & Actual Results			

5.1.3.3. 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	Try inserting and running malicious code/program files from the system, and check that the system blocks malicious code/programs.	Malicious code/program is not running	**N/A**
Detailed Steps	5.1.3.3.1. N/A, as the system does not allow unauthorized device's connection.		
Comments & Actual Results	Comments: - Not tested, TA Actual Results: Devices regarding Remote Access are type approved.		

5.1.3.3. 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	Try inserting and running malicious code/program files from the system, and check that the system blocks malicious code/programs.	Malicious code/program is not running	**N/A**
Detailed Steps	5.1.3.3.1. N/A, as the system does not allow unauthorized device's connection.		
Comments & Actual Results			

5.1.3.4. Use of Cryptography

When cryptography is required, the system shall use appropriate methods for transmit the information.

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

Step No	Task Description	Expected Result	Result
1	Check that when the system uses data cryptography, its algorithm and key are appropriately set based on best practices and recommendations.	Cryptography mechanism is appropriately set	**Pass**
Detailed Steps	5.1.3.4.1. The system would use cryptography when it is required. This can be checked by reviewing packet transmission, or KM Engineer's explanation.		
Comments & Actual Results	Comments: - Not tested Actual Result: Kongsberg engineers has explained that the Bomgar client uses IPSec VPN for remote access sessions.		

5.1.3.4. Use of Cryptography

When cryptography is required, the system shall use appropriate methods for transmit the information.

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

Step No	Task Description	Expected Result	Result
1	Check that when the system uses data cryptography, its algorithm and key are appropriately set based on best practices and recommendations.	Cryptography mechanism is appropriately set	
Detailed Steps	5.1.3.4.1. The system would use cryptography when it is required. This can be checked by reviewing packet transmission, or KM Engineer's explanation.		
Comments & Actual Results			

5.1.3.5. 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	**N/A**
2	Check that the control system data can be restored after following certain procedure, to recover from data loss.	System data can be restored	**N/A**
Detailed Steps	5.1.3.5.1 and 5.1.3.5.2. N/A, as the system does not support this function.		
Comments & Actual Results	Comments: - Not tested Actual Results: Back up and restoration processes were tested earlier in the test procedure for both AMS and BMS.		

5.1.3.5. 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	**N/A**
2	Check that the control system data can be restored after following certain procedure, to recover from data loss.	System data can be restored	**N/A**
Detailed Steps	5.1.3.5.1 and 5.1.3.5.2. N/A, as the system does not support this function.		
Comments & Actual Results			

5.2. Test for Connection via Untrusted Network

Note. When a device is connected to an untrusted network, the following requirements shall be fulfilled.

5.2.1. Identification and Authentication

Human users, software processes or devices, shall be identified and authenticated for access to the system.

(Requirement(s): 4.2.2 User identification and authentication / IEC 62443-3-3 SR 1.1
4.2.3 Application or device identification and authentication / IEC-62443-3-3 SR 1.2)

Step No	Task Description	Expected Result	Result
1	Check that the system identifies and authenticates human user access based on specific processes.	The system shall monitor and control human access	**Pass**
2	Check that the system identifies and authenticates devices and software access.	The system shall monitor and control devices and software access	**Pass**
Detailed Steps	5.2.1.1. When the system is connected to KM GSC(Global Service Center), the system should be able to identify the user access. 5.2.1.2. When the system is connected to KM GSC(Global Service Center), the system should be able to identify its connecting device. This can be checked by GSC or from the Headquarters.		
Comments & Actual Results	Comments: - OK, Bomgar Actual Results: When the Kongsberg engineers allow remote connections from KM GSC, Bomgar prompted an option to allow or deny remote access. When the connection is allowed, the system identified who (name) is connected and monitored what the connected person is doing from KM GSC.		

5.2. Test for Connection via Untrusted Network

Note. When a device is connected to an untrusted network, the following requirements shall be fulfilled.

5.2.1. Identification and Authentication

Human users, software processes or devices, shall be identified and authenticated for access to the system.

(Requirement(s): 4.2.2 User identification and authentication / IEC 62443-3-3 SR 1.1
4.2.3 Application or device identification and authentication / IEC-62443-3-3 SR 1.2)

Step No	Task Description	Expected Result	Result
1	Check that the system identifies and authenticates human user access based on specific processes.	The system shall monitor and control human access	
2	Check that the system identifies and authenticates devices and software access.	The system shall monitor and control devices and software access	
Detailed Steps	5.2.1.1. When the system is connected to KM GSC(Global Service Center), the system should be able to identify the user access. 5.2.1.2. When the system is connected to KM GSC(Global Service Center), the system should be able to identify its connecting device. This can be checked by GSC or from the Headquarters.		
Comments & Actual Results			

5.2.2. Access via Untrusted Network

Any access from or via untrusted networks shall be monitored (e.g., logged, indicated, alarmed) and controlled (e.g., denied, restricted).

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

Step No	Task Description	Expected Result	Result
1	Check whether the system monitors and controls remote access.	The system shall monitor and control access	**Pass**
2	Check whether the system denies access requests via untrusted networks, if the request is not approved.	The system can deny unapproved access request	**Pass**
Detailed Steps	5.2.2.1. When the system is connected to KM GSC(Global Service Center), the system may be able to monitors and controls its access. Monitoring can be checked by GSC or from the Headquarters, and controlling can be checked from either onboard or onshore. 5.2.2.2. When the remote access is not approved (or not planned), then the system should be able to deny that access		
Comments & Actual Results	Comments: - Checked logs, OK Actual Results: The AMS can monitor and control access of connected user. The AMS can disconnect the remote session at any time and can deny access when the request is not approved.		

5.2.2. Access via Untrusted Network

Any access from or via untrusted networks shall be monitored (e.g., logged, indicated, alarmed) and controlled (e.g., denied, restricted).

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

Step No	Task Description	Expected Result	Result
1	Check whether the system monitors and controls remote access.	The system shall monitor and control access	
2	Check whether the system denies access requests via untrusted networks, if the request is not approved.	The system can deny unapproved access request	
Detailed Steps	5.2.2.1. When the system is connected to KM GSC(Global Service Center), the system may be able to monitors and controls its access. Monitoring can be checked by GSC or from the Headquarters, and controlling can be checked from either onboard or onshore. 5.2.2.2. When the remote access is not approved (or not planned), then the system should be able to deny that access		
Comments & Actual Results			

5.2.3. Integrity and Confidentiality

The system shall protect the integrity of transmitted information and sessions, and the system shall be able to protect the confidentiality of information at rest or in transit that has read authorization.

(Requirement(s): 4.4.2 Communication integrity / IEC 62443-3-3 SR 3.1 RE 1
4.4.9 Session integrity / IEC-62443-3-3 SR 3.8
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 integrity.	There is an information integrity protection method	**Pass**
2	Check the system may protect the session integrity.	There is a session integrity protection method	**Pass**
3	Check the system may protect the information confidentiality.	There is an information confidentiality protection method	**Pass**
Detailed Steps	5.2.3.1 to 5.2.3.3. When the system is connected to KM GSC(Global Service Center), the system may be able to protect the transmitted data's integrity and confidentiality, using IPSec VPN method. This can be explained by KM technician.		
Comments & Actual Results	Comments: - Checked vessel FW config Actual Results: The central firewall was shown and explained by the shipowner's IT engineer. It was shown that there is limited access to AMS. Bomgar uses IPSec VPN for any remote connections assuring confidentiality.		

5.2.3. Integrity and Confidentiality

The system shall protect the integrity of transmitted information and sessions, and the system shall be able to protect the confidentiality of information at rest or in transit that has read authorization.

(Requirement(s): 4.4.2 Communication integrity / IEC 62443-3-3 SR 3.1 RE 1
4.4.9 Session integrity / IEC-62443-3-3 SR 3.8
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 integrity.	There is an information integrity protection method	
2	Check the system may protect the session integrity.	There is a session integrity protection method	
3	Check the system may protect the information confidentiality.	There is an information confidentiality protection method	
Detailed Steps	5.2.3.1 to 5.2.3.3. When the system is connected to KM GSC(Global Service Center), the system may be able to protect the transmitted data's integrity and confidentiality, using IPSec VPN method. This can be explained by KM technician.		
Comments & Actual Results			

6. Integration Test

6.1. 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 RE1)

6.1.1. 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.

6.1.2. Test Result

Step No	Task Description	Expected Result	Result
1	Check the cabling within and between zones visually to verify that zones are segmented.	Zones are well segmented	**Pass**
2	Check the device's ACL or VLAN configuration; that network is well segmented, and data cannot be transferred to different zones without approval.	ACL or VLAN is relevantly set	**Pass**
3	Conduct port scanning test to verify that unnecessary ports are not opened.	Unnecessary ports are not opened	**Pass**
Detailed Steps	6.1.2.1. The system's physical cabling should be done appropriately. This can be checked by visual inspection. 6.1.2.2. The system's ACL or VLAN configuration should be set appropriately so that the system network is well segmented. This can be demonstrated by a ping test, or explained by KM technician. 6.1.2.3. The system should not communicate via unnecessary ports. This can be checked by port scanner's scan result.		
Comments & Actual Results	Comments: - mGuard FW checked OK - Checked vessel FW - K-GSN Router Actual Results: Kongsberg firewall (mGuard) and vessel's firewall were checked, and it was proved that all the firewall rules are appropriately set.		

6. Integration Test

6.1. 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 RE1)

6.1.1. 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.

6.1.2. Test Result

Step No	Task Description	Expected Result	Result
1	Check the cabling within and between zones visually to verify that zones are segmented.	Zones are well segmented	
2	Check the device's ACL or VLAN configuration; that network is well segmented, and data cannot be transferred to different zones without approval.	ACL or VLAN is relevantly set	
3	Conduct port scanning test to verify that unnecessary ports are not opened.	Unnecessary ports are not opened	
Detailed Steps	6.1.2.1. The system's physical cabling should be done appropriately. This can be checked by visual inspection. 6.1.2.2. The system's ACL or VLAN configuration should be set appropriately so that the system network is well segmented. This can be demonstrated by a ping test, or explained by KM technician. 6.1.2.3. The system should not communicate via unnecessary ports. This can be checked by port scanner's scan result.		
Comments & Actual Results			

6.2. Denial of Service(DoS) Test

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

6.2.1. 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
AMS	Router(Firewall) & K-Chief OS	100 Mbps	
BMS	CP-12	N/A	No connection via LAN

6.2.2. Test Result

Step No	Task Description	Expected Result	Result
1	Simulate a DoS attack to target device, and verify that 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**
Detailed Steps	6.2.2.1 When the KM technician connects the laptop to one of K-chief OS and generates network storm using KM IP Traffic Generator, the system should be able to detect network overload and give an alarm. Nonetheless, the system may be able to run normally. The alarm can be checked from one of the Workstation.		
Comments & Actual Results	Comments: - Storm A-net, with alarm Actual Results: Kongsberg conducted a network storming attack using their own tool. This caused the AMS to give out an alarm and caused no degradation of the system, as the network is redundantly set.		

6.2. Denial of Service(DoS) Test

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

6.2.1. 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.

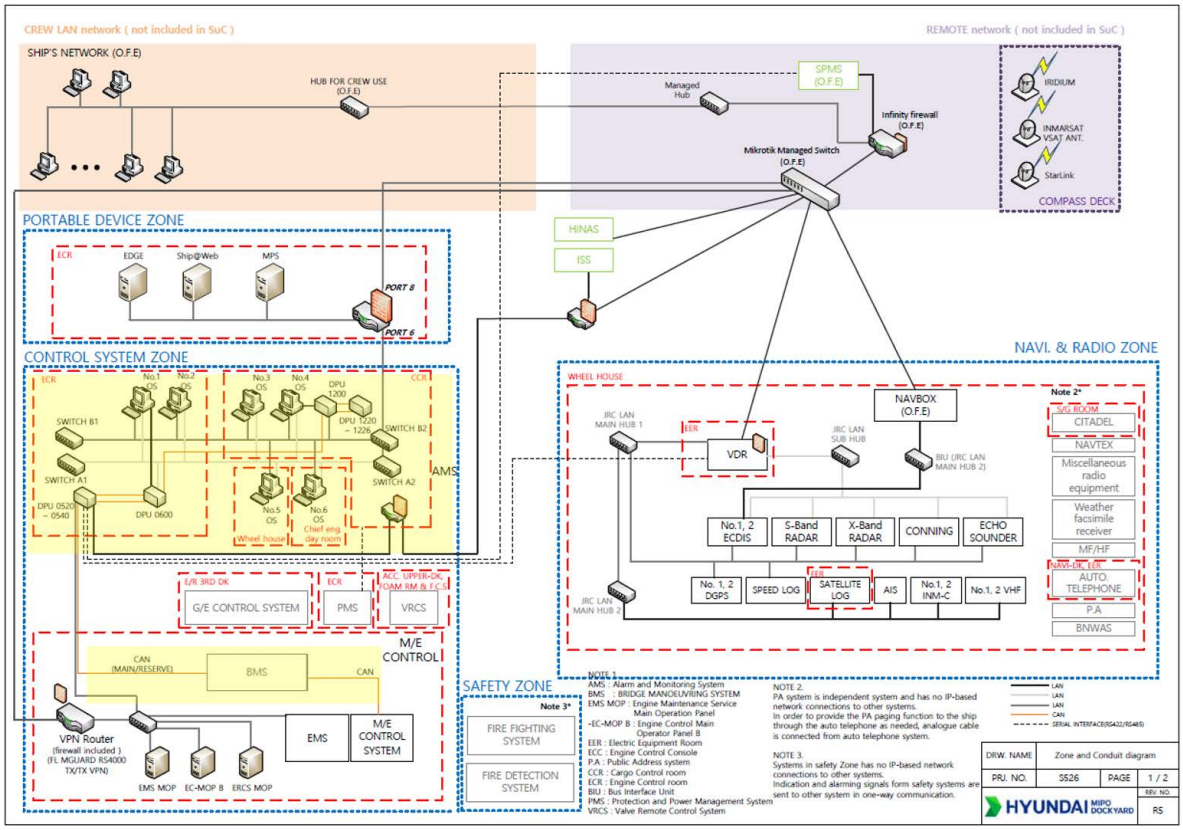
System	Target Device	Maximum Network Load	Remark
AMS	Router(Firewall) & K-Chief OS	100 Mbps	
BMS	CP-12	N/A	No connection via LAN

6.2.2. Test Result

Step No	Task Description	Expected Result	Result
1	Simulate a DoS attack to target device, and verify that 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**
Detailed Steps	6.2.2.1 When the KM technician connects the laptop to one of K-chief OS and generates network storm using KM IP Traffic Generator, the system should be able to detect network overload and give an alarm. Nonetheless, the system may be able to run normally. The alarm can be checked from one of the Workstation.		
Comments & Actual Results			

7. Appendix

7.1. Zone and Conduit Diagram

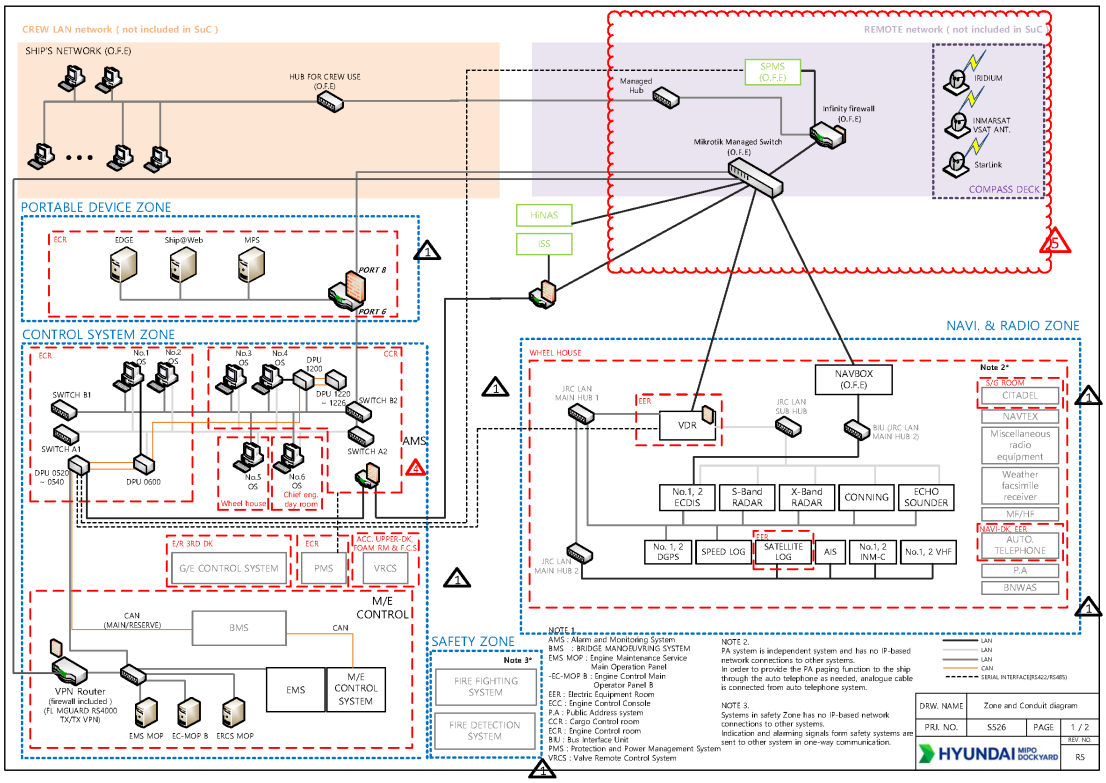


7.2. Device Information

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
1	No.1 Operator Station	Workstation	Lenovo	MC340	-	-	-	
2	No.2 Operator Station	Workstation	Lenovo	MC340	-	-	-	
3	No.3 Operator Station	Workstation	Lenovo	MC340	-	-	-	
4	No.4 Operator Station	Workstation	Lenovo	MC340	-	-	-	
5	No.5 Operator Station	Workstation	Lenovo	MC340	-	-	-	
6	No.6 Operator Station	Workstation	Lenovo	MC340	-	-	-	
7	No.7 Operator Station	Workstation	Lenovo	MC340	-	-	-	
8	No.1 OS Switch	Switch	Moxa	EDS-408A	-	-	-	

7. Appendix

7.1. Zone and Conduit Diagram



7.2. Device Information

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
1	No.1 Operator Station	Workstation	Lenovo	MC340	-	-	-	
2	No.2 Operator Station	Workstation	Lenovo	MC340	-	-	-	
3	No.3 Operator Station	Workstation	Lenovo	MC340	-	-	-	
4	No.4 Operator Station	Workstation	Lenovo	MC340	-	-	-	
5	No.5 Operator Station	Workstation	Lenovo	MC340	-	-	-	
6	No.6 Operator Station	Workstation	Lenovo	MC340				
7	No.7 Operator Station	Workstation	Lenovo	MC340				

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
9	No.2 OS Switch	Switch	Moxa	EDS-408A	-	-	-	
10	No.3 OS Switch	Switch	Moxa	EDS-408A	-	-	-	
11	No.4 OS Switch	Switch	Moxa	EDS-408A	-	-	-	
12	7" Touch Panel PC	HMI	KM	MPS	-	-	-	
13	Ship@Web Server	Servers	Lenovo	MC340	-	-	-	
14	K-GSN Router	Router	Cisco	C891-24X/K9	-	-	-	
15	Work station (W/H)	Workstation	KM	CP-12	-	-	-	
16	Work station (ECR)	Workstation	KM	CP-12	-	-	-	

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
8	No.1 OS Switch	Switch	Moxa	EDS-408A	-	-	-	
9	No.2 OS Switch	Switch	Moxa	EDS-408A	-	-	-	
10	No.3 OS Switch	Switch	Moxa	EDS-408A	-	-	-	
11	No.4 OS Switch	Switch	Moxa	EDS-408A	-	-	-	
12	7" Touch Panel PC	HMI	KM	MPS	-	-	-	
13	Ship@Web Server	Servers	Lenovo	MC340	-	-	-	
14	K-GSN Router	Router	Cisco	C891-24X/K9	-	-	-	
15	Work station (W/H)	Workstation	KM	CP-12	-	-	-	
16	Work station (ECR)	Workstation	KM	CP-12	-	-	-	

Cyber Security Test Procedure For S525s Project (115,000 DWT Class Oil/Product Tanker)

< S527 / Navi. & Comm. System >

Cyber Security Test Results For S525s Project (115,000 DWT Class Oil/Product Tanker)

< S560 / Alarm & Monitoring System & Bridge Maneuvering System>

We, the undersigned, hereby acknowledge that the survey referenced above has been conducted in accordance with the outlined procedures and standards. By signing this form, we agree that the results and findings documented in the survey report are accurate and that this document serves as an official record of the survey.

By signing this form, all parties agree that the survey has been conducted as described and that this document is an official record.

Survey Date	

Surveyor		**System Integrator**	

CONTENTS

Cyber Security Test Procedure For S525s Project (115,000 DWT Class Oil/Product Tanker)

< S560 / Navi. & Comm. System >

1. History

No.	Date (DD/MM/YYYY)	Revision	Description	Remarks
1	00/00/2024	A	First Issue	First Issue

2. Introduction

2.1. Scope

Survey Date	11/09/2024	Surveyor(s) name(s)	Simen, Vike Lande
Test Location	NaviDK, EER, A-DK		

2.2. Definitions

Owner : The entity responsible for possessing and managing the vessel

Yard : HD Hyundai Mipo (HMD), a shipyard where ships are constructed

Supplier : JRC & Navtor, companies that supply 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”

2.3. Applicable Specifications and Standards

2.3.1. Documents

Ref.	Title
4A000E020	Cyber Security Management Plan
TAA000023D	Type Approval Certificate(NavBox)
Ver.06g	Cyber Safety for JRC Equipment

2.3.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2021)
DNV-CG-0325	Cyber Secure (Edition July 2021)
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

CONTENTS

3. Background

Under the S525s 115,000 DWT Class Oil/Product Tanker Project, 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.

4. Perimeter and Approach

4.1. Perimeter

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.	SYSTEM	H/W TYPE	BRAND	MODEL	DESCRIPTION
1	Radar	HMIs	JRC	JMR-9225-6X	X-Band Radar
2	Radar	HMIs	JRC	JMR-9230-S	S-Band Radar
3	ECDIS	HMIs	JRC	JAN-9201	No.1 ECDIS
4	ECDIS	HMIs	JRC	JAN-9201	No.2 ECDIS
5	Conning	HMIs	JRC	JAN-9202	Conning Display
6	DGPS	HMIs	JRC	JLR-8600	No.1 GPS
7	DGPS	HMIs	JRC	JLR-8600	No.2 GPS
8	Speed Log	HMIs	JRC	JLN-740	Doppler Speed Log
9	Speed Log	HMIs	JRC	JLN-720	Satellite Speed Log
10	Echo Sounder	HMIs	JRC	JFE-700	Echo Sounder
11	VDR	HMIs	JRC	JCY-1900	VDR
12	VDR	Switch	Cisco	SG350-08	Switch
13	AIS	HMIs	JRC	JHS-183	AIS
14	GMDSS	HMIs	JRC	JUE-87	No.1 Inmarsat-C
15	GMDSS	HMIs	JRC	JUE-87	No.2 Inmarsat-C
16	VHF	HMIs	JRC	JHS-800	No.1 VHF
17	VHF	HMIs	JRC	JHS-800	No.2 VHF
18	VHF	HMIs	JRC	JHS-800	No.3 VHF
19	NavBox	NavBox	Navtor	NavBox	NavBox

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

NO.	BRAND	MODEL	VERSION	DESCRIPTION
1	EICAR	Anti Malware Test File	-	Malware Protection Function Check
2	Wireshark	Wireshark	4.2.XX	Packet Capture and Monitoring
3	Windows	Command Prompt	-	Ping Test
4	Famatech	Advanced Port Scanner	2.5.XX	Open Port Scan
5	DNV	NetStorm	4.0.XX	DoS Test

4.2. Approach

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

4.3. 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 as they exist at the time of the survey with the established criteria.

1. History

No.	Date (DD/MM/YYYY)	Revision	Description	Remarks
1	00/00/2025	A	First Issue	First Issue

2. Introduction

2.1. Scope

Survey Date	00/00/2025	Surveyor(s) name(s)	
Test Location	NaviDK, EER, A-DK		

2.2. Definitions

Owner : The entity responsible for possessing and managing the vessel

Yard : HD Hyundai Mipo (HMD), a shipyard where ships are constructed

Supplier : JRC & Navtor, companies that supply 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”

2.3. Applicable Specifications and Standards

2.3.1. Documents

Ref.	Title
4A000E020	Cyber Security Management Plan
TAA000023D	Type Approval Certificate(NavBox)
Ver.06g	Cyber Safety for JRC Equipment

2.3.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2021)
DNV-CG-0325	Cyber Secure (Edition July 2021)
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

5. System Test

[Sample]

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

5.1. Navigation & Communication System (JRC)

5.1.1. General Test

5.1.1.1. 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	Check that unused ports are blocked, and device connection is appropriately managed.	Any unused ports are blocked	**Pass**
2	Connect portable and/or mobile devices to the system and check the system can control device usage.	Portable and mobile device usage is controlled	**Pass**
Detailed Steps	5.1.1.1.1. All the devices' unused ports should be blocked. This can be checked by visual inspection. 5.1.1.1.2. When the user tries to connect portable and/or mobile devices to the target systems, the system should block the devices' running. This can be checked by connecting and running portable/mobile device to ECDIS and RADAR. Please note that portable/mobile devices cannot be connected to VDR.		
Comments & Actual Results	Comments: - Physical blocker Actual Results: All systems with open ports (physical) were blocked using physical port blockers. It was tested on ECDIS and RADAR that inserting a USB/mobile device did not open automatically. For VDR, the device is in its own cabinet with special key.		

3. Background

Under the S525s 115,000 DWT Class Oil/Product Tanker Project, 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.

4. Perimeter and Approach

4.1. Perimeter

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.	SYSTEM	H/W TYPE	BRAND	MODEL	DESCRIPTION
1	Radar	HMIs	JRC	JMR-9225-6X	X-Band Radar
2	Radar	HMIs	JRC	JMR-9230-S	S-Band Radar
3	ECDIS	HMIs	JRC	JAN-9201	No.1 ECDIS
4	ECDIS	HMIs	JRC	JAN-9201	No.2 ECDIS
5	Conning	HMIs	JRC	JAN-9202	Conning Display
6	DGPS	HMIs	JRC	JLR-8600	No.1 GPS
7	DGPS	HMIs	JRC	JLR-8600	No.2 GPS
8	Speed Log	HMIs	JRC	JLN-740	Doppler Speed Log
9	Speed Log	HMIs	JRC	JLN-720	Satellite Speed Log
10	Echo Sounder	HMIs	JRC	JFE-700	Echo Sounder
11	VDR	HMIs	JRC	JCY-1900	VDR
12	VDR	Switch	Cisco	SG350-08	Switch
13	AIS	HMIs	JRC	JHS-183	AIS
14	GMDSS	HMIs	JRC	JUE-87	No.1 Inmarsat-C
15	GMDSS	HMIs	JRC	JUE-87	No.2 Inmarsat-C
16	VHF	HMIs	JRC	JHS-800	No.1 VHF
17	VHF	HMIs	JRC	JHS-800	No.2 VHF
18	VHF	HMIs	JRC	JHS-800	No.3 VHF
19	NavBox	NavBox	Navtor	NavBox	NavBox

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

NO.	BRAND	MODEL	VERSION	DESCRIPTION
1	EICAR	Anti Malware Test File	-	Malware Protection Function Check
2	Wireshark	Wireshark	4.2.XX	Packet Capture and Monitoring
3	Windows	Command Prompt	-	Ping Test
4	Famatech	Advanced Port Scanner	2.5.XX	Open Port Scan
5	DNV	NetStorm	4.0.XX	DoS Test

4.2. Approach

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

4.3. 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 as they exist at the time of the survey with the established criteria.

5.1.1.2. 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	5.1.1.2.1 For ECDIS and RADAR, the event logs can be checked from 'Event List'. For VDR, its security logs can be saved and checked by connected laptop. The logs would contain timestamp, source, priority, and process information.		
Comments & Actual Results	Comments: - Windows logs - No application logs Actual Results: It was checked that ECDIS and RADAR were able to create logs on windows event viewer. It was also checked that the logs for the VDR were downloadable and included timestamps with security related logs.		

5. System Test

[Sample]

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

5.1. Navigation & Communication System (JRC)

5.1.1. General Test

5.1.1.1. 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	Check that unused ports are blocked, and device connection is appropriately managed.	Any unused ports are blocked	
2	Connect portable and/or mobile devices to the system and check the system can control device usage.	Portable and mobile device usage is controlled	
Detailed Steps	5.1.1.1.1. All the devices' unused ports should be blocked. This can be checked by visual inspection. 5.1.1.1.2. When the user tries to connect portable and/or mobile devices to the target systems, the system should block the devices' running. This can be checked by connecting and running portable/mobile device to ECDIS and RADAR. Please note that portable/mobile devices cannot be connected to VDR.		
Comments & Actual Results			

5.1.1.3. 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	Try inserting and running malicious code/program files from the system, and check that the system blocks malicious code/programs.	Malicious code/program is not running	**Pass**
Detailed Steps	5.1.1.3.1. When the user tries to connect portable and/or mobile devices containing malicious program to the target systems, the system should block the programs from running. This can be checked by connect portable/mobile device to ECDIS and RADAR. Please note that portable/mobile devices cannot be connected to VDR.		
Comments & Actual Results	Comments: - Whitelisting Actual Results: The Trend Micro antivirus was running as expected. When trying to run executables (.com file) for this vessel, Trend Micro creates a log at "Computer\Local Disk (D:)\Logs\TrendMicro SafeLock.evtx" which could be opened using windows event viewer showing that it blocked the execution of eicar files.		

5.1.1.2. 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	5.1.1.2.1 For ECDIS and RADAR, the event logs can be checked from 'Event List'. For VDR, its security logs can be saved and checked by connected laptop. The logs would contain timestamp, source, priority, and process information.		
Comments & Actual Results			

5.1.1.4. Use of Cryptography

When cryptography is required, the system shall use appropriate methods for transmit the information.

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

Step No	Task Description	Expected Result	Result
1	Check that when the system uses data cryptography, its algorithm and key are appropriately set based on best practices and recommendations.	Cryptography mechanism is appropriately set	**Pass**
Detailed Steps	5.1.1.4.1. N/A, as the system is not connected to untrusted network. Its connection is managed by Mikrotic firewall, which is in the scope of IT network.		
Comments & Actual Results	Comments: Actual Results: The VDR did not have remote access capabilities enabled and the VDR was not connected to an untrusted or a different network. It was also tested that user can access from external network only when VDR's firewall allows, which is denied by default.		

5.1.1.3. 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	Try inserting and running malicious code/program files from the system, and check that the system blocks malicious code/programs.	Malicious code/program is not running	
Detailed Steps	5.1.1.3.1. When the user tries to connect portable and/or mobile devices containing malicious program to the target systems, the system should block the programs from running. This can be checked by connect portable/mobile device to ECDIS and RADAR. Please note that portable/mobile devices cannot be connected to VDR.		
Comments & Actual Results			

5.1.1.5. 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	5.1.1.5.1 For ECDIS and RADAR, the system configuration data and backup data can be saved to USB Drive, after clicking 'Data Backup/Restore' button from task Menu. For VDR, the system configuration data only can be saved to its connected laptop by its web interface. 5.1.1.5.2. For ECDIS and RADAR, the system configuration data and backup data can be restored from saved data, after clicking 'Data Backup/Restore' button from task Menu. For VDR, the system configuration data only can be restored from saved data by its web interface.		
Comments & Actual Results	Comments: - ECDIS: Config backup - VDR: Config backup Actual Results: ECDIS has a backup functionality that saves configuration data. It was also explained that windows image backup is possible using the Windows backup procedure. The VDR has an integrated backup and restoration capability where the VDR can download and upload configuration files.		

5.1.1.4. Use of Cryptography

When cryptography is required, the system shall use appropriate methods for transmit the information.

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

Step No	Task Description	Expected Result	Result
1	Check that when the system uses data cryptography, its algorithm and key are appropriately set based on best practices and recommendations.	Cryptography mechanism is appropriately set	**N/A**
Detailed Steps	5.1.1.4.1. N/A, as the system is not connected to untrusted network. Its connection is managed by Mikrotic firewall, which is in the scope of IT network.		
Comments & Actual Results			

5.1.2. Test for Connection via Untrusted Network

Note. When the device is connected to untrusted network, following requirements shall be fulfilled.

5.1.2.1. Identification and Authentication

Human users, software processes, or devices shall be identified and authenticated for access to the system.

(Requirement(s): 4.2.2 User identification and authentication / IEC 62443-3-3 SR 1.1
4.2.3 Application or device identification and authentication / IEC-62443-3-3 SR 1.2)

Step No	Task Description	Expected Result	Result
1	Check that the system identifies and authenticates human user access based on certain processes.	The system shall monitor and control human access	**N/A**
2	Check that the system identifies and authenticates devices and software access.	The system shall monitor and control devices and software access	**N/A**
Detailed Steps	5.1.2.1.1. and 5.1.2.1.2. N/A, as the system is not connected to untrusted network, and its remote access function is disabled.		
Comments & Actual Results	Comments: - No remote Actual Results: As per DNV-RU-SHIP 2021 regulations for cyber security, test for identification and authentication is not necessary if the system is not connected to an untrusted network and has no remote access functionalities.		

5.1.1.5. 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	5.1.1.5.1 For ECDIS and RADAR, the system configuration data and backup data can be saved to USB Drive, after clicking 'Data Backup/Restore' button from task Menu. For VDR, the system configuration data only can be saved to its connected laptop by its web interface. 5.1.1.5.2. For ECDIS and RADAR, the system configuration data and backup data can be restored from saved data, after clicking 'Data Backup/Restore' button from task Menu. For VDR, the system configuration data only can be restored from saved data by its web interface.		
Comments & Actual Results			

5.1.2.2. Access via Untrusted Network

Any access from or via untrusted networks shall be monitored (e.g., logged, indicated, alarmed) and controlled (e.g., denied, restricted).

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

Step No	Task Description	Expected Result	Result
1	Check whether the system monitors and controls remote access.	The system shall monitor and control access	**N/A**
2	Check whether the system denies access requests via untrusted networks, if the request is not approved.	The system can deny unapproved access request	**N/A**
Detailed Steps	5.1.2.2.1. and 5.1.2.2.2. N/A, as the system is not connected to untrusted network, and its remote access function is disabled.		
Comments & Actual Results	Comments: - No remote Actual Results: As per DNV-RU-SHIP 2021 regulations for cyber security, test for identification and authentication is not necessary if the system is not connected to an untrusted network and has no remote access functionalities.		

5.1.2. Test for Connection via Untrusted Network

Note. When the device is connected to untrusted network, following requirements shall be fulfilled.

5.1.2.1. Identification and Authentication

Human users, software processes, or devices shall be identified and authenticated for access to the system.

(Requirement(s): 4.2.2 User identification and authentication / IEC 62443-3-3 SR 1.1
4.2.3 Application or device identification and authentication / IEC-62443-3-3 SR 1.2)

Step No	Task Description	Expected Result	Result
1	Check that the system identifies and authenticates human user access based on certain processes.	The system shall monitor and control human access	**N/A**
2	Check that the system identifies and authenticates devices and software access.	The system shall monitor and control devices and software access	**N/A**
Detailed Steps	5.1.2.1.1. and 5.1.2.1.2. N/A, as the system is not connected to untrusted network, and its remote access function is disabled.		
Comments & Actual Results			

5.1.2.3. Integrity and Confidentiality

The system shall protect the integrity of transmitted information and sessions, and the system shall be able to protect the confidentiality of information at rest or in transit that has read authorization.

(Requirement(s): 4.4.2 Communication integrity / IEC 62443-3-3 SR 3.1 RE 1
4.4.9 Session integrity / IEC-62443-3-3 SR 3.8
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 integrity.	There is an information integrity protection method	**N/A**
2	Check the system may protect the session integrity.	There is a session integrity protection method	**N/A**
3	Check the system may protect the information confidentiality.	There is an information confidentiality protection method	**N/A**
Detailed Steps	5.1.2.3.1. to 5.1.2.3.3. N/A, as the system is not connected to untrusted network, and its remote access function is disabled.		
Comments & Actual Results	Comments: - No remote Actual Results: As per DNV-RU-SHIP 2021 regulations for cyber security, test for integrity and confidentiality is not necessary if the system is not connected to an untrusted network and has no remote access functionalities.		

5.1.2.2. Access via Untrusted Network

Any access from or via untrusted networks shall be monitored (e.g., logged, indicated, alarmed) and controlled (e.g., denied, restricted).

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

Step No	Task Description	Expected Result	Result
1	Check whether the system monitors and controls remote access.	The system shall monitor and control access	**N/A**
2	Check whether the system denies access requests via untrusted networks, if the request is not approved.	The system can deny unapproved access request	**N/A**
Detailed Steps	5.1.2.2.1. and 5.1.2.2.2. N/A, as the system is not connected to untrusted network, and its remote access function is disabled.		
Comments & Actual Results			

5.2. NavBox (Navtor)

5.2.1. 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) : 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.	**Pass**
2	Check the system's configuration information to verify that the system is appropriately set.	Configuration is appropriately set.	**Fail**
Detailed Steps	5.2.1.1. The asset inventory of installed hardware and software should be identical to the Type Approval document, or its regarding information. 5.2.1.2. The system's configuration should be identical with Type Approval document, or its regarding information.		
Comments & Actual Results	Comments: - Check if Window firewall is configured correctly with vendor Actual Results: The NavBox was commissioned as shown in the type approval with windows firewall running. However, as its outgoing rules are not set during the survey, the IT engineer additionally set outgoing rules after survey. The result was delivered to the investigator and confirmed as this comment was closed.		

5.1.2.3. Integrity and Confidentiality

The system shall protect the integrity of transmitted information and sessions, and the system shall be able to protect the confidentiality of information at rest or in transit that has read authorization.

(Requirement(s): 4.4.2 Communication integrity / IEC 62443-3-3 SR 3.1 RE 1
4.4.9 Session integrity / IEC-62443-3-3 SR 3.8
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 integrity.	There is an information integrity protection method	**N/A**
2	Check the system may protect the session integrity.	There is a session integrity protection method	**N/A**
3	Check the system may protect the information confidentiality.	There is an information confidentiality protection method	**N/A**
Detailed Steps	5.1.2.3.1. to 5.1.2.3.3. N/A, as the system is not connected to untrusted network, and its remote access function is disabled.		
Comments & Actual Results			

6. Integration Test

6.1. 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 RE1)

6.1.1. 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.

6.1.2. Test Result

Step No	Task Description	Expected Result	Result
1	Check the cabling within and between zones visually to verify that zones are segmented.	Zones are well segmented	**Pass**
2	Check the device's ACL or VLAN configuration; that network is well segmented, and data cannot be transferred to different zones without approval.	ACL or VLAN is relevantly set	**Pass**
3	Conduct port scanning test to verify that unnecessary ports are not opened.	Unnecessary ports are not opened	**Pass**
Detailed Steps	6.1.2.1. The system's physical cabling should be done appropriately. This can be checked by visual inspection. 6.1.2.2. The system's ACL or VLAN configuration should be set appropriately that the system network is well segmented. This can be checked from VDR's firewall rules. Please note that VDR's only outbound traffic should be UDP, and only 6500 and 6501 ports are opened. 6.1.2.3. The system does not communicate via unnecessary ports. This can be checked by port scanner's scan result.		
Comments & Actual Results	Comments: - Scan of VDR, OK Actual Results: For VDR, it was checked that the VDR's firewall and IT network's firewall are both appropriately set. Also, the firewall was configured so that only a single PC is allowed to connect to the NavBox and only necessary ports were open to communicate with the ECDIS and VDR.		

5.2. NavBox (Navtor)

5.2.1. 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) : 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.	
2	Check the system's configuration information to verify that the system is appropriately set.	Configuration is appropriately set.	
Detailed Steps	5.2.1.1. The asset inventory of installed hardware and software should be identical to the Type Approval document, or its regarding information. 5.2.1.2. The system's configuration should be identical with Type Approval document, or its regarding information.		
Comments & Actual Results			

6.2. Denial of Service(DoS) Test

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

6.2.1. 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
Navi. & Comm.	VDR	100 Mbps	

6.2.2. Test Result

Step No	Task Description	Expected Result	Result
1	Simulate a DoS attack to a target device and verify that the system works normally as it prevents a DoS attack or detects a DoS attack and restarts automatically to be resilient to a DoS attack.	The system works normally, or restart automatically to resilient	**Pass**
Detailed Steps	6.2.2.1 After a DoS attack is generated by DNV NetStorm, even if a network overload is detected, the system may be able to run normally or in a degraded mode. Also, excess logs alarm would be generated from VDR, and this can be checked from downloaded security logs.		
Comments & Actual Results	Comments: - Function OK, but no alarm Actual Results: When performing a network storm on the VDR, VDR was able to create logs regarding excessive network load. VDR was still functional after the attack. DoS test was also conducted to ECDIS/RADAR, and it was checked that the system works well although no alarm was given.		

6. Integration Test

6.1. 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 RE1)

6.1.1. Test Prerequisite

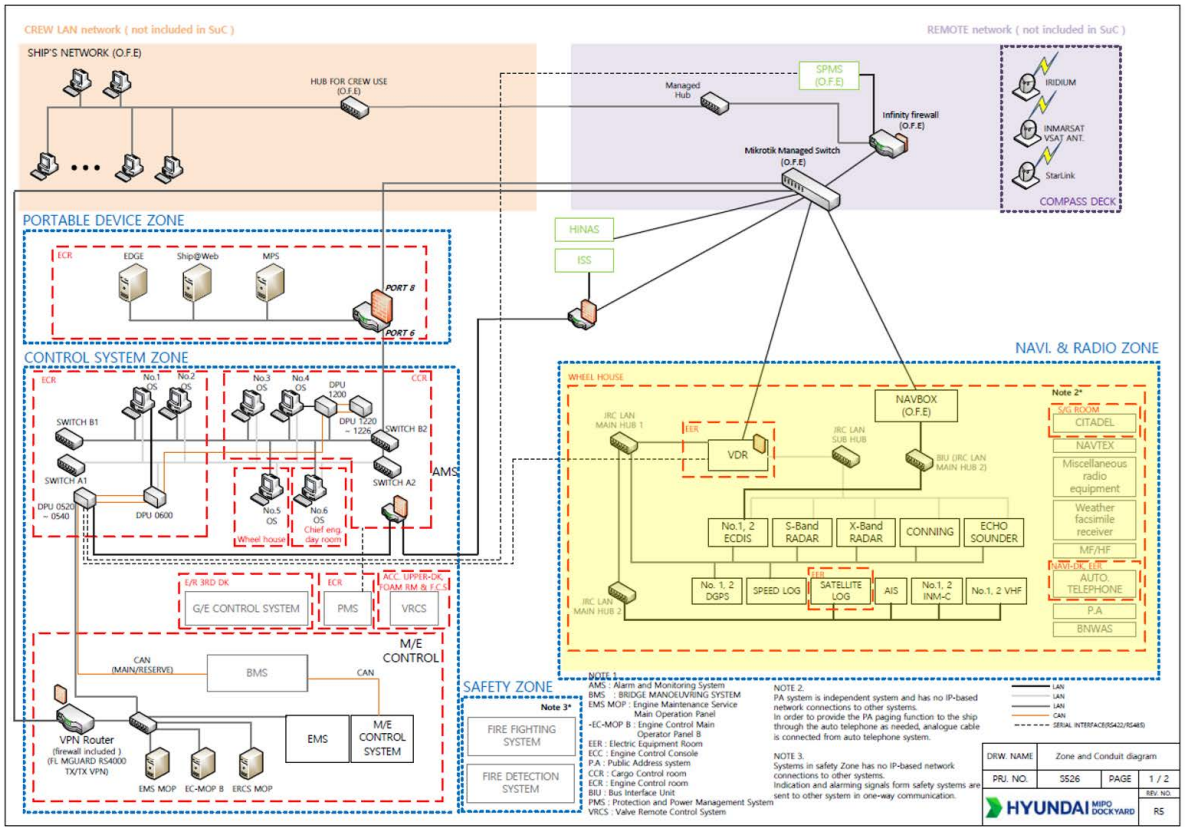
1) Different network zones must be physically or logically separated.
2) Communication between different zones should be controlled and monitored.
   Communication should be controlled based on 'deny by default, allow by exception' principle.

6.1.2. Test Result

Step No	Task Description	Expected Result	Result
1	Check the cabling within and between zones visually to verify that zones are segmented.	Zones are well segmented	
2	Check the device's ACL or VLAN configuration; that network is well segmented, and data cannot be transferred to different zones without approval.	ACL or VLAN is relevantly set	
3	Conduct port scanning test to verify that unnecessary ports are not opened.	Unnecessary ports are not opened	
Detailed Steps	6.1.2.1. The system's physical cabling should be done appropriately. This can be checked by visual inspection. 6.1.2.2. The system's ACL or VLAN configuration should be set appropriately that the system network is well segmented. This can be checked from VDR's firewall rules. Please note that VDR's only outbound traffic should be UDP, and only 6500 and 6501 ports are opened. 6.1.2.3. The system does not communicate via unnecessary ports. This can be checked by port scanner's scan result.		
Comments & Actual Results			

7. Appendix

7.1. Zone and Conduit Diagram



7.2. Device Information

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
1	X-Band Radar	HMIs	JRC	JMR-9225-6X	-	-	-	-
2	S-Band Radar	HMIs	JRC	JMR-9230-S	-	-	-	-
3	No.1 ECDIS	HMIs	JRC	JAN-9201	-	-	-	-
4	No.2 ECDIS	HMIs	JRC	JAN-9201	-	-	-	-
5	Conning Display	HMIs	JRC	JAN-9202	-	-	-	-
6	No.1 GPS	HMIs	JRC	JLR-8600	-	-	-	-
7	No.2 GPS	HMIs	JRC	JLR-8600	-	-	-	-
8	Doppler Speed Log	HMIs	JRC	JLN-740	-	-	-	-
9	Satellite Speed Log	HMIs	JRC	JLN-720	-	-	-	-
10	Echo Sounder	HMIs	JRC	JFE-700	-	-	-	-
11	VDR	HMIs	JRC	JCY-1900	-	-	-	-

6.2. Denial of Service(DoS) Test

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

6.2.1. 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
Navi. & Comm.	VDR	100 Mbps	

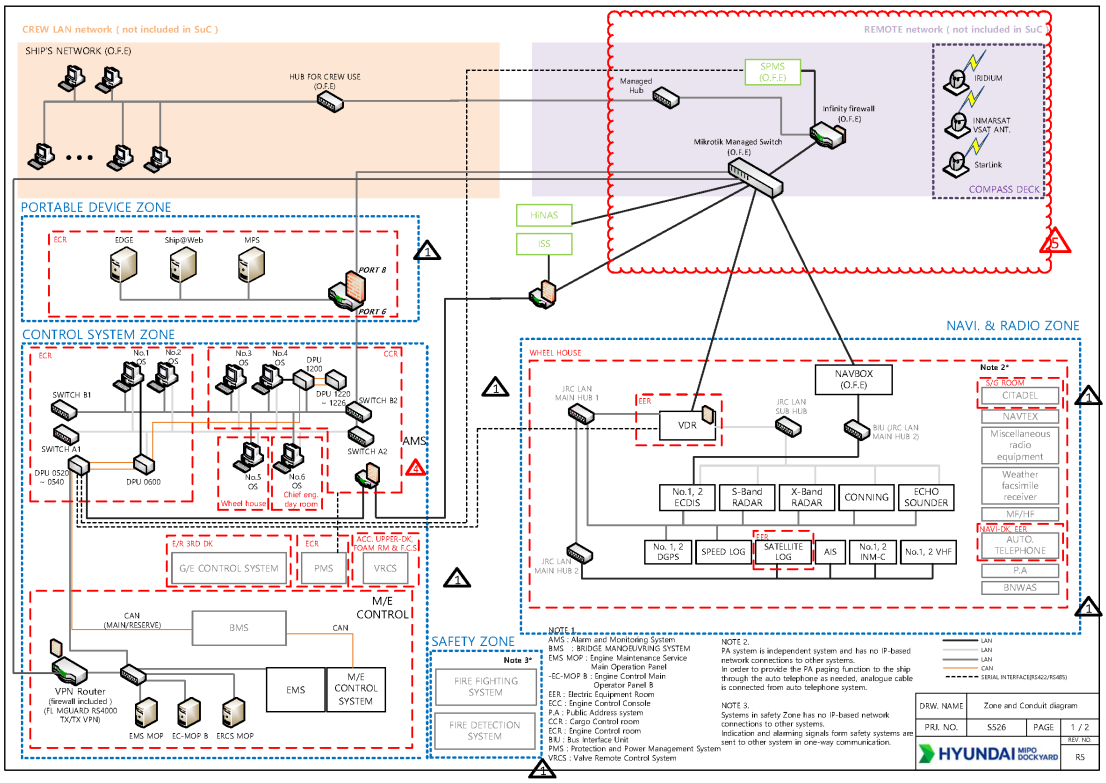
6.2.2. Test Result

Step No	Task Description	Expected Result	Result
1	Simulate a DoS attack to a target device and verify that the system works normally as it prevents a DoS attack or detects a DoS attack and restarts automatically to be resilient to a DoS attack.	The system works normally, or restart automatically to resilient	
Detailed Steps	6.2.2.1 After a DoS attack is generated by DNV NetStorm, even if a network overload is detected, the system may be able to run normally or in a degraded mode. Also, excess logs alarm would be generated from VDR, and this can be checked from downloaded security logs.		
Comments & Actual Results			

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
12	VDR Switch	Switch	Cisco	SG350-08	-	-	-	-
13	AIS	HMIs	JRC	JHS-183	-	-	-	-
14	No.1 Inmarsat-C	HMIs	JRC	JUE-87	-	-	-	-
15	No.2 Inmarsat-C	HMIs	JRC	JUE-87	-	-	-	-
16	No.1 VHF	HMIs	JRC	JHS-800	-	-	-	-
17	No.2 VHF	HMIs	JRC	JHS-800	-	-	-	-
18	No.3 VHF	HMIs	JRC	JHS-800	-	-	-	-
19	NavBox	NavBox	Navtor	NavBox	-	-	-	-

7. Appendix

7.1. Zone and Conduit Diagram



7.2. Device Information

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
1	X-Band Radar	HMIs	JRC	JMR-9225-6X	-	-	-	-
2	S-Band Radar	HMIs	JRC	JMR-9230-S	-	-	-	-
3	No.1 ECDIS	HMIs	JRC	JAN-9201	-	-	-	-
4	No.2 ECDIS	HMIs	JRC	JAN-9201	-	-	-	-
5	Conning Display	HMIs	JRC	JAN-9202	-	-	-	-
6	No.1 GPS	HMIs	JRC	JLR-8600	-	-	-	-
7	No.2 GPS	HMIs	JRC	JLR-8600	-	-	-	-
8	Doppler Speed Log	HMIs	JRC	JLN-740	-	-	-	-
9	Satellite Speed Log	HMIs	JRC	JLN-720	-	-	-	-
10	Echo Sounder	HMIs	JRC	JFE-700	-	-	-	-
11	VDR	HMIs	JRC	JCY-1900	-	-	-	-

Cyber Security Test Procedure For S525s Project (115,000 DWT Class Oil/Product Tanker)

< S527 / Fire Detection System >

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
12	VDR Switch	Switch	Cisco	SG350-08	-	-	-	-
13	AIS	HMIs	JRC	JHS-183	-	-	-	-
14	No.1 Inmarsat-C	HMIs	JRC	JUE-87	-	-	-	-
15	No.2 Inmarsat-C	HMIs	JRC	JUE-87	-	-	-	-
16	No.1 VHF	HMIs	JRC	JHS-800	-	-	-	-
17	No.2 VHF	HMIs	JRC	JHS-800	-	-	-	-
18	No.3 VHF	HMIs	JRC	JHS-800	-	-	-	-
19	NavBox	NavBox	Navtor	NavBox	-	-	-	-

CONTENTS

Cyber Security Test Procedure For S525s Project (115,000 DWT Class Oil/Product Tanker)

< S560 / Fire Detection System >

1. History

No.	Date (DD/MM/YYYY)	Revision	Description	Remarks
1	00/00/2024	A	First Issue	First Issue

2. Introduction

2.1. Scope

Survey Date	11/09/2024	Surveyor(s) name(s)	Simen, Vike Lande
Test Location	NaviDK, CCR, ECR, Foam Room		

2.2. Definitions

Owner : The entity responsible for possessing and managing the vessel

Yard : HD Hyundai Mipo (HMD), a shipyard where ships are constructed

Supplier : Consilium, a company that supply 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”

2.3. Applicable Specifications and Standards

2.3.1. Documents

Ref.	Title
4A000E020	Cyber Security Management Plan

2.3.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2021)
DNV-CG-0325	Cyber Secure (Edition July 2021)
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

CONTENTS

3. Background

Under the S525s 115,000 DWT Class Oil/Product Tanker Project, 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.

4. Perimeter and Approach

4.1. Perimeter

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.	SYSTEM	H/W TYPE	BRAND	MODEL	DESCRIPTION
1	Control Panel	PLC	Consilium	Control Panel M 4.3	Control Panel

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

NO.	BRAND	MODEL	VERSION	DESCRIPTION
1	EICAR	Anti Malware Test File	-	Malware Protection Function Check

4.2. Approach

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

4.3. 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 as they exist at the time of the survey with the established criteria.

1. History

No.	Date (DD/MM/YYYY)	Revision	Description	Remarks
1	00/00/2025	A	First Issue	First Issue

2. Introduction

2.1. Scope

Survey Date	00/00/2025	Surveyor(s) name(s)	
Test Location	NaviDK, CCR, ECR, Foam Room		

2.2. Definitions

Owner : The entity responsible for possessing and managing the vessel

Yard : HD Hyundai Mipo (HMD), a shipyard where ships are constructed

Supplier : Consilium, a company that supply 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”

2.3. Applicable Specifications and Standards

2.3.1. Documents

Ref.	Title
4A000E020	Cyber Security Management Plan

2.3.2. International Standards

Ref.	Title
DNV-RU-SHIP-Pt6Ch5.	Section 21 Cyber Security (Edition July 2021)
DNV-CG-0325	Cyber Secure (Edition July 2021)
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

5. System Test

[Sample]

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

5.1. General Test

5.1.1. 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	Check that unused ports are blocked, and device connection is appropriately managed.	Any unused ports are blocked	**Pass**
2	Connect portable and/or mobile devices to the system and check the system can control device usage.	Portable and mobile device usage is controlled	**Pass**
Detailed Steps	5.1.1.1. All the devices' unused ports should be blocked. This can be checked by visual inspection. 5.1.1.2. When the user tries to connect portable and/or mobile devices to Control Panel, the system would block the devices or programs' running. This can be checked by connecting and running files from USB stick.		
Comments & Actual Results	Comments: Actual Results: All USB ports were blocked and there were no RJ45 ports.		

3. Background

Under the S525s 115,000 DWT Class Oil/Product Tanker Project, 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.

4. Perimeter and Approach

4.1. Perimeter

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.	SYSTEM	H/W TYPE	BRAND	MODEL	DESCRIPTION
1	Control Panel	PLC	Consilium	Control Panel M 4.3	Control Panel

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

NO.	BRAND	MODEL	VERSION	DESCRIPTION
1	EICAR	Anti Malware Test File	-	Malware Protection Function Check

4.2. Approach

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

4.3. 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 as they exist at the time of the survey with the established criteria.

5.1.2. 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	5.1.2.1 The event logs and system logs can be checked from control panel, by accessing 'Service Menu' -> 'System log'. Please note that accessing the menu requires accounts with certain access level.		
Comments & Actual Results	Comments: Actual Results: The FDS main panel was able to save logs in clear text including timestamps and type of event.		

5. System Test

[Sample]

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

5.1. General Test

5.1.1. 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	Check that unused ports are blocked, and device connection is appropriately managed.	Any unused ports are blocked	
2	Connect portable and/or mobile devices to the system and check the system can control device usage.	Portable and mobile device usage is controlled	
Detailed Steps	5.1.1.1. All the devices' unused ports should be blocked. This can be checked by visual inspection. 5.1.1.2. When the user tries to connect portable and/or mobile devices to Control Panel, the system would block the devices or programs' running. This can be checked by connecting and running files from USB stick.		
Comments & Actual Results			

5.1.3. 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	Try inserting and running malicious code/program files from the system, and check that the system blocks malicious code/programs.	Malicious code/program is not running	**Pass**
Detailed Steps	5.1.3.1 When the user tries to connect portable and/or mobile devices to Control Panel, the system would block the devices or programs' running. This can be checked by connecting and running files from USB stick.		
Comments & Actual Results	Comments: Actual Results: When connecting a USB stick to the FDS panel, the FDS panel was not able to read any files in the USB. The FDS is only able to run files with specific file extensions.		

5.1.2. 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	5.1.2.1 The event logs and system logs can be checked from control panel, by accessing 'Service Menu' -> 'System log'. Please note that accessing the menu requires accounts with certain access level.		
Comments & Actual Results			

5.1.4. Use of Cryptography

When cryptography is required, the system shall use appropriate methods for transmit the information.

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

Step No	Task Description	Expected Result	Result
1	Check that when the system uses data cryptography, its algorithm and key are appropriately set based on best practices and recommendations.	Cryptography mechanism is appropriately set	**N/A**
Detailed Steps	5.1.4.1. N/A, The system communicates with other devices via CAN cables, and thus it does not use cryptography.		
Comments & Actual Results	Comments: Actual Results: The system communicates entirely by CAN communication; therefore, this test was not needed.		

5.1.3. 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	Try inserting and running malicious code/program files from the system, and check that the system blocks malicious code/programs.	Malicious code/program is not running	
Detailed Steps	5.1.3.1 When the user tries to connect portable and/or mobile devices to Control Panel, the system would block the devices or programs' running. This can be checked by connecting and running files from USB stick.		
Comments & Actual Results			

5.1.5. 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	5.1.5.1 The system data can be backed up from control panel, by accessing 'Service Menu' -> 'Configure'. Please note that accessing the menu requires accounts with certain access level. 5.1.5.2. The system data can be restored from control panel, using backup data from 5.1.5.1. Please note that accessing the menu requires accounts with certain access level, and system reboot.		
Comments & Actual Results	Comments: Actual Results: The FDS has a procedure where they can back up configuration, BIOS and firmware data which can then be restored using the same file.		

5.1.4. Use of Cryptography

When cryptography is required, the system shall use appropriate methods for transmit the information.

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

Step No	Task Description	Expected Result	Result
1	Check that when the system uses data cryptography, its algorithm and key are appropriately set based on best practices and recommendations.	Cryptography mechanism is appropriately set	**N/A**
Detailed Steps	5.1.4.1. N/A, The system communicates with other devices via CAN cables, and thus it does not use cryptography.		
Comments & Actual Results			

6. Integration Test

6.1. 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 RE1)

6.1.1. 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.

6.1.2. Test Result

Step No	Task Description	Expected Result	Result
1	Check the cabling within and between zones visually to verify that zones are segmented.	Zones are well segmented	**Pass**
2	Check the device's ACL or VLAN configuration; that network is well segmented, and data cannot be transferred to different zones without approval.	ACL or VLAN is relevantly set	**N/A**
3	Conduct port scanning test to verify that unnecessary ports are not opened.	Unnecessary ports are not opened	**N/A**
Detailed Steps	6.1.2.1. The system's physical cabling should be done appropriately. This can be checked by visual inspection. 6.1.2.2. N/A, The system' communicates using CAN network, and thus it does not have ACL/VLAN configuration. 6.1.2.3. N/A, The system communicates using CAN network, and thus port scanning is not applicable.		
Comments & Actual Results	Comments: Actual Results: Visual inspections were conducted on every panel and repeaters in the FDS. As the FDS does not have any IP communications, ACL and VLAN configurations and open ports were not checked.		

5.1.5. 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	5.1.5.1 The system data can be backed up from control panel, by accessing 'Service Menu' -> 'Configure'. Please note that accessing the menu requires accounts with certain access level. 5.1.5.2. The system data can be restored from control panel, using backup data from 5.1.5.1. Please note that accessing the menu requires accounts with certain access level, and system reboot.		
Comments & Actual Results			

6.2. Denial of Service(DoS) Test

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

6.2.1. 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
FDS	Control Panel M 4.3	N/A	No connection via LAN

6.2.2. Test Result

Step No	Task Description	Expected Result	Result
1	Simulate a DoS attack to a target device and verify that the system works normally as it prevents a DoS attack or detects a DoS attack and restarts automatically to be resilient to a DoS attack.	The system works normally, or restart automatically to resilient	**N/A**
Detailed Steps	6.2.2.1 N/A, The system communicates using CAN network, and thus DoS test is not applicable.		
Comments & Actual Results	Comments: Actual Results: The FDS does not use any protocols other than CAN communication, therefore, a DoS test was not conducted.		

6. Integration Test

6.1. 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 RE1)

6.1.1. Test Prerequisite

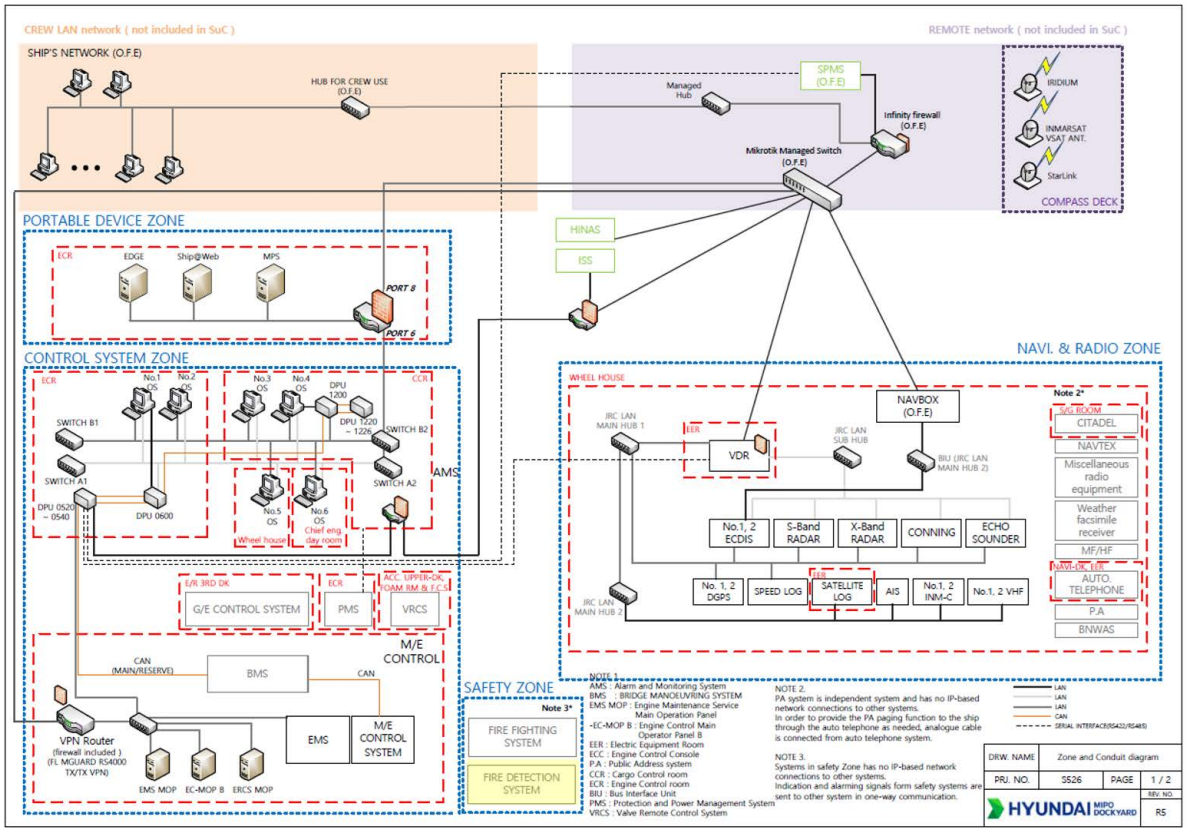
1) Different network zones must be physically or logically separated.
2) Communication between different zones should be controlled and monitored.
   Communication should be controlled based on 'deny by default, allow by exception' principle.

6.1.2. Test Result

Step No	Task Description	Expected Result	Result
1	Check the cabling within and between zones visually to verify that zones are segmented.	Zones are well segmented	
2	Check the device's ACL or VLAN configuration; that network is well segmented, and data cannot be transferred to different zones without approval.	ACL or VLAN is relevantly set	**N/A**
3	Conduct port scanning test to verify that unnecessary ports are not opened.	Unnecessary ports are not opened	**N/A**
Detailed Steps	6.1.2.1. The system's physical cabling should be done appropriately. This can be checked by visual inspection. 6.1.2.2. N/A, The system' communicates using CAN network, and thus it does not have ACL/VLAN configuration. 6.1.2.3. N/A, The system communicates using CAN network, and thus port scanning is not applicable.		
Comments & Actual Results			

7. Appendix

7.1. Zone and Conduit Diagram



7.2. Device Information

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
1	Control Panel	PLC	Consilium	Control Panel M 4.3	-	-	-	-

6.2. Denial of Service(DoS) Test

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

6.2.1. 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.

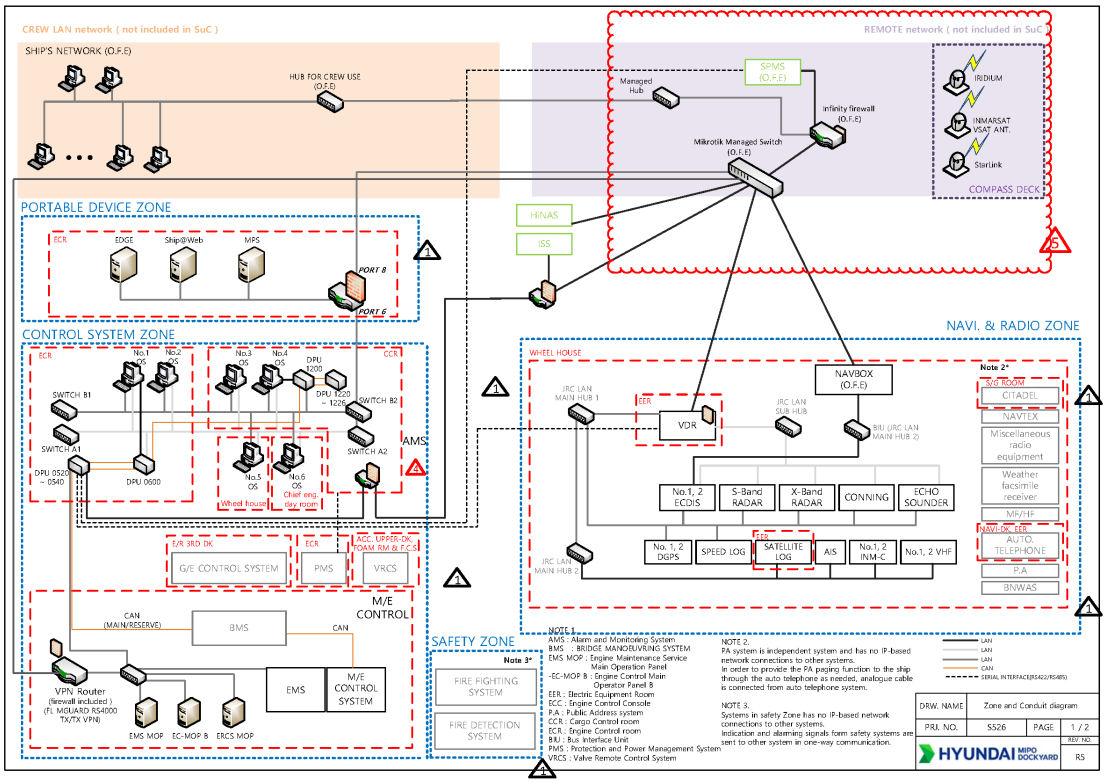
System	Target Device	Maximum Network Load	Remark
FDS	Control Panel M 4.3	N/A	No connection via LAN

6.2.2. Test Result

Step No	Task Description	Expected Result	Result
1	Simulate a DoS attack to a target device and verify that the system works normally as it prevents a DoS attack or detects a DoS attack and restarts automatically to be resilient to a DoS attack.	The system works normally, or restart automatically to resilient	**N/A**
Detailed Steps	6.2.2.1 N/A, The system communicates using CAN network, and thus DoS test is not applicable.		
Comments & Actual Results			

7. Appendix

7.1. Zone and Conduit Diagram



7.2. Device Information

No.	Device Name	Hardware Type	Brand	Model	IP Address	ID & Password		Remark
						ID	Password	
1	Control Panel	PLC	Consilium	Control Panel M 4.3	-	-	-	-