Maritime Cyber Vulnerability Review Report

Project Acronym:	CyberSEA
Full Title:	CyberSEA - Increasing Cyber Security at SEA through digital training
Project no.:	2023-1-ES01-KA220-VET-000159793
File Ref:	WP2.T1.- Identification of cyber vulnerabilities at sea
Version:	0.1
Status:	Final
Start date of the project:	01.09.2023 ***Duration:*** 36 months

Funding body: Co-funded by the European Union

Partners' logo:

Co-funded by the European Union

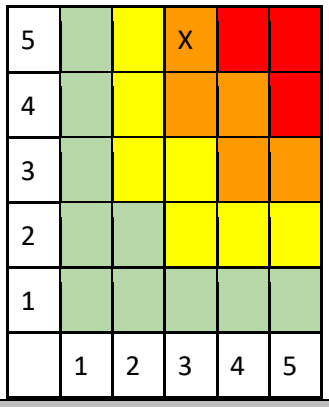
The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.

List of Output Contributors

No.	Participant Organisation Name	Participant Short Name	Country
1	UNIVERSITAT POLITECNICA DE CATALUNYA	UPC	ES
2	AINTEK SYMVOULOI EPICHEIRISEON EFARMOGES YPSILIS TECHNOLOGIAS EKPAIDEFSI ANONYMI ETAIREIA	IDEC	GR
3	SPINAKER, navticno izobrazevanje in trgovina, d.o.o.	SPINAKER	SI
4	Academia Navala "Mircea cel Batran"	RNA	RO
5	Berlin School of Business and Innovation GmbH	BSBI	DE
6	Centre for Factories of the Future	C4FF	SE
7	POLITECHNIKA MORSKA W SZCZECINIE PM	MUS	PL
8	ELLINIKO MESOGEIAKO PANEPISTIMIO	HMU	GR
9	SATAKUNNAN AMMATTIKORKEAKOULU OY	SAMK	FI

Contents

1. Cargo Management Systems

Identified hazard 1.	
Permanent/temporary loss of data with financial impact and damage to reputation	
Identified risk	
Ransomware attack that prevents access to the CMS	
Risk assessment	
Likelihood	3
Impact	5
Risk rating	Risk Matrix (Likelihood x Impact) Risk Score 1-5 = Low Risk Risk Score 6-10 = Medium Risk Risk Score 11-19 = High Risk Risk Score 20-25 = Extreme Risk 
Mitigation strategies	
Technical measures	**Security policy:** Implement security policy on used system (IT-network, computers /OT – Cargo Control Room) – control access (user/password), block and monitor ports (USB ports etc.) **Antivirus:** Use licensed and updated software to protect IT/OT system from ransomware and malware attack
Procedural measures (Training and awareness, etc.)	**Regular Training:** In the training programs, the crew is warned about cybersecurity threats, including ransomware. Learn through examples about the methods of recognizing malicious code attempting to pass as regular business documents or regular software. Train the crew to identify and respond to abnormal Cargo Management systems behaviour.
Supply chain management	**Secure Hardware Procurement:** Ensure that cargo management systems are sourced from reputable manufacturers with focus on security. Validate the

	security features of the hardware and firmware to minimize the risk of vulnerabilities. **Firmware and Software Updates:** Establish a systematic approach to regularly update and patch cargo management systems firmware and software to address known vulnerabilities and enhance security features.

Conclusion - Residual Risk Calculation

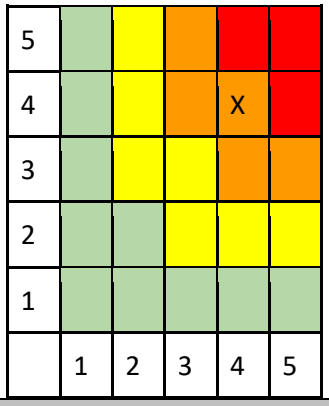
Residual Risk = Initial Risk – Risk Mitigation Effectiveness
Initial Risk Assessment
Likelihood = 3
Impact = 5
Initial Risk = 3 x 5 = 15
Risk Mitigation Effectiveness is a subjective measure based on the effectiveness of the mitigation measures implemented. For this risk we can assume the rating of 80%.

Residual Risk = 15 – (15* 0.8) = 15 – 12 = **3**

This means that, after implementing the specified mitigation measures with a 80% effectiveness, the remaining risk associated with the spoofing of Cargo Management Systems is reduced to a residual risk level of 3. Continuous monitoring and reassessment of the risk landscape will be crucial to adjust mitigation strategies as needed.

References

https://www.hstoday.us/subject-matter-areas/maritime-security/cyber-risk-management-maritime-transportation-system/
https://www.researchgate.net/publication/362483966_Guidelines_for_cyber_risk_management_in_shipboard_operational_technology_systems

Identified hazard 2.	
Remote manipulation of the cargo manifest, financial impact, damage to reputation	
Identified risk	
Malware attack that affects the proper functionality of the CMS	
Risk assessment	
Likelihood	4
Impact	4
Risk rating	Risk Matrix (Likelihood x Impact) Risk Score 1-5 = Low Risk Risk Score 6-10 = Medium Risk Risk Score 11-19 = High Risk Risk Score 20-25 = Extreme Risk 
Mitigation strategies	
Technical measures	**Security policy:** Implement security policy on used system (IT-network, computers /OT – Cargo Control Room) – control access (user/password), block and monitor ports (USB ports etc.) **Antivirus:** Use licensed and updated software to protect IT/OT system from ransomware and malware attack
Procedural measures (Training and awareness, etc.)	**Regular Training:** In the training programs, the crew is warned about cybersecurity threats, including malware software disguised as regular software. Learn through examples about the company approved methods of obtaining/installing/updating regular software. Train the crew to identify and respond to abnormal Cargo Management systems behaviour.
Supply chain management	**Secure Hardware Procurement:** Ensure that cargo management systems are sourced from reputable manufacturers with focus on security. Validate the security features of the hardware and firmware to minimize the risk of vulnerabilities. **Firmware and Software Updates:** Establish a systematic approach to regularly update and patch cargo management systems firmware and software to address known vulnerabilities and enhance security features.

Conclusion - Residual Risk Calculation

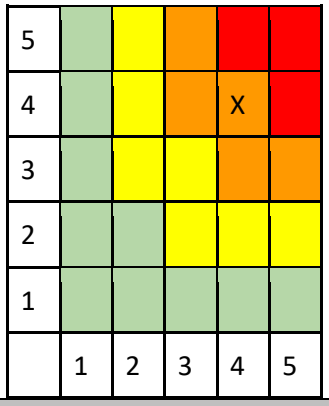
Residual Risk = Initial Risk – Risk Mitigation Effectiveness
Initial Risk Assessment
Likelihood = 4
Impact = 4
Initial Risk = 4 x 4 = 16
Risk Mitigation Effectiveness is a subjective measure based on the effectiveness of the mitigation measures implemented. For this risk we can assume the rating of 80%.

Residual Risk = 16 – (16* 0.8) = 16 – 12.8 = **3.2**

This means that, after implementing the specified mitigation measures with a 80% effectiveness, the remaining risk associated with the spoofing of Cargo Management Systems is reduced to a residual risk level of 3.2. Continuous monitoring and reassessment of the risk landscape will be crucial to adjust mitigation strategies as needed.

References

https://www.hstoday.us/subject-matter-areas/maritime-security/cyber-risk-management-maritime-transportation-system/
https://www.researchgate.net/publication/362483966_Guidelines_for_cyber_risk_management_in_shipboard_operational_technology_systems

Identified hazard 3.	
Unauthorized access to restricted systems with financial impact and damage to reputation	
Identified risk	
Phishing emails that disclose confidential information and/or credentials	
Risk assessment	
Likelihood	4
Impact	4
Risk rating	Risk Matrix (Likelihood x Impact) Risk Score 1-5 = Low Risk Risk Score 6-10 = Medium Risk Risk Score 11-19 = High Risk Risk Score 20-25 = Extreme Risk 
Mitigation strategies	
Technical measures	**Security policy:** Implement security policy on used system (IT-network, computers /OT – Cargo Control Room) – control access (user/password), block and monitor ports (USB ports etc.) **Antivirus:** Use licensed and updated software to protect IT/OT system from ransomware and malware attack
Procedural measures (Training and awareness, etc.)	**Regular Training:** In the training programs, the crew is warned about phishing threats. Learn about the methods of recognizing phishing attack attempts through examples Train the crew to identify and respond to abnormal Cargo Management systems behaviour
Supply chain management	**Secure Hardware Procurement:** Ensure that cargo management systems are sourced from reputable manufacturers with focus on security. Validate the security features of the hardware and firmware to minimize the risk of vulnerabilities. **Firmware and Software Updates:** Establish a systematic approach to regularly update and patch cargo management systems firmware and software to address known vulnerabilities and enhance security features.

Conclusion - Residual Risk Calculation
Residual Risk = Initial Risk – Risk Mitigation Effectiveness Initial Risk Assessment Likelihood = 4 Impact = 4 Initial Risk = 4 x 4 = 16 Risk Mitigation Effectiveness is a subjective measure based on the effectiveness of the mitigation measures implemented. For this risk we can assume the rating of 80%. **Residual Risk** = 16 – (16* 0.8) = 16 – 12.8 = **3.2** This means that, after implementing the specified mitigation measures with a 80% effectiveness, the remaining risk associated with the spoofing of Cargo Management Systems is reduced to a residual risk level of 3.2. Continuous monitoring and reassessment of the risk landscape will be crucial to adjust mitigation strategies as needed.
References
https://www.hstoday.us/subject-matter-areas/maritime-security/cyber-risk-management-maritime-transportation-system/ https://www.researchgate.net/publication/362483966_Guidelines_for_cyber_risk_management_in_shipboard_operational_technology_systems

2. Communication Networks

Identified hazard 1.
Interception and Eavesdropping on SATCOM, SATCOM Jamming and Spoofing, AIS Spoofing and Data Manipulation, RF Communication Interference, Unauthorized Access to RF Channels, IoT Device Compromise, Crew Personal Device Malware, Social Engineering and Phishing, OT System Vulnerabilities
Identified risk
Data breach, Loss of communication, navigational errors, False vessel identities, increased collision risk, Communication failure, Data manipulation, Botnet infiltration, Network infection, Credential theft, System control takeover
Risk assessment

Initial risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	**16**	20
FREQUENT 5	5	10	15	20	25

Initial result: 16 (4 - Likelihood: Possible, 4 - Consequences: Major)

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. Implement end-to-end encryption for SATCOM and AIS communications.
2. Use secure communication protocols such as TLS/SSL for data transmission.
3. Enhance authentication mechanisms with MFA for accessing communication systems.

<table>
<tr><td></td><td>4. Employ firewalls and IDS/IPS to monitor and control network traffic.
5. Regularly update and patch all systems and software.
6. Use strong passwords and change them regularly.</td></tr>
<tr><td>Procedural measures (Training, awareness)</td><td>1. Conduct regular cybersecurity training for crew members.
2. Implement phishing awareness programs to help crew recognize and report phishing attempts.
3. Establish protocols for the safe use of personal devices onboard.
4. Regularly conduct cybersecurity drills and exercises.</td></tr>
<tr><td>Supply chain management</td><td>1. Limit access to critical communication systems during port calls.
2. Vet suppliers and service providers for their cybersecurity practices.
3. Implement strict access controls for maintenance and support personnel.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><th rowspan="2">LIKELYHOOD</th><th colspan="5">CONSEQUENCES</th></tr>
<tr><th>INSIGNIFICANT
1</th><th>MINOR
2</th><th>MEDIUM
3</th><th>MAJOR
4</th><th>CATASTROPHIC
5</th></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 6 (2 - Likelihood: Unlikely, 3 - Consequences: Medium)</td></tr>
</table>

References

1. Polestar Global: What is Spoofing - Your Complete Guide
2. CISA Insights: GPS Interference
3. IEEE Spectrum: Tracking GPS Interference

3. Integrated Bridge Systems

Identified hazard 1.	
Collision, grounding, schedule impact, financial impact, damage to reputation	
Identified risk	
Malicious software attack	
Risk assessment	
Initial risk	

LIKELIHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	**16**	20
FREQUENT 5	5	10	15	20	25

Initial result: 16

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions	
Technical measures	1. External service providers must have strict cybersecurity protocols. 2. Remote access to integrated systems should not be preferred. 3. Physical access to the equipment should be limited. 4. Maintain dual-redundancy of the system. 5. Use MFA and strong password protocol for access to security information. 6. Maintain effective anti-virus protection on computers.

Procedural measures (Training, awareness)	1. Train personnel to interact with external service providers. 2. Do not connect non-dedicated USB- devices to any bridge equipment. 3. Comply with the cybersecurity protocols provided. 4. Conduct a cyber security assessment.
Supply chain management	1. During port calls limit access to the navigation area.
Residual risk	

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	**4**	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Residual result: 4

References

https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-cyber-threat-against-marine-aid-to-navigation-.pdf
https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/

Identified hazard 2.

Schedule impact, financial impact, damage to reputation

Identified risk

Use of remote maintenance service

Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 12

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. External service providers must have strict cybersecurity protocols.
2. Remote access to integrated systems should not be preferred.
3. Prioritize physical visits of maintenance personnel.
4. Use MFA and strong password protocol for access to security information.
5. Maintain effective anti-virus protection on computers.

Procedural measures (Training, awareness)

1. Train personnel to interact with external service providers.
2. Comply with the cybersecurity protocols provided.
3. Conduct a cyber security assessment.

Supply chain management	1. During port calls limit access to the navigation area. 2. Do not pass on admin rights to systems. 3. Do not pass on passwords to the systems.
Residual risk	

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	**3**	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Residual result: 3

References

https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-cyber-threat-against-marine-aid-to-navigation-.pdf
https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/

Identified hazard 3.
Schedule impact, financial impact, damage to reputation
Identified risk
Leakage of ISPS information
Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	**15**
POSSIBLE 4	4	8	*12*	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 15

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions	
Technical measures	1. Restrict access to spaces where the security information is held. 2. Restrict personnel access to security information. 3. Do not share security related information online.
Procedural measures (Training, awareness)	1. Use MFA and strong password protocol for access to security information. 2. Comply with the cybersecurity protocols provided. 3. Do not pass on admin rights to computers. 4. Maintain effective anti-virus protection on computers. 5. Conduct a cyber security assessment.
Supply chain management	1. During port calls limit access to the sensitive areas. 2. Control visitor access to vessel and find out who they are. 3. Do not allow visitors to roam in the vessel unaccompanied.

	4. Do not pass on admin rights to systems. 5. Do not pass on passwords to the systems.
Residual risk	

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	**4**	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Residual result: 4

References

https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/ism-guidance.html
https://portalcip.org/wp-content/uploads/2019/08/C05-Cyber-Security-Assessment.pdf

4. Navigation Systems

Identified hazard 1.
Loss of position, collision, grounding, schedule impact
Identified risk
GPS positioning disturbance
Risk assessment

Initial risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	**16**	20
FREQUENT 5	5	10	15	20	25

Initial result: 16

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. Have multiple GSP receivers in use and have them all connected to different satellites for positioning.
2. Have multiple GSP receivers in use and have them all connected to different satellites for differential correction.
3. Maintain terrestrial navigation principals and use radar for fixes when navigating in congested waters such as in archipelagos.
4. Physical access to the equipment should be limited.
5. Use MFA and strong password protocol for access to security information.

<table>
<tr><td></td><td>6. Maintain effective anti-virus protection on computers.</td></tr>
<tr><td>Procedural measures (Training, awareness)</td><td>1. Compare the positions between GPS receivers and have this included to the voyage planning.
2. Train regularly the correct action in case of a GPS signal failure.
3. Train regularly the detection of a GPS position disturbance.
4. Comply with the cybersecurity protocols provided.</td></tr>
<tr><td>Supply chain management</td><td>1. During port calls limit access to the navigation area.
2. During port calls limit access to the area where the GPS aerials are installed.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><td rowspan="2">LIKELYHOOD</td><td colspan="5">CONSEQUENCES</td></tr>
<tr><td>INSIGNIFICANT
1</td><td>MINOR
2</td><td>MEDIUM
3</td><td>MAJOR
4</td><td>CATASTROPHIC
5</td></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 4</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">https://www.cisa.gov/sites/default/files/2023-02/CISA-Insights_GPS-Interference_508.pdf
https://spectrum.ieee.org/the-networks-that-aim-to-track-gps-interference-around-the-world</td></tr>
</table>

Identified hazard 2.

Collision, grounding, schedule impact

Identified risk

AIS spoofing

Risk assessment

Initial risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	**12**	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 12

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. Maintain terrestrial navigation principals and use radar for determining position to other vessels when navigating in congested waters such as in archipelagos.
2. Avoid over reliance to the AIS information.
3. When possible use radar overlay on ECDIS.
4. Physical access to the equipment should be limited.
5. Use MFA and strong password protocol for access to security information.
6. Maintain effective anti-virus protection on computers.

Procedural measures (Training, awareness)

1. Inform other vessel of their false position information broadcasted through AIS.
2. Train regularly the correct action in case of AIS spoofing.
3. Train regularly the detection of AIS spoofing.

	4. Comply with the cybersecurity protocols provided. 5. Conduct a cyber security assessment.
Supply chain management	1. During port calls limit access to the navigation area. 2. During port calls limit access to the area where the GPS aerials are installed.
Residual risk	

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	**4**	8	12	16	20
FREQUENT 5	5	10	15	20	25

Residual result: 4

References

https://www.polestarglobal.com/resources/what-is-spoofing-your-complete-guide-4-key-ais-spoofing-typologies
https://www.cisa.gov/sites/default/files/2023-02/CISA-Insights_GPS-Interference_508.pdf
https://spectrum.ieee.org/the-networks-that-aim-to-track-gps-interference-around-the-world

Identified hazard 3.

Collision, grounding, schedule impact

Identified risk

ECDIS malicious software

Risk assessment

Initial risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	**9**	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 9

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. Maintain terrestrial navigation principals and use radar for determining position to other vessels when navigating in congested waters such as in archipelagos.
2. Use chart providers that use CD's and secure protocols for updates.
3. When possible use radar overlay on ECDIS.
4. Maintain dual-redundancy of the system.
5. Compare the information between the ECDIS units.
6. Physical access to the equipment should be limited.
7. Use MFA and strong password protocol for access to security information.
8. Maintain effective anti-virus protection on computers.

<table>
<tr><td>Procedural measures (Training, awareness)</td><td>1. Do not connect ECDIS to internet even for updates of chart cells.
2. Do not connect non-dedicated USB- devices to ECDIS-computer.
3. Train personnel to conduct ECDIS updates securely.
4. Comply with the cybersecurity protocols provided.
5. Conduct a cyber security assessment.</td></tr>
<tr><td>Supply chain management</td><td>1. During port calls limit access to the navigation area.
2. Always limit access to the ECDIS computers and graphical user interfaces.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><td rowspan="2">LIKELYHOOD</td><td colspan="5">CONSEQUENCES</td></tr>
<tr><td>INSIGNIFICANT
1</td><td>MINOR
2</td><td>MEDIUM
3</td><td>MAJOR
4</td><td>CATASTROPHIC
5</td></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 3</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/the-cyber-threat-against-marine-aid-to-navigation-.pdf
https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/</td></tr>
</table>

5. Onboard Entertainment Systems

Identified hazard 1.
Unusable onboard entertainment system due to its extremely slow performance -> passengers unsatisfaction. Almost unable communication between other systems (navigation, weather monitoring etc.) -> ship safety.
Identified risk
Distributed Denial of Service (DDoS) attack through passenger public network
Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	**12**	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 12

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions	
Technical measures	1. 100% isolation of passenger public network (internet access through wifi) from any safety critical system on board, even onboard entertainment system.
Procedural measures (Training, awareness)	

Supply chain management	
Residual risk	

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	**1**	2	**3**	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Residual result: 3

References

https://www.nepia.com/the-guidelines-on-cybersecurity-on-board-ships
https://www.hattelandtechnology.com/blog/cyber-security-vulnerabilities-on-board-ships

Identified hazard 2.

Steel of passengers data stored within onboard entertainment system. Taking control of onboard entertainment system which may be misused to take a ship into panic situation among passengers and also crew.

Identified risk

Man-in-the-Middle Attack at onboard entertainment system

Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 12

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. Limit access to onboard entertainment system to MAC addresses of all known connected access-points only. That means passengers are not able to access onboard entertainment system with their mobiles/computers but only with allocated TV/remote control/similar in their rooms.
2. All communication (data exchange) within onboard entertainment system should be encrypted.
3. Strong and unique credentials for any TV/remote control/similar to connect to onboard entertainment system should be used.
4. Make available only essential information about passengers at onboard entertainment system (e.g. name,

<table>
<tr><td></td><td>surname, room nr.; but not address, credit card info etc. from Passenger and Crew Management Systems as you don’t need them at all).
5. Disable Root SSH Logins.</td></tr>
<tr><td>Procedural measures (Training, awareness)</td><td>1. People who maintain onboard entertainment system should be aware of cyber threats.
2. Comply with the cybersecurity protocols provided.
3. Conduct a cyber security assessment.</td></tr>
<tr><td>Supply chain management</td><td>1. Limit access to the area where onboard entertainment system is controlled.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><td rowspan="2">LIKELYHOOD</td><td colspan="5">CONSEQUENCES</td></tr>
<tr><td>INSIGNIFICANT
1</td><td>MINOR
2</td><td>MEDIUM
3</td><td>MAJOR
4</td><td>CATASTROPHIC
5</td></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 3</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">https://www.fool.com/the-ascent/small-business/endpoint-security/articles/mitm/</td></tr>
</table>

Identified hazard 3.

Steel of passengers data stored within onboard entertainment system. Taking control of onboard entertainment system which may be misused to take a ship into panic situation among passengers and also crew.

Identified risk

Brute Force Attack to onboard entertainment system

Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 12

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. Limit access to onboard entertainment system to MAC addresses of all known connected access-points only. That means passengers are not able to access onboard entertainment system with their mobiles/computers but only with allocated TV/remote control/similar in their rooms.
2. Strong and unique credentials for any TV/remote control/similar to connect to onboard entertainment system should be used.
3. Make available only essential information about passengers at onboard entertainment system (e.g. name, surname, room nr.; but not address, credit card info etc.

<table>
<tr><td></td><td>from Passenger and Crew Management Systems as you don’t need them at all).
4. Disable Root SSH Logins.
5. Limit login attempts.</td></tr>
<tr><td>Procedural measures (Training, awareness)</td><td>1. People who maintain onboard entertainment system should be aware of cyber threats.
2. Monitor multiple login attempts to onboard entertainment system which never happen in normal situation. Setting up an automatic alert is even better option.
3. Comply with the cybersecurity protocols provided.
4. Conduct a cyber security assessment.</td></tr>
<tr><td>Supply chain management</td><td>1. Limit access to the area where onboard entertainment system is controlled.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><td rowspan="2">LIKELYHOOD</td><td colspan="5">CONSEQUENCES</td></tr>
<tr><td>INSIGNIFICANT
1</td><td>MINOR
2</td><td>MEDIUM
3</td><td>MAJOR
4</td><td>CATASTROPHIC
5</td></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 3
</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks</td></tr>
</table>

6. Passenger and Crew Management Systems

Identified hazard 1.

Unauthorized access to sensitive data and potential manipulation of system databases, leading to data integrity loss and operational disruptions.

Identified risk

SQL injection on passenger and crew management systems

Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	**4**	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 4

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:

https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

<table>
<tr><td>Technical measures</td><td>1. Prepared Statements: Use prepared statements with parameterized queries. This means you clearly distinguish between the SQL code and the data passed through it.
2. Validate Sanitize Input Data: Ensure that the application validates input data for type, length, format, and range.
3. Sanitize Input Data: Remove or replace characters in the input that are not required for its intended purpose, or adding an escape character before potentially dangerous characters in the input data.
4. Implement Application Firewalls: Database firewalls are security solutions designed to monitor, control, and protect database traffic from unauthorized access, SQL injection attacks, and other malicious activities.</td></tr>
<tr><td>Procedural measures (Training, awareness)</td><td>Conduct Regular Security Awareness Training for IT crew: Hold frequent training sessions focused on the importance of secure coding practices, with a strong emphasis on preventing SQL injection attacks. Use tools and techniques like penetration testing and ethical hacking to provide hands-on experience.</td></tr>
<tr><td>Supply chain management</td><td>Software Updates: Establish a systematic approach to regularly update and patch crew and management systems software to address known vulnerabilities and enhance security features.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><th>LIKELYHOOD</th><th colspan="5">CONSEQUENCES</th></tr>
<tr><th></th><th>INSIGNIFICANT
1</th><th>MINOR
2</th><th>MEDIUM
3</th><th>MAJOR
4</th><th>CATASTROPHIC
5</th></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 1</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">https://www.crowdstrike.com/cybersecurity-101/sql-injection/</td></tr>
</table>

Identified hazard 2.

Risk of malware installation, data breaches, and compromised sensitive information due to phishing attempts targeting crew members.

Identified risk

Phishing and malware attacks on passenger and crew management systems

Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	**8**	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	**8**	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 8

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:

https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures	1. **Email Filtering:** Use advanced email filtering solutions that can detect and block phishing emails before they reach users' inboxes. 2. **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security, making it harder for attackers to gain access even if they obtain login credentials. 3. **Anti-Phishing Toolbars:** Install anti-phishing toolbars in web browsers that can help identify malicious websites. 4. **AI-Driven Intrusion Detection:** Leverage artificial intelligence for detecting and preventing phishing attacks by analyzing patterns and flagging anomalies that suggest malicious activity. 5. **Limit Access with Network Segmentation:** Enforce the principle of least privilege by granting users minimal access necessary for their roles, paired with network segmentation to isolate and secure different network zones. This approach not only restricts user access to reduce risk but also confines potential breaches, minimizing the impact of compromised accounts. 6. **Bring Your Own Device (BYOD) policy:** Implement a BYOD policy that establishes guidelines for securely using personal devices in the workplace. This should include security requirements, access controls, and user responsibility to protect corporate data and network integrity.
Procedural measures (Training, awareness)	**Phishing Awareness Training for seafarers:** Regularly conduct employee training sessions to identify phishing threats, run simulated phishing tests to evaluate awareness, and organize workshops for practical recognition skills, strengthening the human element of cybersecurity.
Supply chain management	1. **Regular Updates and Patch Management:** Keep all systems, software, and applications updated with the latest security patches to protect against vulnerabilities that phishers might exploit. 2. **Password Update and Account Termination Policies:** Mandate periodic password changes for all users every 3-6 months to reinforce security. Ensure immediate account deactivation for individuals who depart the company to maintain system integrity.

Residual risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	**2**	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Residual result: 2

References

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Identified hazard 3.

Interception and manipulation of sensitive communications, leading to unauthorized access to network traffic and potential credential theft.

Identified risk

Man-in-the-Middle Attack (MITM) on passenger and crew management systems

Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	**12**	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 12

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:

https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions	
Technical measures	1. **Encryption:** Use services that offer end-to-end encryption for messaging and email, ensuring that only the communicating users can read the messages. Advanced encryption protocols, like AES (Advanced Encryption Standard). Homomorphic encryption is also used as it allows for computations on encrypted data without needing decryption. These services are widely used to secure these data exchanges. and 2. **Secure Connections:** Use secure, password-protected networks rather than public networks, which are more susceptible to MitM attacks. 3. **Firewalls:** Use firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules.
Procedural measures (Training, awareness)	1. **Regular Training and awareness for IT Professionals:** IT teams should undergo advanced training in network security, encryption, and threat detection to identify and mitigate man-in-the-middle (MITM) attacks. This includes understanding the latest cybersecurity tools and techniques.
Supply chain management	1. **Secure Communications:** Implementing end-to-end encryption for all digital communications, including email, instant messaging, and file transfers, to prevent unauthorized access and ensure privacy. 2. **Collaboration with Major Network Providers:** Major providers can offer enhanced security features, dedicated support, and tailored solutions that meet the specific needs of maritime operations.

Residual risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Residual result: 4

References

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Identified hazard 4.

Disruption of crew access to critical systems, leading to reduced service availability, potential operational delays, and impact on passenger experience.

Identified risk

Denial of service (DOS) on passenger and crew management systems

Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 16

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:

https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

<table>
<tr><td>Technical measures</td><td>1. Unauthorized physical access to a CCR or OT assets on deck and engine room,
2. controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows.
3. restrictions on the use of removable media and disabling USB and similar ports on critical systems.
4. restrictions access and prevent unauthorized access to critical system network infrastructure like power management system</td></tr>
<tr><td>Procedural measures (Training, awareness)</td><td>1. Use MFA and strong password protocol for access to security information.
2. Comply with the cybersecurity protocols provided.
3. Do not pass on admin rights to computers.
4. Maintain effective anti-virus protection on computers.
5. Conduct a cyber security assessment.
6. emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment
7. Give to all company personnel to receive basic cyber awareness training in support of the company’s CRM policies and procedures and the personnel, who have been assigned CRM duties, should receive a type and level of cyber training appropriate to their responsibility and authority</td></tr>
<tr><td>Supply chain management</td><td>1. During port calls limit access to CCR or OT assets the sensitive areas.
2. Do not allow visitors to roam in the vessel unaccompanied.
3. Do not pass on admin rights to systems.
4. Do not pass on passwords to the systems.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><th>LIKELYHOOD</th><th colspan="5">CONSEQUENCES</th></tr>
<tr><th></th><th>INSIGNIFICANT
1</th><th>MINOR
2</th><th>MEDIUM
3</th><th>MAJOR
4</th><th>CATASTROPHIC
5</th></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
</td></tr>
</table>

	Residual result: 3
References	
https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/ism-guidance.html https://portalcip.org/wp-content/uploads/2019/08/C05-Cyber-Security-Assessment.pdf	

7. Power Management Systems

Identified hazard 1.
Loss of electric Energy, Loss of propulsion, loss of manoeuvring, Environmental impact, collision, grounding, etc.
Identified risk
Power management system
Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	*12*	16	**20**
FREQUENT 5	5	10	15	20	25

Initial result: 20

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. Unauthorized physical access to a CCR or OT assets on deck and engine room,
2. controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows.
3. restrictions on the use of removable media and disabling USB and similar ports on critical systems.
4. restrictions access and prevent unauthorized access to critical system network infrastructure like power management system.

<table>
<tr><td>Procedural measures (Training, awareness)</td><td>1. Use MFA and strong password protocol for access to security information.
2. Comply with the cybersecurity protocols provided.
3. Do not pass on admin rights to computers.
4. Maintain effective anti-virus protection on computers.
5. Conduct a cyber security assessment.
6. emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment
7. Give to all company personnel to receive basic cyber awareness training in support of the company’s CRM policies and procedures and the personnel, who have been assigned CRM duties, should receive a type and level of cyber training appropriate to their responsibility and authority</td></tr>
<tr><td>Supply chain management</td><td>1. During port calls limit access to CCR or OT assets the sensitive areas.
2. Do not allow visitors to roam in the vessel unaccompanied.
3. Do not pass on admin rights to systems.
4. Do not pass on passwords to the systems.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><th rowspan="2">LIKELYHOOD</th><th colspan="5">CONSEQUENCES</th></tr>
<tr><th>INSIGNIFICANT
1</th><th>MINOR
2</th><th>MEDIUM
3</th><th>MAJOR
4</th><th>CATASTROPHIC
5</th></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 3</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/ism-guidance.html
https://portalcip.org/wp-content/uploads/2019/08/C05-Cyber-Security-Assessment.pdf</td></tr>
</table>

8. Propulsion and Engine Control Systems

Identified hazard 1.
Main propulsion
Identified risk
Loss of propulsion, loss of manoeuvring, possibility of collision and grounding, environmental problems.
Risk assessment

Initial Use risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	**15**
POSSIBLE 4	4	8	*12*	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 15

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. Unauthorized physical access to a CCR or OT assets on deck and engine room,
2. controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows.
3. restrictions on the use of removable media and disabling USB and similar ports on critical systems of main engines.
4. restrictions access and prevent unauthorized access to critical system network infrastructure like main engines.

<table>
<tr><td>Procedural measures (Training, awareness)</td><td>1. Use MFA and strong password protocol for access to security information.
2. Comply with the cybersecurity protocols provided.
3. Do not pass on admin rights to computers.
4. Maintain effective anti-virus protection on computers.
5. Conduct a cyber security assessment.
6. emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment
7. Give to all company personnel to receive basic cyber awareness training in support of the company’s CRM policies and procedures and the personnel, who have been assigned CRM duties, should receive a type and level of cyber training appropriate to their responsibility and authority</td></tr>
<tr><td>Supply chain management</td><td>1. During port calls limit access to CCR or OT assets the sensitive areas.
2. Control visitor access to vessel and find out who they are.
3. Do not allow visitors to roam in the vessel unaccompanied.
4. Do not pass on admin rights to systems.
5. Do not pass on passwords to the systems.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><td rowspan="2">LIKELYHOOD</td><td colspan="5">CONSEQUENCES</td></tr>
<tr><td>INSIGNIFICANT
1</td><td>MINOR
2</td><td>MEDIUM
3</td><td>MAJOR
4</td><td>CATASTROPHIC
5</td></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 4
</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/ism-guidance.html
https://portalcip.org/wp-content/uploads/2019/08/C05-Cyber-Security-Assessment.pdf</td></tr>
</table>

9. Satellite Communication Systems

Identified hazard 1.
Degradation of the signal, loss of the signal, inability to establish communication
Identified risk
Jamming
Risk assessment

Initial risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	**12**	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 12

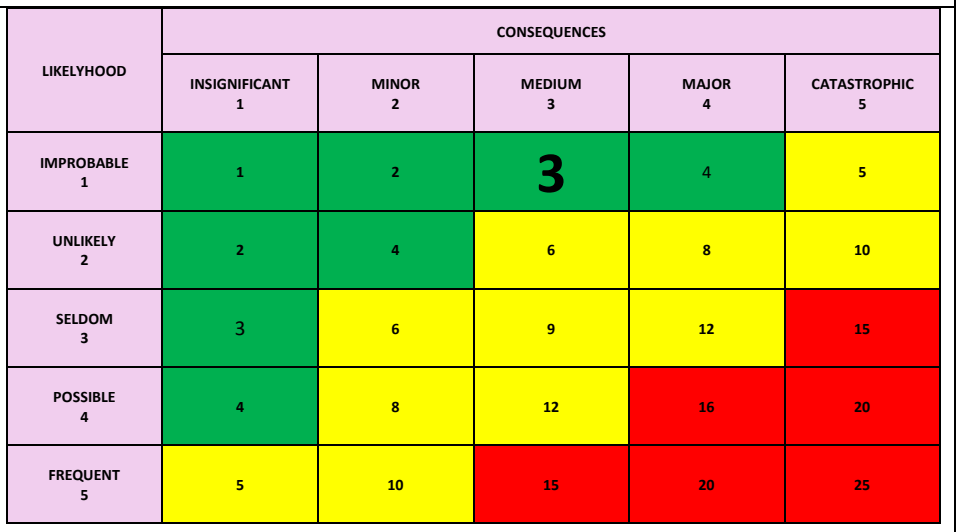
≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures

1. Try to identify the source, type, and location of the jammer.
2. Try to recognize the jamming techniques, such as noise, spot, sweep, barrage, or deceptive jamming.
3. Change your operating frequency.
4. Increase/ decrease your transmit or receive power.
5. Use modulation and coding techniques that can enhance your signal's resistance and resilience to interference.
6. Employ antenna diversity techniques that can exploit the spatial dimension of your signal.

	7. Implement network diversity techniques that can leverage the connectivity and redundancy of your satcom network.
Procedural measures (Training, awareness)	1. Train personnel to test the system. 2. Train personnel on the malfunctioning of the satellite communication systems during a jamming attack. 3. Train personnel on understanding the impact of spoofing of the satellite communication systems. 4. It is recommended that regular GNSS failure drills are carried out to maintain the familiarity with handling jamming events
Supply chain management	1. Before departure test the systems. 2. Observing systems during the voyage constantly.
Residual risk	

Residual result: 3

References

https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity-0/4-technical-aspects-cyberthreats-satellites
https://www.linkedin.com/advice/0/what-most-effective-countermeasures
https://www.sciencedirect.com/science/article/pii/S138912862200319X
https://www.researchgate.net/publication/265008517_Detecting_Meaconing_Attacks_by_Analysing_the_Clock_Bias_of_Gnss_Receivers
https://www.researchgate.net/publication/333615708_Meaconing_and_Spoofing_Attacks_Evaluation_with_Enhancement_in_Security_for_Satellite_Communication

Identified hazard 2.	
Degradation of the signal, loss of the signal, inability to establish communication	
Identified risk	
Spoofing	
Risk assessment	
Initial risk	

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	**16**	20
FREQUENT 5	5	10	15	20	25

Initial result: 16

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions	
Technical measures	1. Use of array antennas, such as CRPA. 2. Monitoring of certain GNSS receiver Key Performance Indicators (KPI), such as monitoring for clock jumps, unusual or implausible signal-to-noise density ratios, or differences between code and carrier measurements. 3. Use multiple satellite communication systems. 4. Usage of PHY-layer information. 5. Use cryptographic protocols.
Procedural measures (Training, awareness)	1. Train personnel to test the system. 2. Train personnel on the malfunctioning of the satellite communication systems during a spoofing attack.

	3. Train personnel on understanding the impact of spoofing of the satellite communication systems. 4. It is recommended that regular GNSS failure drills are carried out to maintain the familiarity with handling spoofing events.
Supply chain management	1. Before departure test the systems. 2. Observing systems during the voyage constantly.
Residual risk	

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	**4**	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Residual result: 4

References

https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity-0/4-technical-aspects-cyberthreats-satellites
https://scholar.afit.edu/etd/2729/
https://www.sciencedirect.com/science/article/pii/S138912862200319X
https://www.researchgate.net/publication/265008517_Detecting_Meaconing_Attacks_by_Analysing_the_Clock_Bias_of_Gnss_Receivers
https://www.researchgate.net/publication/333615708_Meaconing_and_Spoofing_Attacks_Evaluation_with_Enhancement_in_Security_for_Satellite_Communication

Identified hazard 3.	
Loss of position, incorrect position, collision, grounding	
Identified risk	
Meaconing	
Risk assessment	
Initial risk	

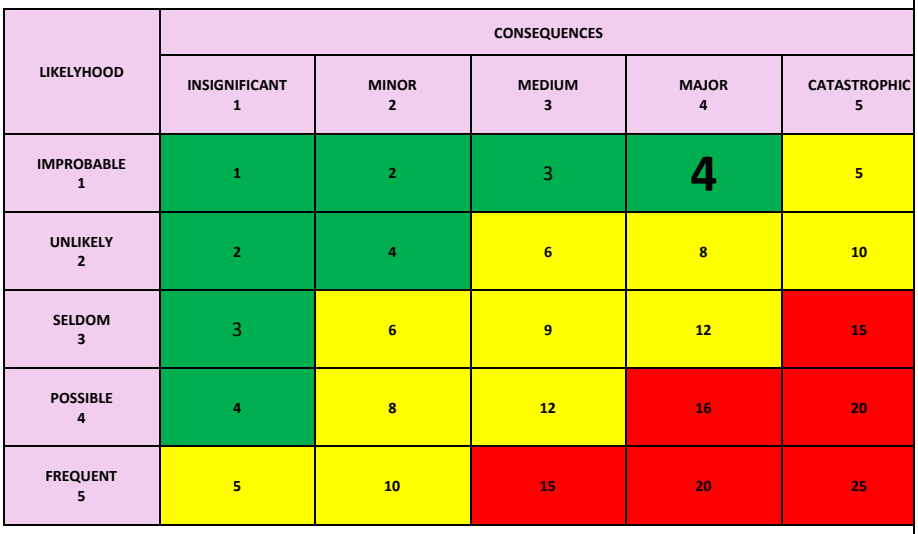
LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	**12**	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 12

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions	
Technical measures	1. Use of array antennas, such as CRPA. 2. Monitoring of certain GNSS receiver Key Performance Indicators (KPI), such as monitoring for clock jumps, unusual or implausible signal-to-noise density ratios, or differences between code and carrier measurements. 3. Use multiple satellite communication systems. 4. Usage of PHY-layer information. 5. Use cryptographic protocols.
Procedural measures (Training, awareness)	1. Train personnel to test the system. 2. Train personnel on the malfunctioning of the satellite communication systems during a meaconing attack. 3. Train personnel on understanding the impact of meaconing of the satellite communication systems.

	4. It is recommended that regular GNSS failure drills are carried out to maintain the familiarity with handling meaconing events.
Supply chain management	1. Before departure test the systems. 2. Observing systems during the voyage constantly.
Residual risk	 Residual result: 4

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	**4**	5
UNLIKELY 2	2	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

References

https://www.sciencedirect.com/science/article/pii/S138912862200319X
https://www.researchgate.net/publication/265008517_Detecting_Meaconing_Attacks_by_Analysing_the_Clock_Bias_of_Gnss_Receivers
https://www.researchgate.net/publication/333615708_Meaconing_and_Spoofing_Attacks_Evaluation_with_Enhancement_in_Security_for_Satellite_Communication

10. Weather Monitoring Systems

Identified hazard 1.
Collision, grounding, sinking, loss of cargo
Identified risk
Wrong weather prediction in case of wind/sea state/ atmospheric pressure
Risk assessment

Initial risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	**4**	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 4

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions	
Technical measures	1. Have an alternate system for monitoring weather conditions. 2. Check the previous weather prediction and compare the weather condition development with the previous condition. 3. Confirm the information with other weather monitoring system.
Procedural measures	1. Train personnel to test the system.

<table>
<tr><td>(Training, awareness)</td><td>2. Train personnel on the malfunctioning of the weather monitoring systems.
3. Train personnel on different interferences of weather monitoring systems.</td></tr>
<tr><td>Supply chain management</td><td>1. During port calls check the weather prediction from other that onboard systems.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><td rowspan="2">LIKELYHOOD</td><td colspan="5">CONSEQUENCES</td></tr>
<tr><td>INSIGNIFICANT
1</td><td>MINOR
2</td><td>MEDIUM
3</td><td>MAJOR
4</td><td>CATASTROPHIC
5</td></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 2
</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">The risk areas have been defined on the basis of expert knowledge and have no external reference.</td></tr>
</table>

Identified hazard 2.
Collision, grounding, sinking, loss of cargo
Identified risk
Distorted position of the weather map
Risk assessment

Initial risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	2	4	**6**	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 6

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions

Technical measures	1. Have an alternate system for monitoring weather conditions. 2. Check the previous weather prediction and compare the weather condition development with the previous condition. 3. Confirm the information with other weather monitoring system. 4. Check the positioning system.
Procedural measures (Training, awareness)	1. Train personnel to test the system. 2. Train personnel on the malfunctioning of the weather monitoring systems. 3. Train personnel on different interferences of weather monitoring systems.

<table>
<tr><td>Supply chain management</td><td>1. During port calls check the weather prediction from other that onboard systems.</td></tr>
<tr><td>Residual risk</td><td>
<table>
<tr><td rowspan="2">LIKELYHOOD</td><td colspan="5">CONSEQUENCES</td></tr>
<tr><td>INSIGNIFICANT
1</td><td>MINOR
2</td><td>MEDIUM
3</td><td>MAJOR
4</td><td>CATASTROPHIC
5</td></tr>
<tr><td>IMPROBABLE
1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>UNLIKELY
2</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>SELDOM
3</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>POSSIBLE
4</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>FREQUENT
5</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
</table>
Residual result: 2
</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">The risk areas have been defined on the basis of expert knowledge and have no external reference.</td></tr>
</table>

Identified hazard 3.	
Delay in arrival, higher fuel consumption, longer route	
Identified risk	
Improper route planning/ extended route times (to avoid heavily bad weather condition)	
Risk assessment	
Initial risk	

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	**2**	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Initial result: 2

≤4: Maintain effective risk management procedures in place
5-12: Recommended to take mitigating actions to reduce risk.
>12: Immediate mitigating actions are required to reduce risk.

GUIDANCE FOR THE USE OF MATRIX:
https://www.hse.gov.uk/enforce/expert/alarpglance.htm

Mitigation actions	
Technical measures	1. Have/use an alternate system for monitoring weather conditions. 2. Check the previous weather prediction and compare the weather condition development with the previous condition. 3. Confirm the information with other weather monitoring systems.
Procedural measures (Training, awareness)	1. Train personnel to test the system. 2. Train personnel on the malfunctioning of the weather monitoring systems. 3. Train personnel on different interferences of weather monitoring systems.
Supply chain management	During port calls check the weather prediction from other than onboard systems.

Residual risk

LIKELYHOOD	CONSEQUENCES				
	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	CATASTROPHIC 5
IMPROBABLE 1	1	2	3	4	5
UNLIKELY 2	**2**	4	6	8	10
SELDOM 3	3	6	9	12	15
POSSIBLE 4	4	8	12	16	20
FREQUENT 5	5	10	15	20	25

Residual result: 2

References

The risk areas have been defined on the basis of expert knowledge and have no external reference.

11. Summary

The document contains detailed vulnerability assessments for various maritime systems. To evaluate and rate vulnerabilities on their frequency and severity, following steps were done:

- categorize vulnerabilities by their identified systems
- analyse frequency and danger levels based on the provided impact and likelihood ratings
- summarize ratings in tables, including frequency, severity, and combined risk ratings.

Top 10 vulnerabilities analysis results:

Rank	Vulnerability	Frequency (1-5)	Severity (1-5)	Risk Score
1	Power Management System failure	5	5	25
2	GPS Disturbance in Navigation Systems	4	5	20
3	Propulsion and Engine Control failure	4	5	20
4	Malware attack on Cargo Management Systems	4	4	16
5	Phishing emails on Cargo Management Systems	4	4	16
6	Malicious Software on Integrated Bridge Systems	4	4	16
7	DDoS attack on Onboard Entertainment Systems	4	4	16
8	Ransomware attack on Cargo Management Systems	3	5	15
9	SQL Injection on Passenger and Crew Management Systems	3	4	12
10	AIS Spoofing in Navigation Systems	3	4	12

Summary statistics:

Metric	Frequency (1-5)	Severity (1-5)	Risk Score
Mean	3.8	4.4	16.8
Minimum	3.0	4.0	12.0
Maximum	5.0	5.0	25.0
Standard Deviation	0.63	0.52	3.94

Analysis

1. Power Management System failure represents the highest risk with a maximum score of 25, driven by its high likelihood and catastrophic consequences.
2. GPS Disturbance and Propulsion/Engine Control issues follow closely, indicating critical vulnerabilities in navigation and propulsion systems.
3. Most vulnerabilities are frequent or possible (scores 3-4) and have severe to catastrophic impacts (scores 4-5).
4. Lower-ranked issues like SQL Injection and AIS Spoofing, while important, present moderate combined risks due to reduced frequency.

Recommendations

1. Priority Mitigations: Focus on high-risk systems like Power Management and Navigation
2. Awareness Programs: Train staff on phishing and malware defence for common vulnerabilities.
3. Technical Enhancements: Strengthen system redundancies and implement robust monitoring protocols.

12. Important documents and sources

Here are the official sources used in analysing this document and verifying general information about vulnerabilities and risk management:

1. **European Union Agency for Cybersecurity (ENISA)**:
    - Reports such as **ENISA Threat Landscape 2023**, providing detailed insights into the latest trends in cyber threats and vulnerabilities.
2. **DNV (Det Norske Veritas)**:
    - **Guidelines on Maritime Cyber Security**, addressing specific threats to the maritime sector and recommended mitigation measures.
3. **CISA (Cybersecurity and Infrastructure Security Agency)**:
    - **Guidance on GPS and AIS Spoofing**, critical for understanding security issues in navigation systems.
4. **IMO (International Maritime Organization)**:
    - **Maritime Cyber Risk Management Guidelines**, outlining standards for managing cyber threats in the maritime industry.
5. **ResearchGate and IEEE**:
    - Academic publications, including:
        - "Detecting Meaconing Attacks by Analysing the Clock Bias of GNSS Receivers".
        - "Evaluation of Spoofing and Meaconing Attacks in Maritime Satellite Communications".
6. **HSE (Health and Safety Executive)**:
    - Guidance on **Risk Matrix Usage**, explaining methodologies for risk