Communication and cybersecurity for autonomous passenger ferries

Dr. Ahmed Amro

Supervisors: Associate Professor Vasileios Gkioulos and Professor Sokratis Katsikas

Department of Information Security and Communication Technology (IIK), Gjøvik

NTNU

The What

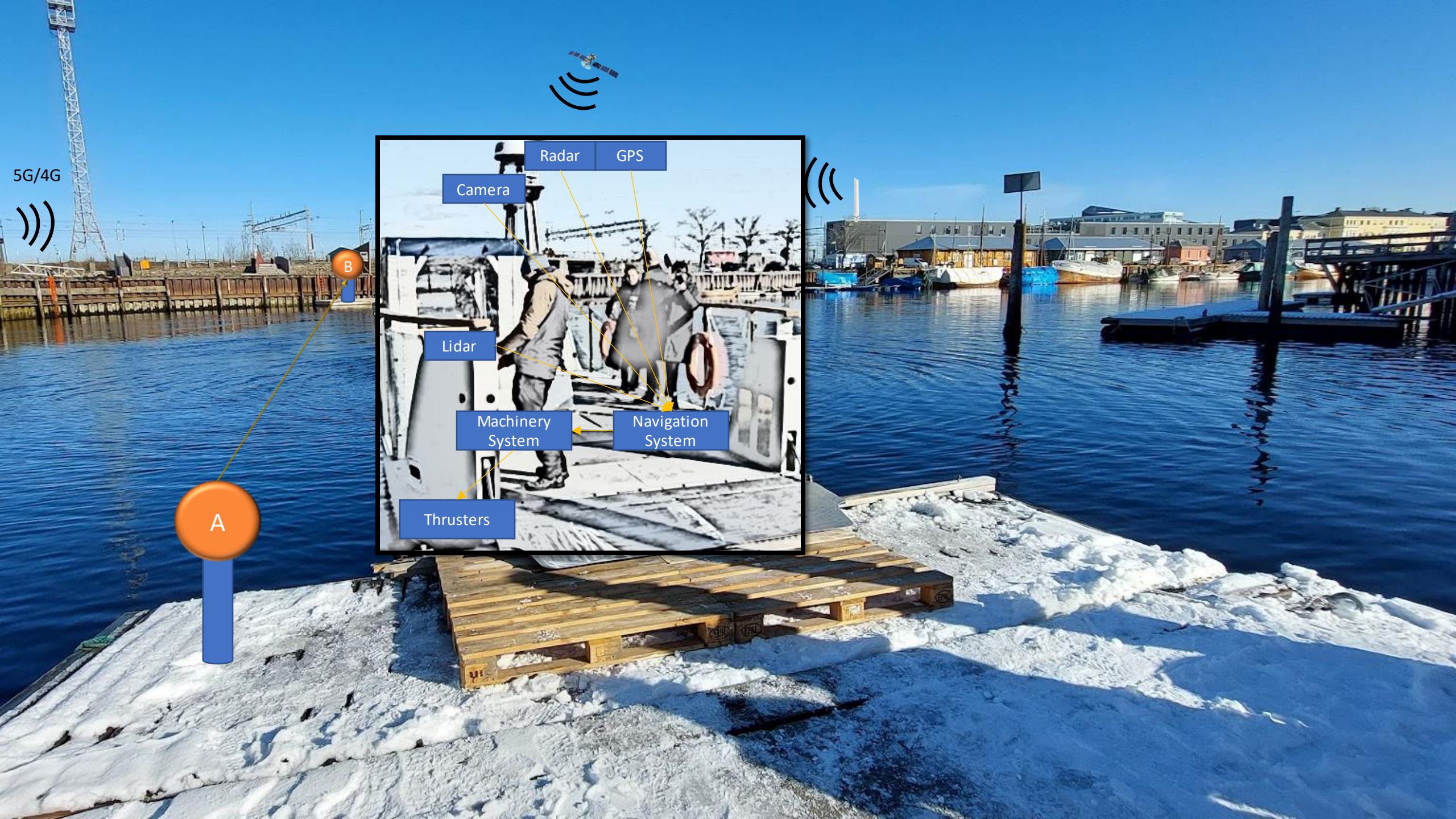
What is the mission?


HANMO AS
SIMRA
NTNU


SIMRA


B
A


5G/4G
B
A


5G/4G
B
A
Radar
GPS
Camera
Lidar
Machinery System
Navigation System
Thrusters


B
How to connect them
How to secure them
A

The Why

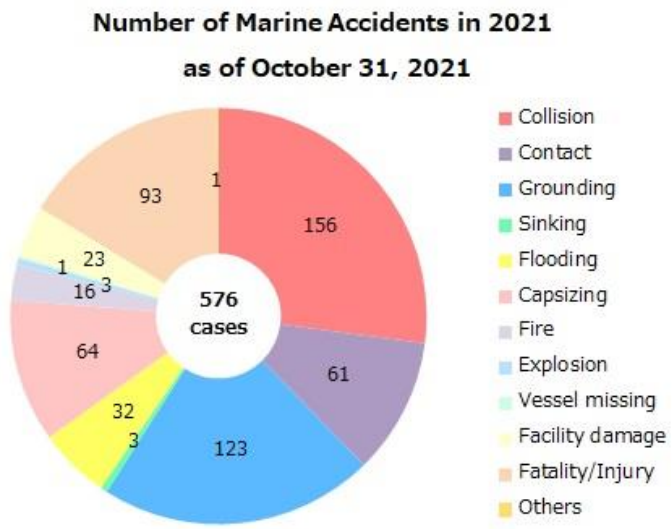
Why communications and cybersecurity are important?


Some time in the future

Breaking News

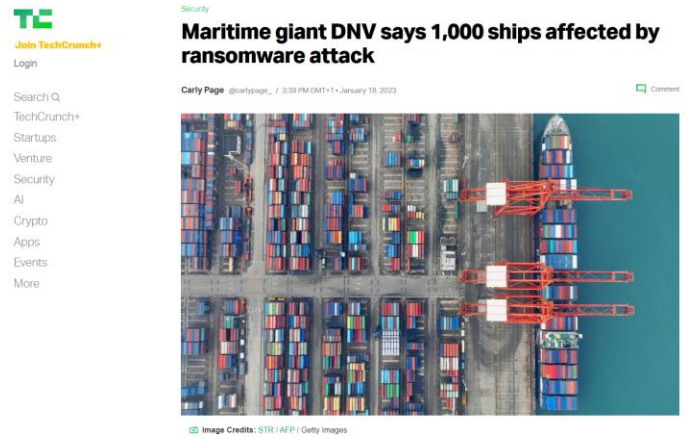
A passenger ferry was hacked and led to collision.

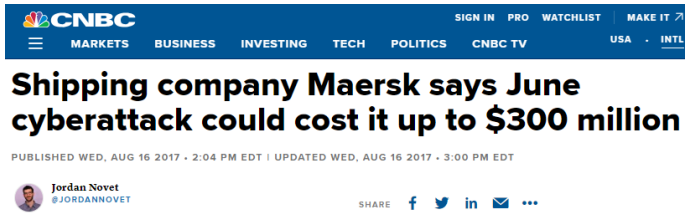
Some passengers are injured.



https://www.mlit.go.jp/jtsb/statistics_mar.html#p02

Some Cyber Attacks against Maritime Systems





Cyber risk management in maritime systems

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

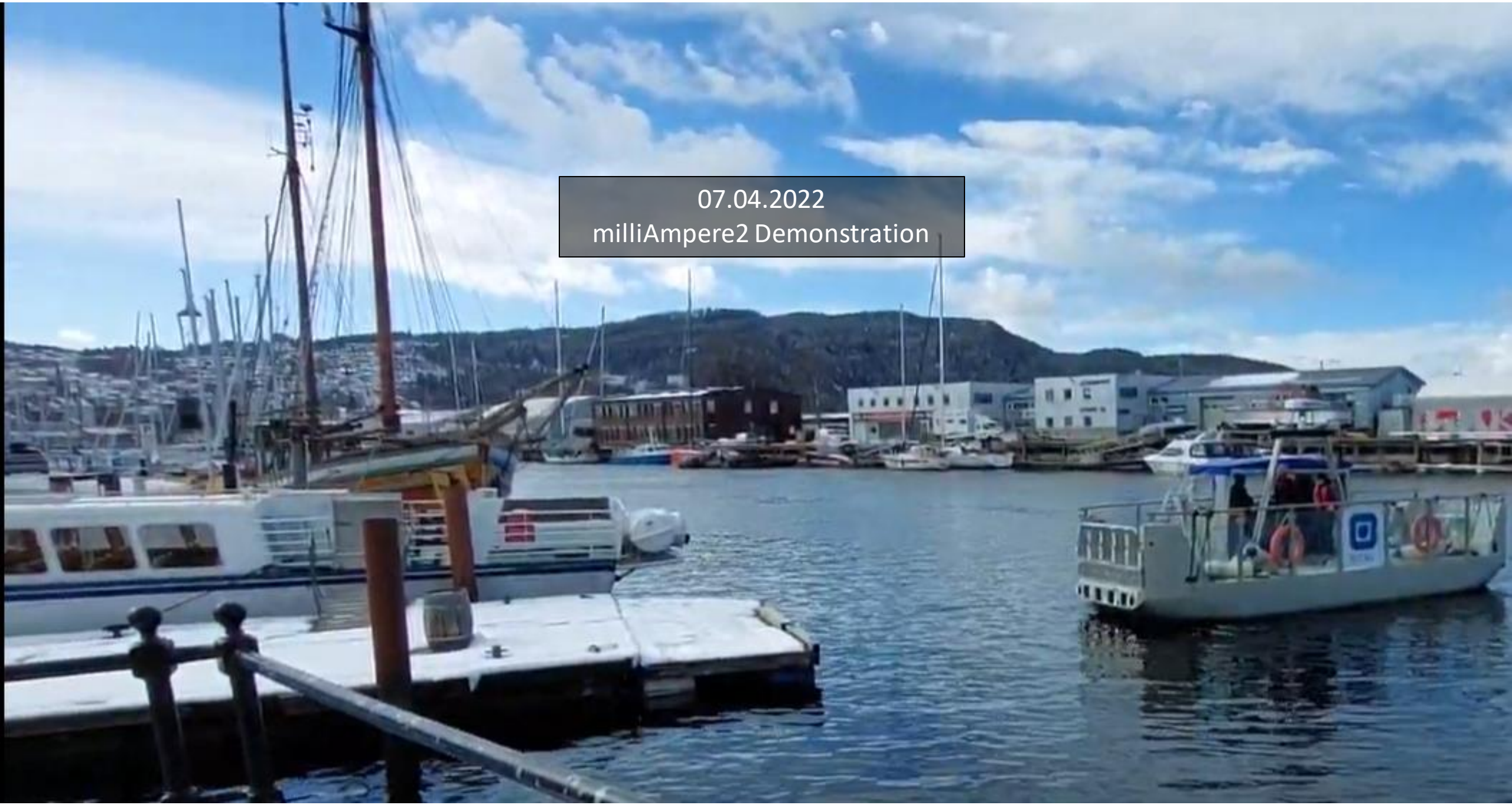
MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

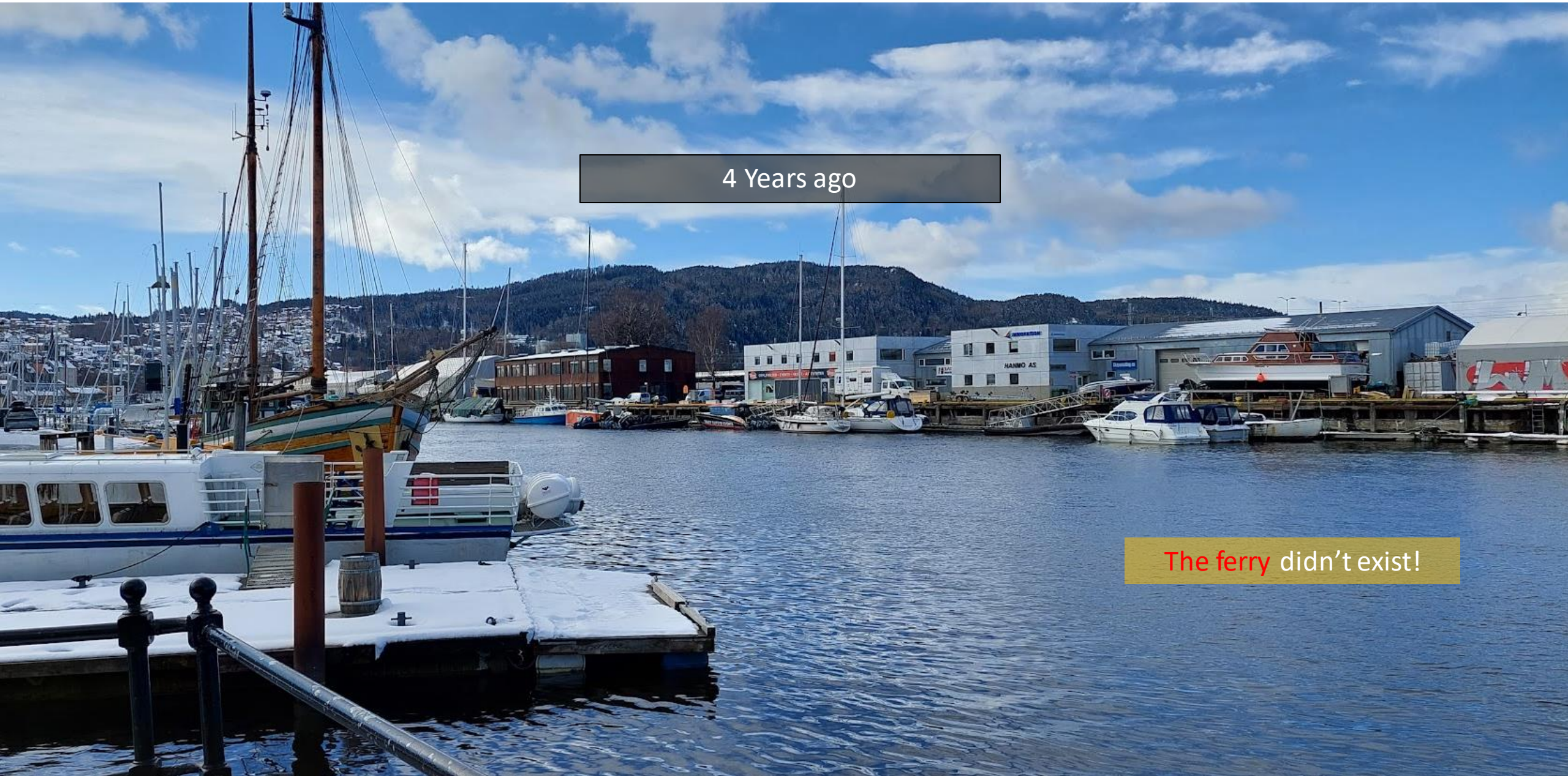
THE MARITIME SAFETY COMMITTEE,

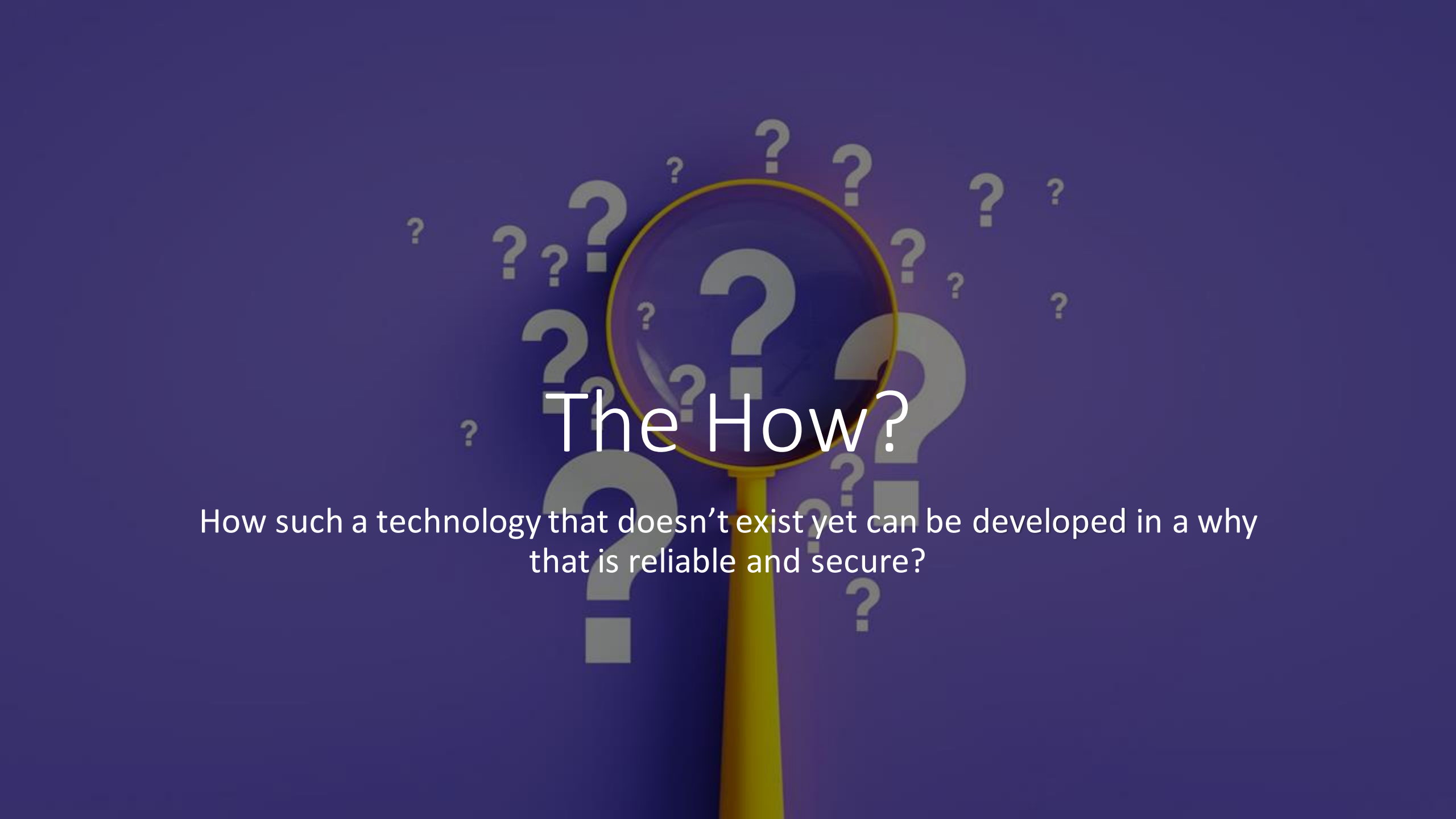
RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

First Challenge

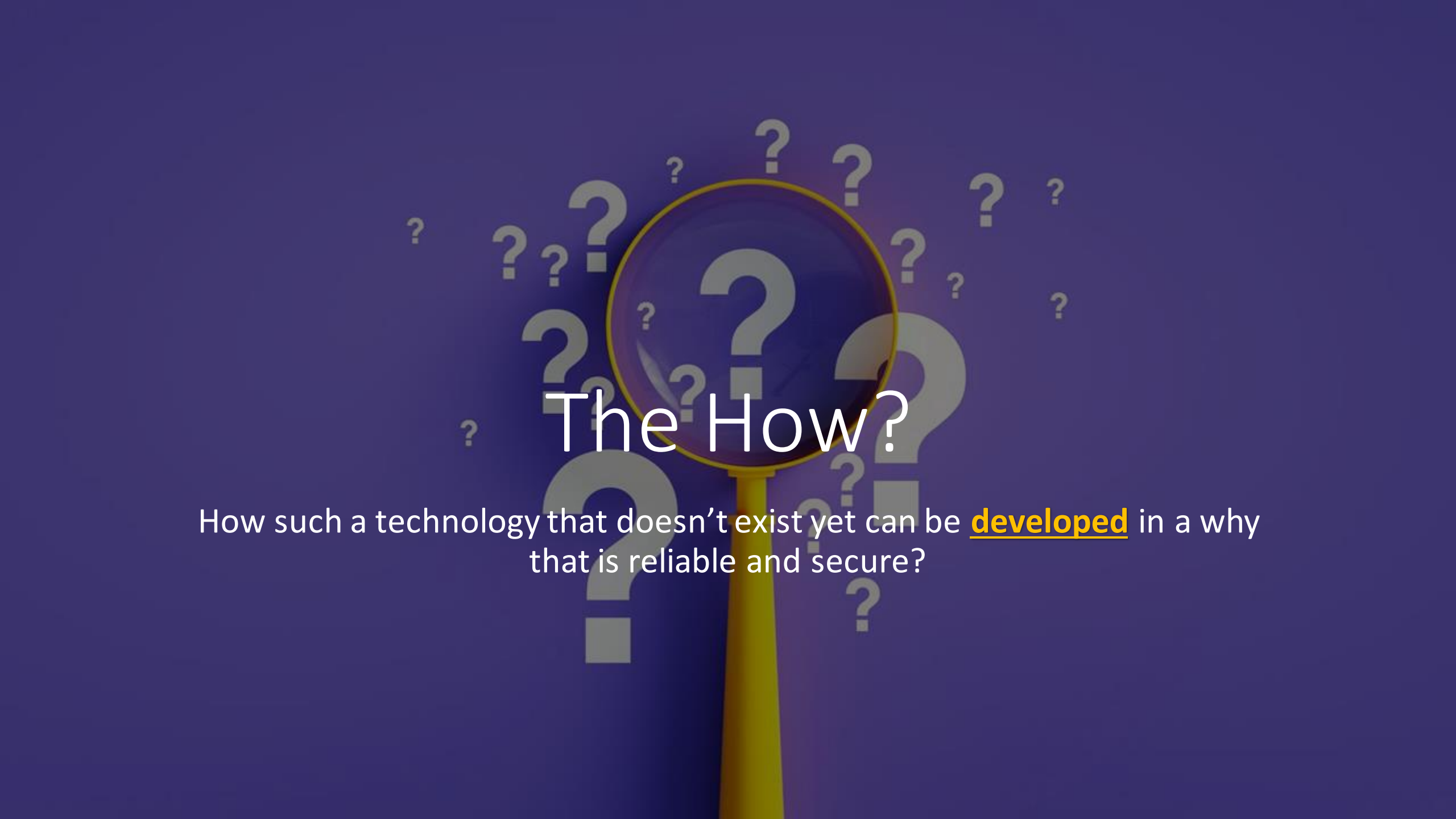

07.04.2022
milliAmpere2 Demonstration


4 Years ago
The ferry didn’t exist!



The How?

How such a technology that doesn’t exist yet can be developed in a why that is reliable and secure?

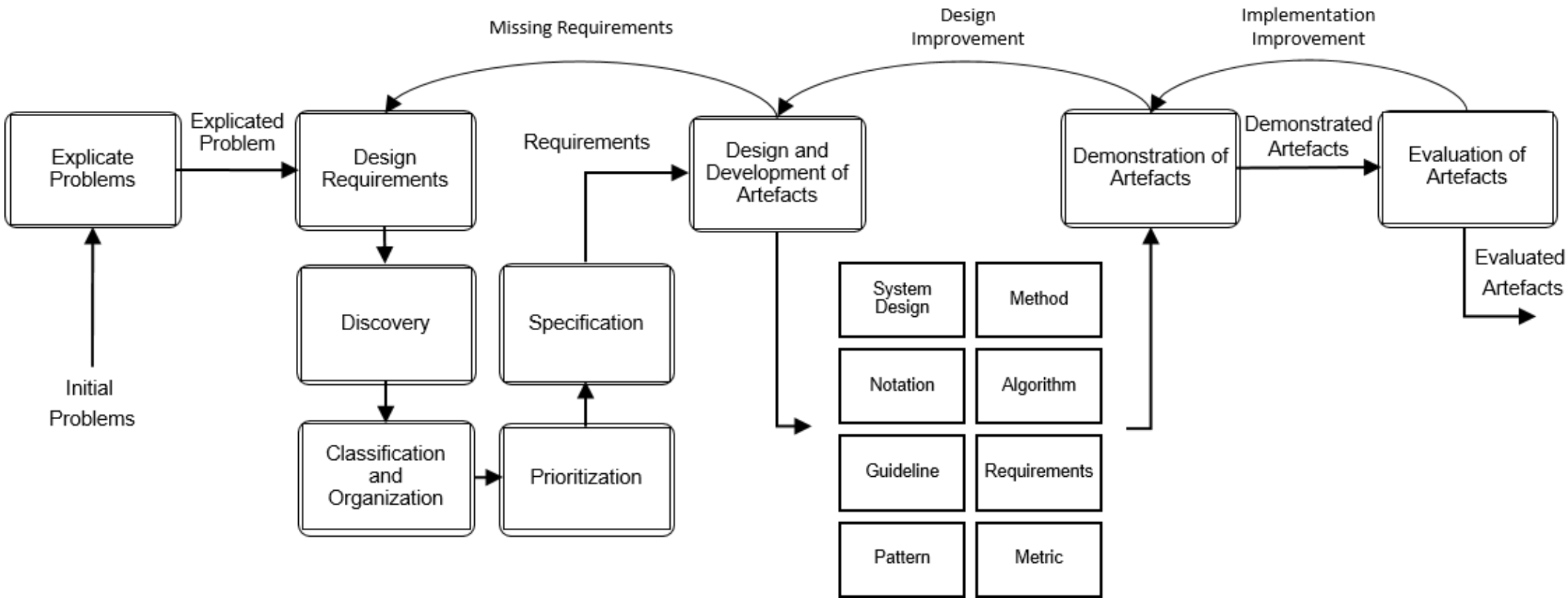


The How?

How such a technology that doesn’t exist yet can be **developed** in a why that is reliable and secure?

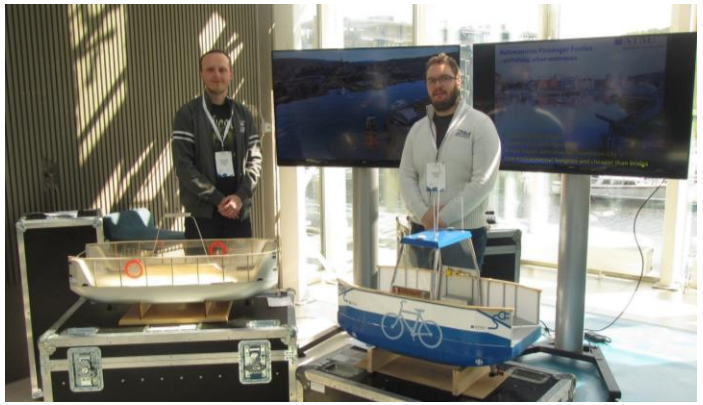
The methodology

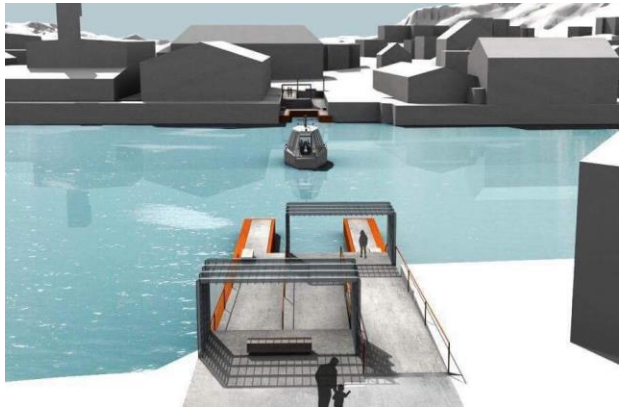
- Design Science research methodology
- System engineering approach



The Journey

From concept to application

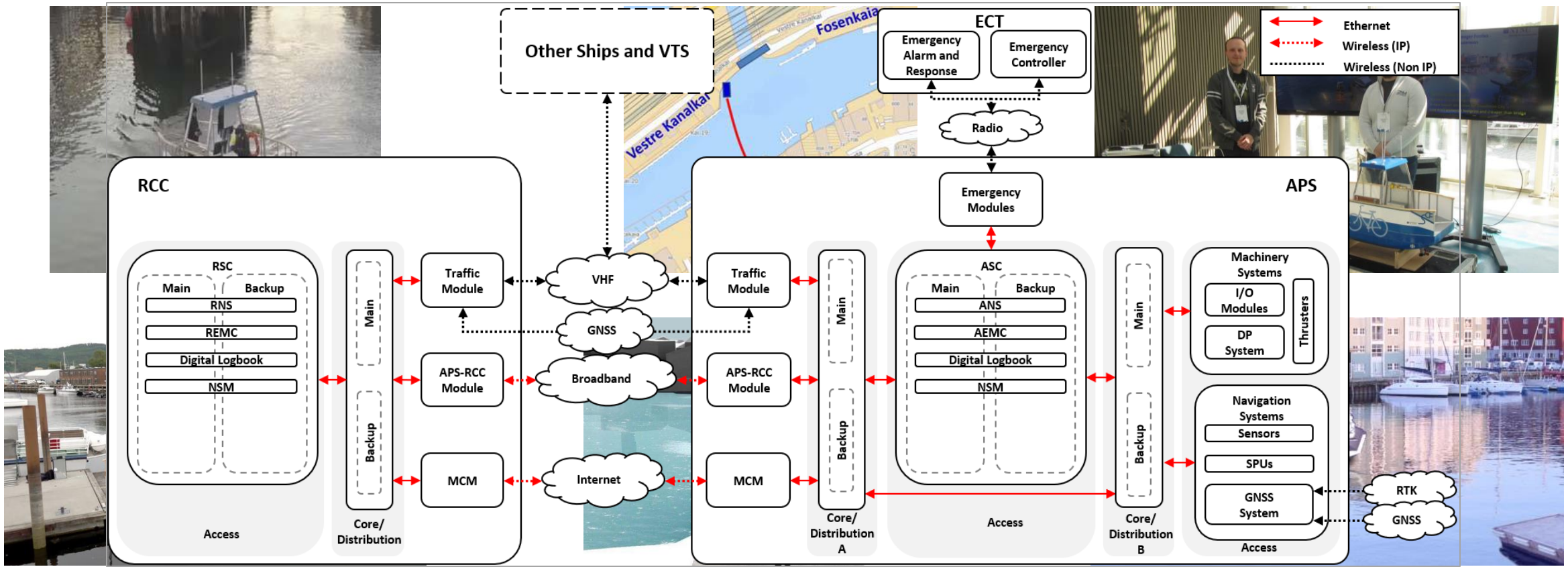




- Operational Mode
- Stakeholders
- Requirements
- Functions
- Components

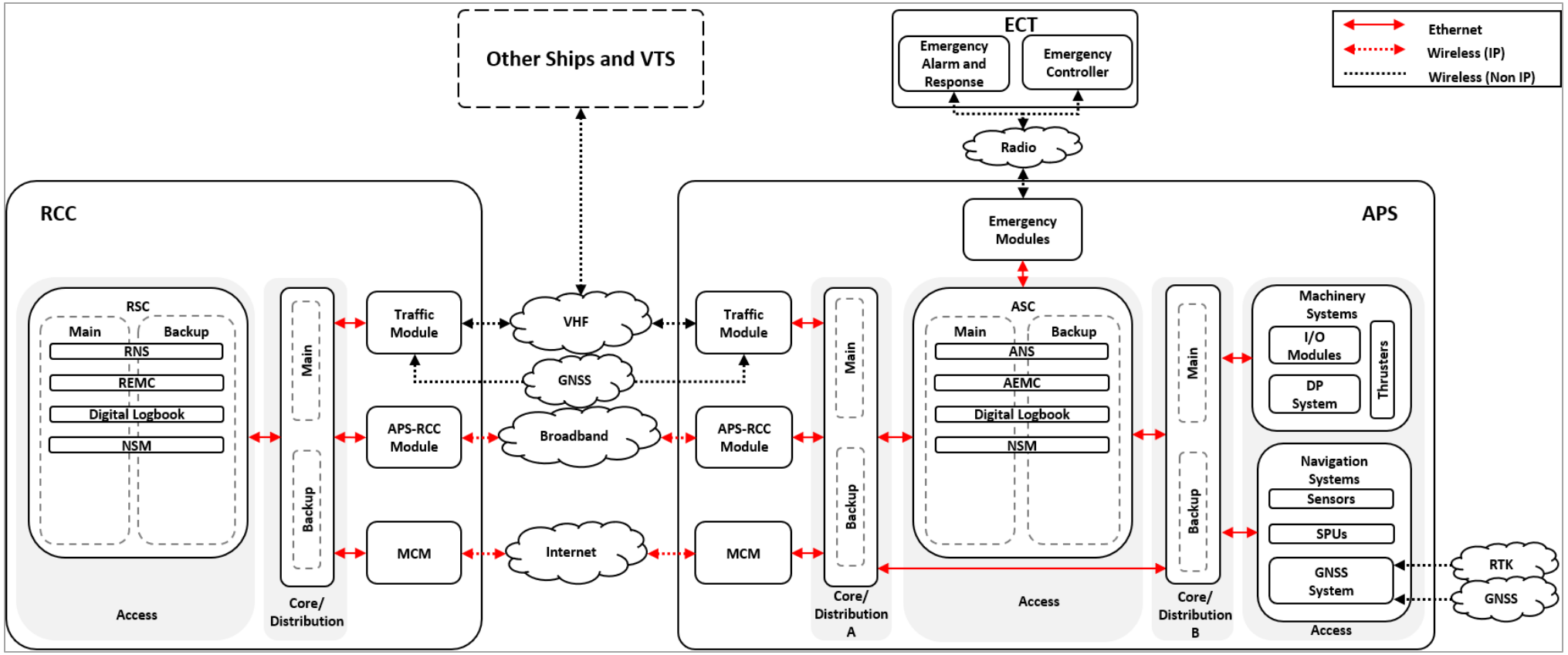
Concept to Design

Publication:
Amro, A., Gkioulos, V., & Katsikas, S. (2020). Connect and protect: requirements for maritime autonomous surface ship in urban passenger transportation. In *Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26–27, 2019 Revised Selected Papers 5* (pp. 69-85). Springer International Publishing.



Concept to Design

Publication:
Amro, A., Gkioulos, V., & Katsikas, S. (2023). Communication architecture for autonomous passenger ship. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 237(2), 459-484.



Cyber Risk Management

Threat-informed approach

What can go wrong?

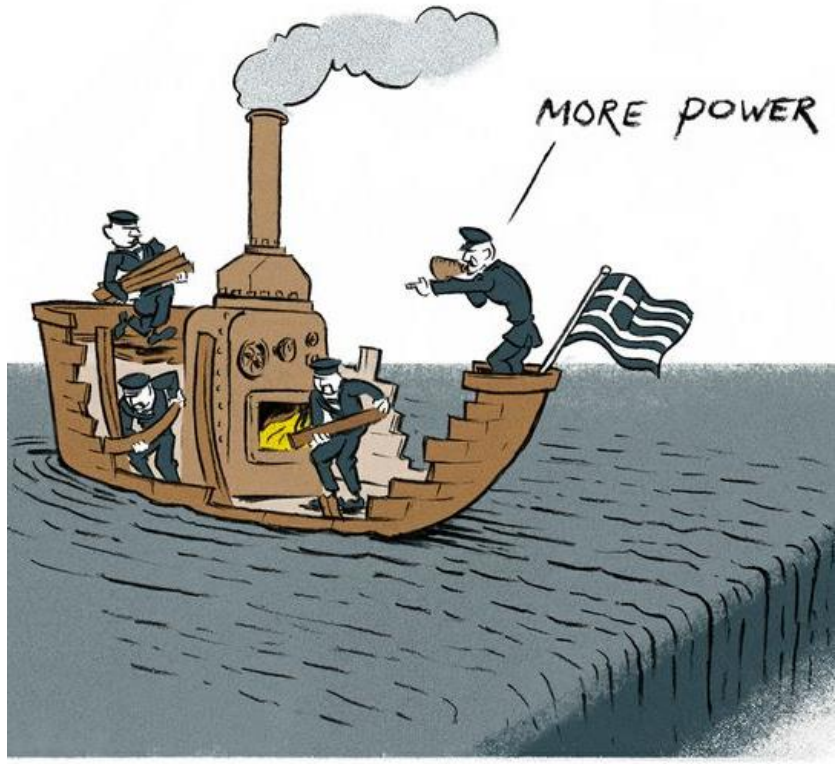
Objectives

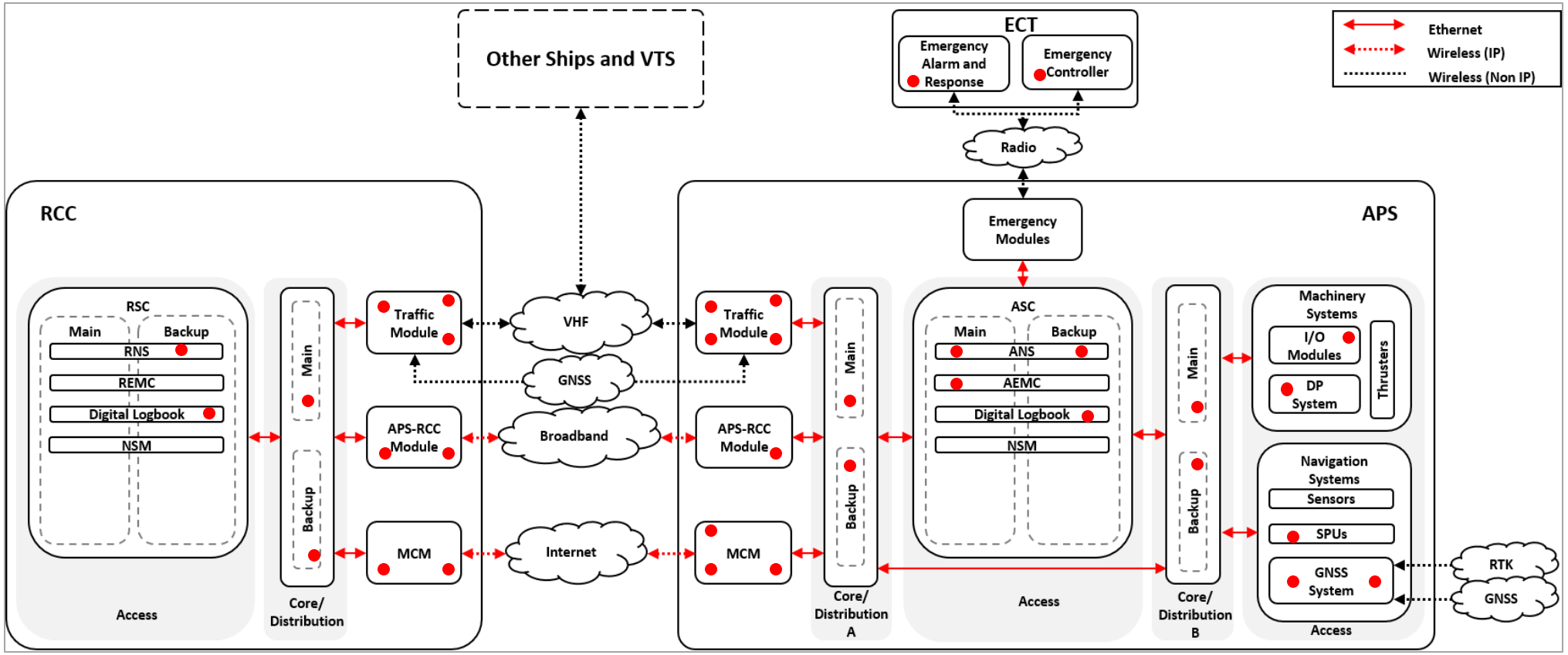
Techniques

Risks

How to avoid it?

Security controls





Identify Risks

Publications:

- Amro, A., Gkioulos, V., & Katsikas, S. (2023). Assessing cyber risk in cyber-physical systems using the ATT&CK framework. ACM Transactions on Privacy and Security, 26(2), 1-33.
- Amro, A., & Gkioulos, V. (2023). Evaluation of a Cyber Risk Assessment Approach for Cyber–Physical Systems: Maritime-and Energy-Use Cases. Journal of Marine Science and Engineering, 11(4), 744.

16 Failure Category (Objectives)

736 Failure Mechanism (Attacks)

Initial Access

16 Failure Category (Objectives)

16 Failure Category (Objectives)

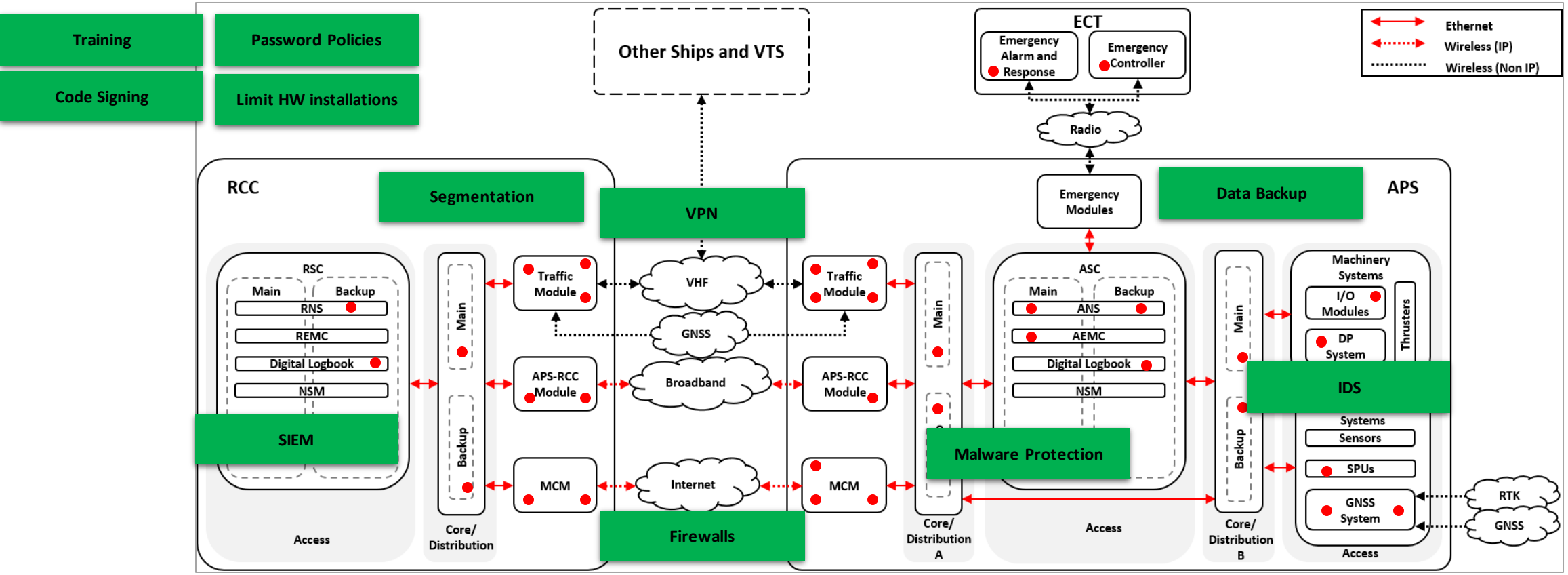
Exfiltration

16 Failure Category (Objectives)

Command and Control

16 Failure Category (Objectives)

Impact



Risks treatment

Publication:
Amro, A., & Gkioulos, V. (2023). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. International Journal of Information Security, 22(1), 249-288.

New attacks and defensive measures

Navigation Data Security

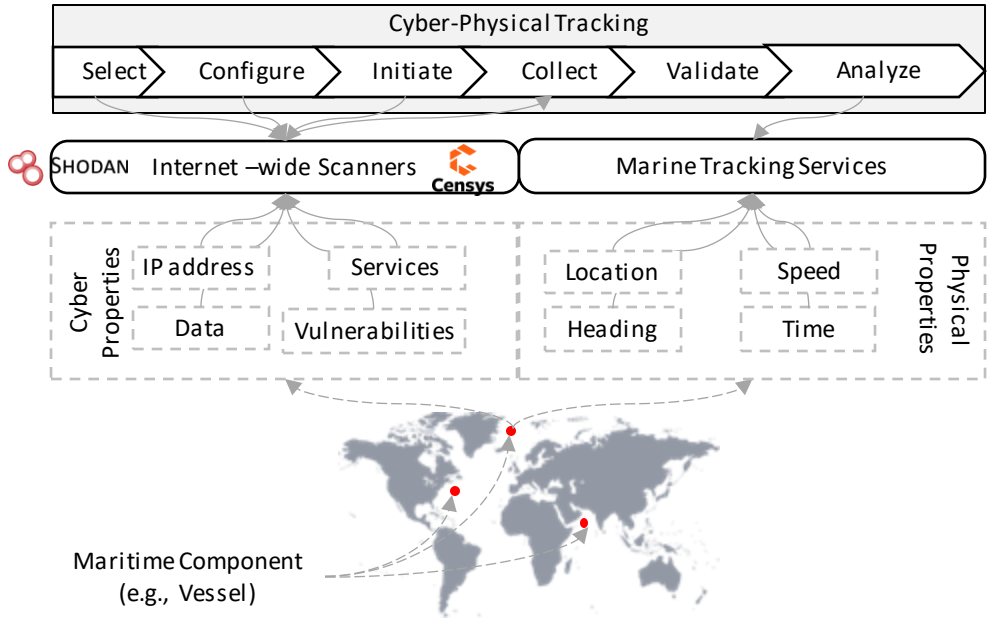
Reconnaissance

Cyber-Physical Tracking of Maritime Components

Publication

Amro, A. (2021). Cyber-Physical Tracking of IoT devices: A maritime use case. In Norsk IKT-konferanse for forskning og utdanning (No. 3).

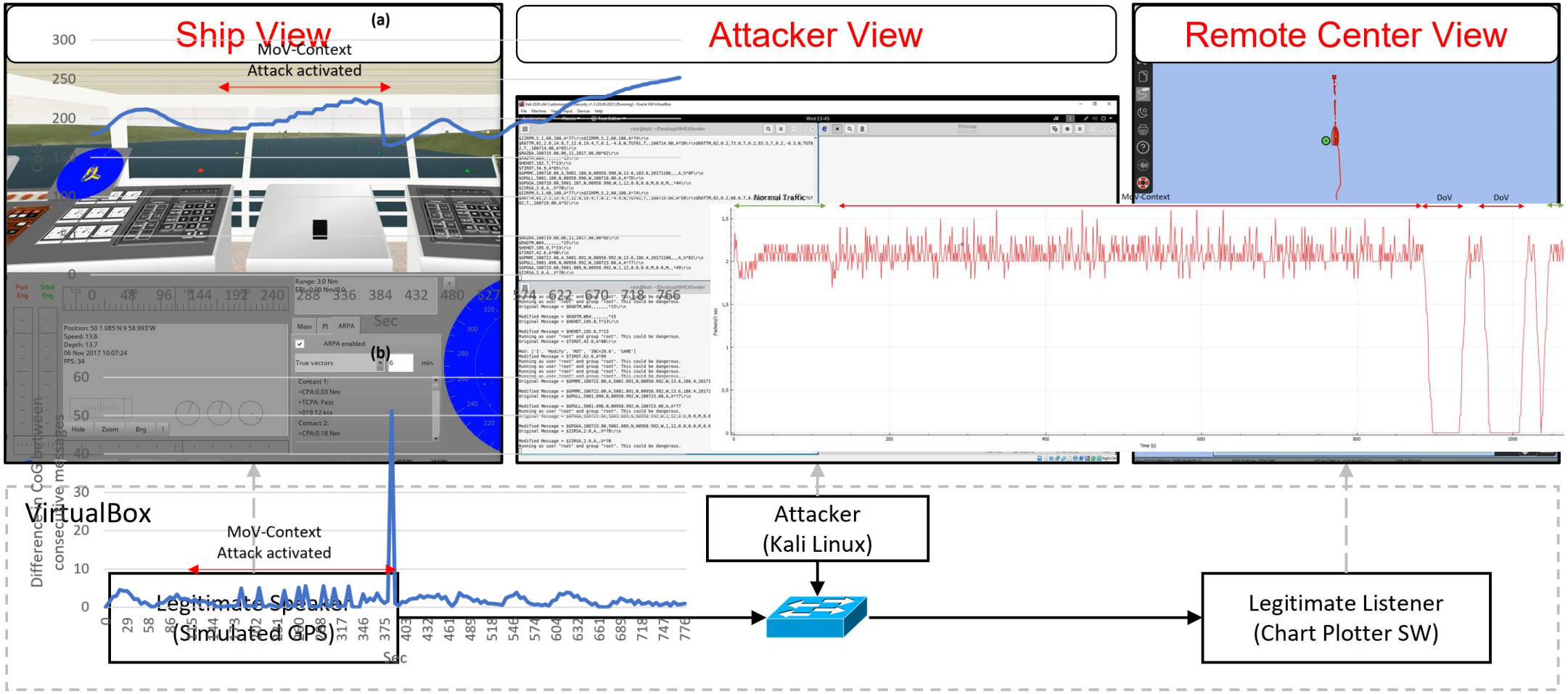
Messages	Description	Host Count (%)	Possible CVEs (CVSS)
Most common: PMTKAGC, PMTKGALM, PMTKGEPH ,PMTKTSX1	MediaTek MTK chipsets	1662 (97,6%)	CVE-2020-13841 (9.8) CVE-2020-13842 (7.8)
PSTT	Saab Systems position receiver	35 (0,9%)	None
PCPTI	Cradlepoint Router	28 (0,7%)	
PLEIR	LEICA GPS receiver	21 (0,5%)	
PTNL	Trimble GNSS Receiver	3 (0,1%)	CVE-2012-5053 (4.2)
PQXFI	Qualcomm chipset	1 (0,0%)	CVE-2021-1965 (9.8) CVE-2021-1955 (7.5)



Impact

Navigation Data Anomaly Analysis and Detection

Publication
Amro, A.; Oruc, A.; Gkioulos, V.; Katsikas, S. Navigation Data Anomaly Analysis and Detection. Information 2022, 13, 104. https://doi.org/10.3390/info13030104

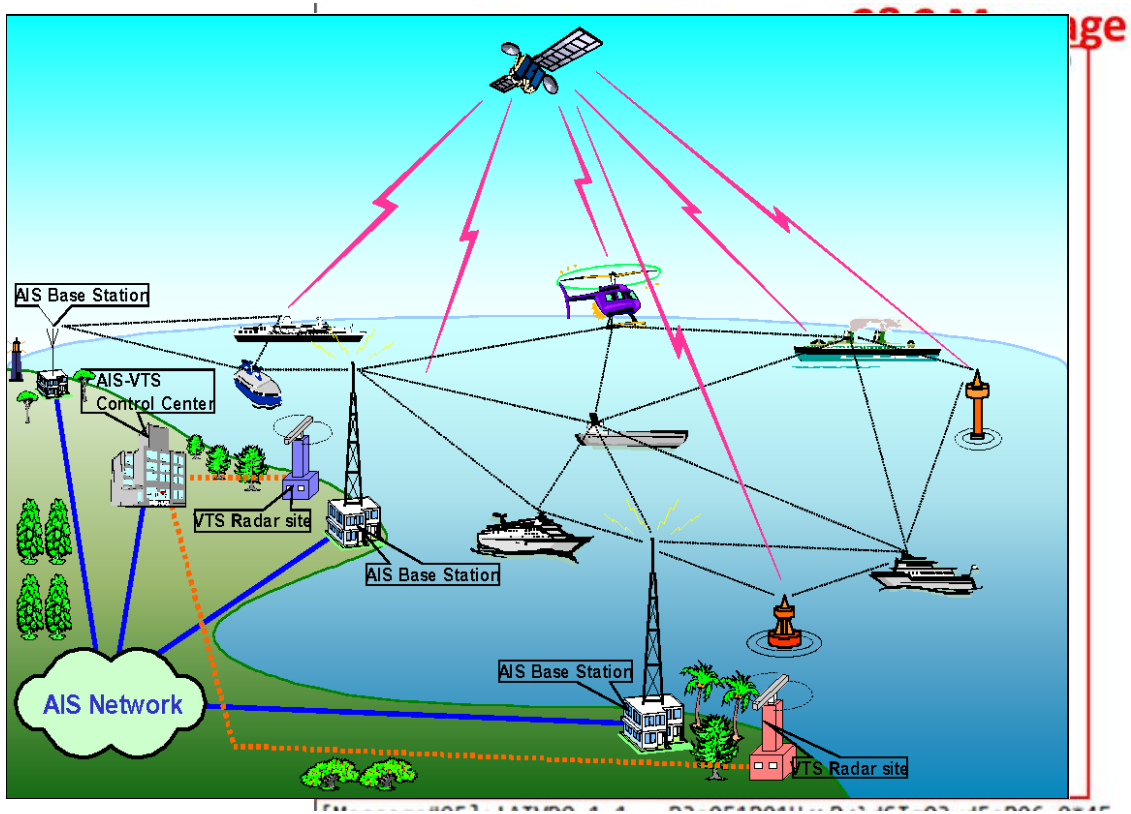


Command and Control

AIS as Covert Channel

Publication

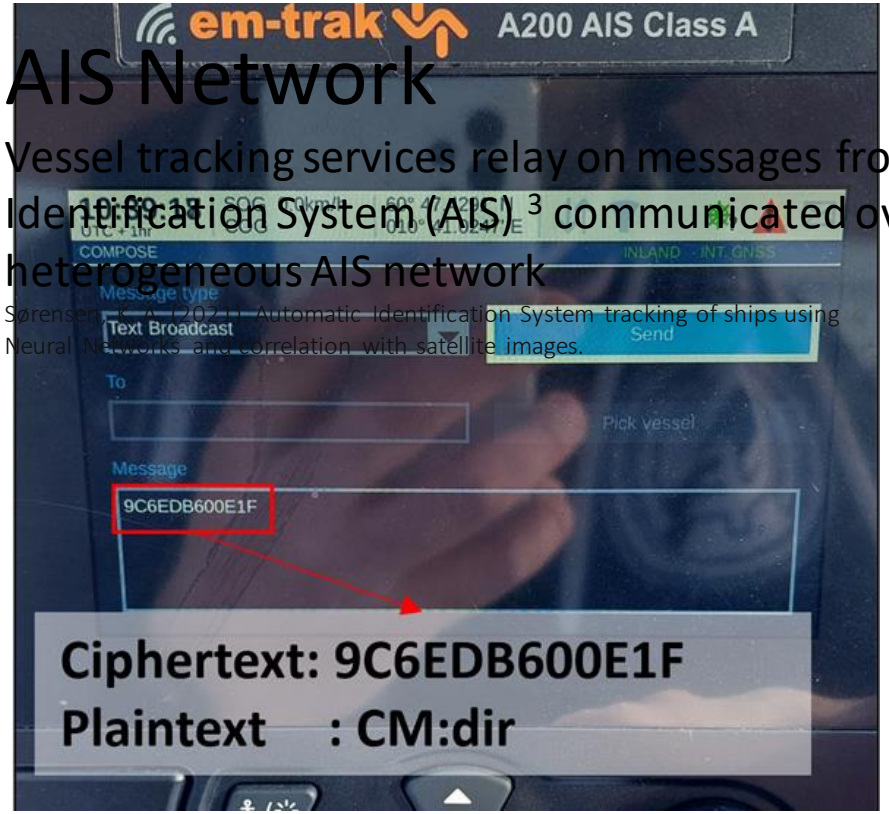
Amro, A., & Gkioulos, V. (2022, September). From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks. In Computer Security–ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part III (pp. 535-553). Cham: Springer Nature Switzerland.

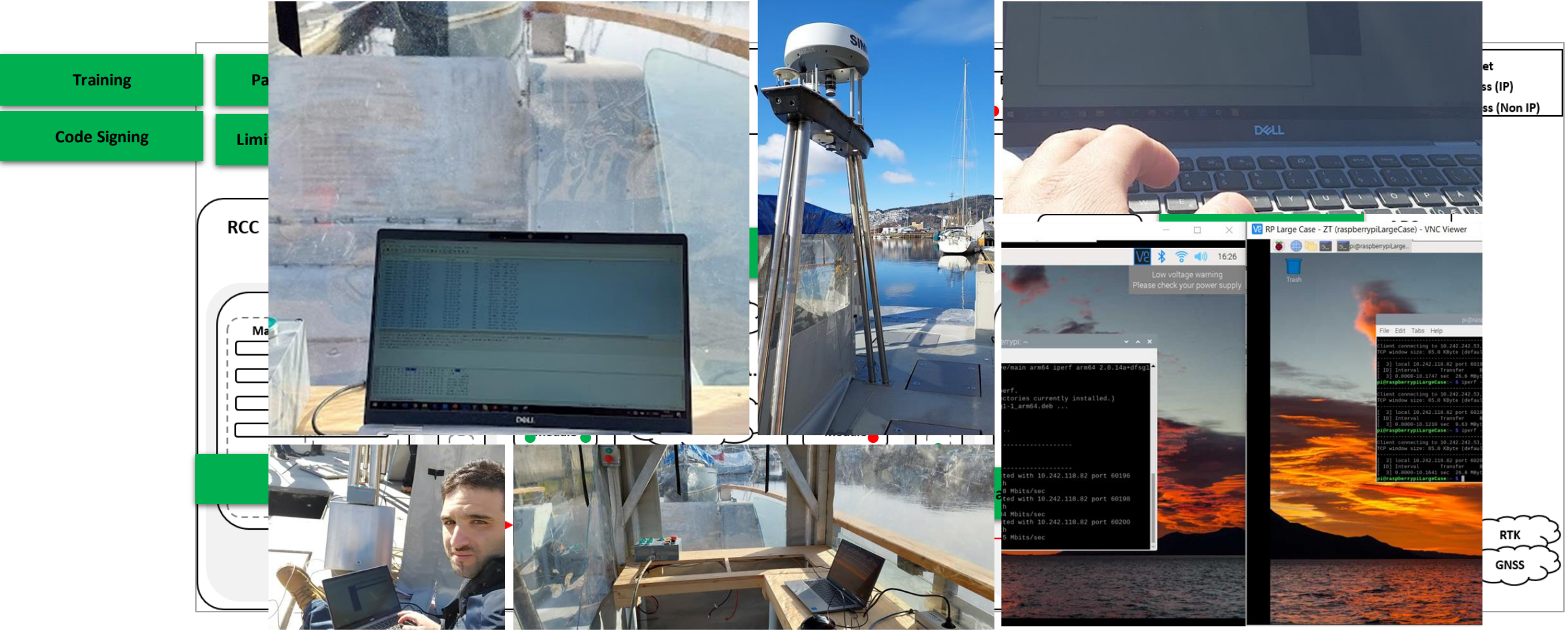


AIS Network

Vessel tracking services relay on messages from Automatic Identification System (AIS) [3] communicated over a heterogeneous AIS network

Sørensen, K. A. (2021). Automatic Identification System tracking of ships using Neural Networks and correlation with satellite images.





From Design to Application

Table 8: A summary of planned and executed tests in the adversary emulation process

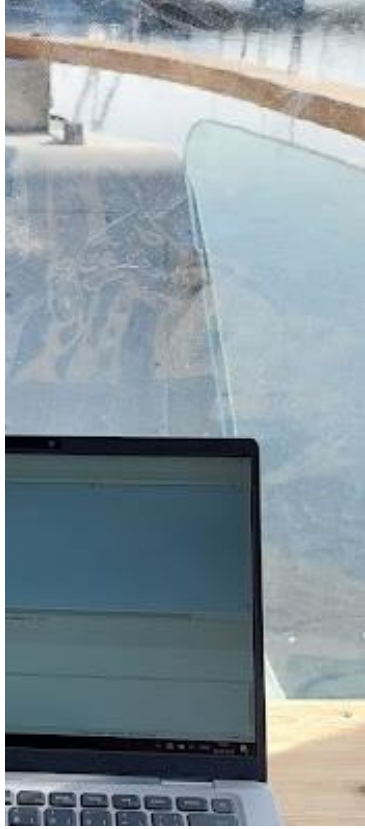
ATT&CK Tactic	Test objective	ATT&CK techniques	Test method	Results	Corrective action
Reconnaissance	identify remotely open services	Gather Victim Host Information (T1592), Search Open Websites/Domains (T1593)	Searching internet scanners (Shodan, Censys, and BinaryEdge) using the ferry's 5G router's public IP address	Only shodan identified an open port for an IP camera at some time in the past. The port was not open at the time of the test.	None
		Network Service Scanning (T1018), Remote System Discovery (T0846), Active Scanning (T1595)	Scanning the ferry's 5G router's public IP address using Nmap	2 open ports for the router remote authentication and signaling services	None
	Learn ferry network topology	Remote System Discovery (T0846), Active Scanning (T1595)	Using netdiscover to identify hosts and networks. This was only possible after gaining access to the network.	2 local networks were identified. One by the 5G router and another by a network switch. In total, 13 hosts were discovered.	NIDS tuning to detect network scanning,
	Discover vulnerabilities	Search Open Technical Databases (T1596)	Using the National Vulnerability Database (NVD) to search for vulnerabilities in the network components.	several vulnerabilities were found for one critical component [illegible] vulnerability has a 9.8 CVSS rating.	Updating the component to latest version.
Initial Access	gain access to the ferry network	Transient Cyber Asset (T0864) , Hardware Additions (T1200)	Insert a Raspberry Pi into the network	Sufficient controls exist providing physical security to mitigate this threat. However, permission to insert the Pi was granted to allow further tests.	NIDS tuning to detect newly installed devices in the network
	remotely access the 5G network	Valid Accounts (T0859), Default Credentials (T0812)	Assuming the attacker acquired the user credentials of the 5G network management platform. Using the stolen credentials to access the network.	The platform implements a 2FA service associated with an authenticator mobile application.	None
Collection	Sniff network traffic	Network Sniffing (T0842 or T1040)	Using Wireshark to sniff network traffic. Identify and collect navigation messages for planning further attacks.	Network traffic is captured at several intervals including NMEA messages emitted from the GPS and broadcasted within the network.	Limit access to resource over network
		Adversary-in-the-Middle: ARP Cache Poisoning (T1557.002)	Using Ettercap to run ARP spoofing attack to sniff unicast traffic between different hosts in the network.	Only ICMP messages between hosts were collected.	NIDS tuning to detect ARP spoofing
Execution	Run a script with several commands to collect host information	Hardware Additions (T1200), System Information Discovery (T1082)	Using a USB stick with customized autorun function	No permission was granted from the network vendor to run this test.	None*
Exfiltration	Transfer captured network traffic to a remote location.	Automated Exfiltration (T1020), Exfiltration Over Web Service (T1567)	Transferring the captured network traffic from the Raspberry Pi to a remote location.	Was conducted on several occasions without any obstruction.	Data Loss Prevention Solution
Discovery	Identify hosts and networks	Remote System Discovery (T0846), Active Scanning (T1595)	Using netdiscover to identify hosts and networks.	2 local networks were identified. One by the 5G router and another by a network switch. In total, 13 hosts were discovered.	NIDS tuning to detect network scanning,
	Identify open services in the network	Network Service Scanning (T1018) , Remote System Discovery (T0846), Active Scanning (T1595)	Using Nmap to identify network services.	A lot of open services were discovered ranging from HTTP, HTTPS, FTP, SSH,RDP, telnet, and NFS.	NIDS tuning to detect network scanning,
Lateral Movement	Identify remote services that can allow lateral movement		Using Nmap to identify remote desktop services.	The majority of findings were related to well-known remote desktop software and network sharing service.	Updating the component to the latest version and enforcing a password policy
	Remotely access a host from another	Remote Services: Remote Desktop Protocol (T1021.001)	Using the identified RDP software, attempt to access other devices.	No permission was granted from the network vendor to run this test.	None*
	Using default credentials to access other components	Valid Accounts (T0859), Default Credentials (T0812)	Using default credentials found online for accessing network devices.	2 devices were found [illegible] the default credentials [illegible]	Enforcing a password policy
Command & Control	Establish C&C channel between a victim and a remote C&C server	Encrypted Channel (T1573)	Using a covert channel software (e.g. Recub) run a client on a host in the network and run the server on a remote location.	No permission was granted from the network vendor to run this test.	None*
Credential Access	Identify default or weak passwords	Brute Force (T1110)	Using Metasploit to brute force open network services.	No permission was granted from the network vendor to run this test.	
	Sniff credentials	Network Sniffing (T0842 or T1040)	Using Wireshark to sniff network traffic. Identify and collect credentials.	No credentials were identified. Several display filters were used. However, no network traffic was found for known remotely accessible services.	None**
Persistence	Access other hosts in the network to maintain a foothold	Remote Services: Remote Desktop Protocol (T1021.001)	Using the identified RDP software, attempt to access other devices.	No permission was granted from the network vendor to run this test.	None*
Defense Evasion	Will the network scanning be detected	Network Service Scanning (T1018) , Remote System Discovery (T0846), Active Scanning (T1595)	Using Nmap to scan the network with different configurations ranging from aggressive to polite scans.	Aggressive scans were detected and stopped. Polite scans were not stopped. The status of the detection is unknown.	NIDS tuning to detect network scanning,
	Changing the IP address	Fallback Channels (T1008)	Manually configuring the IP address of the Pi.	When the scans were stopped, the Pi lost access to the network. However, access was regained after manually changing the IP address.	NIDS tuning to detect IP changes in the network
Privilege Escalation	Gain administrative privileges using operating system vulnerabilities	Abuse Elevation Control Mechanism (T1548)	Run a pre-built malware.	No permission was granted from the network vendor to run this test.	None*
Impair Process Control	Modify control parameters	Manipulation of Control (T0831)	Using Ettercap, manipulate control commands in the network		
Inhibit Response Function	Drop navigation messages	Denial of View (T0815)	using Ettercap filters to drop some navigation messages (NMEA)	Attack did not succeed.	None**
Network Effect	Manipulate network traffic	Manipulation of View (T0832)	Using Ettercap, manipulate some navigation messages (NMEA)	Attack did not succeed.	
	Jamming GPS data	Denial of View (T0815), Network Denial of Service (T1464)	Using GPS jammer to impact positioning data collection.	Future work	
Remote Service Effect	Obtain device backups stored remotely	Obtain Device Cloud Backups (T1470)	Obtain online stored configurations of hosts.	The configuration files of the 5G routers are secure with 2FA authentication.	None
Impact	Manipulate network traffic	Manipulation of View (T0832)	Using Ettercap, manipulate some navigation messages (NMEA)	Attack did not succeed.	None**
	Stealing operational information	Theft of Operational Information (T0882)	Identifying proprietary information from the network traffic	Proprietary information was identified in the network traffic related to the vendor's navigation system.	Limit access to resource over network

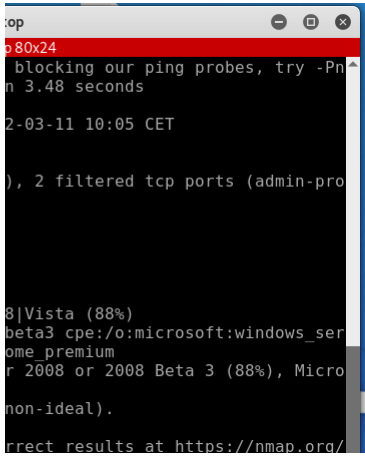
* none at the moment due to lack of information as a result of not allowing to run the tests.
** none at the moment due to lack of information as a result of insufficient testing. Additional testing in the future is needed.

Vulnerability

Vulnerabilities

Vulnerabilities





Project Impact

Cybersecurity Education and Awareness

Master-level courses

Industrial webinars

Master projects (4 completed)

System and Technology Development

Communication and cybersecurity solutions for:

- Autonomous ferry (milliAmpere2)
- Shore Control Lab (SCL)

Research

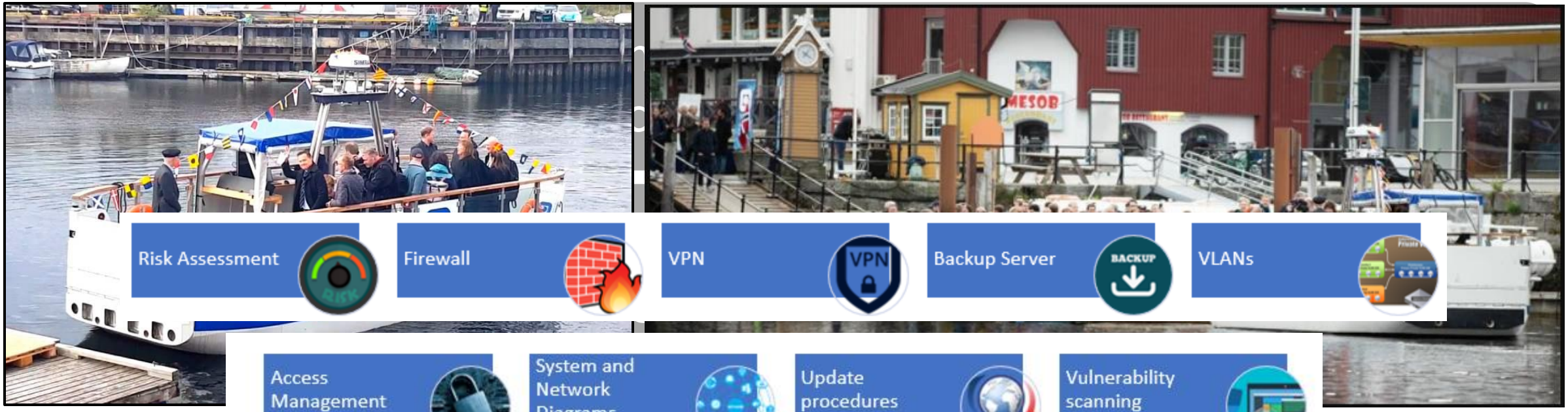
Publications (6 journal, 4 conferences)

Collaborations

Clear future directions

Conclusions (Final Remarks)

The ferry has demonstrated success in trials involving existing communication technologies.



Thank you for your attention

Ahmed Amro – (ahmed.amro@ntnu.no)