The Communication and Cyber Security of an Autonomous Passenger Ferry, 4 years Project

Critical Infrastructure Security and Resilience Group
Dep. of Information Security and Communication technology

Ph.D student: Ahmed Amro, ahmed.amro@ntnu.no

Supervisor: Sokratis K. Katsikas

Agenda

- Autonomous Navigation and Autoferry
- Project goals
- Related Work
- Communication Architecture
- Cybersecurity Mission Objectives
- Communication and Cybersecurity testbeds for Autonomous vessels.
- Progress

Autonomous Navigation

- 50% of global shipping companies will implement autonomous ships by 2050 [1].
- Trondheim was stamped by EU as smart city aiding the development of autonomous ships through the smart transportation domain [2][3].
- Autoferry project targets the development of passenger smart transportation in urban water.

[1] N. S. Association et al., “Maritime outlook 2018,” Report March, 2018.
[2] https://www.trondheim.kommune.no/trondheim-blir-smartby/
[3] https://www.sintef.no/en/latestnews/test-site-opens-for-unmanned-vessels/

Autoferry

Intended to be an alternative for a high-cost bridge. Bridge estimated cost 42 million kroner, compared to 1.5 million kroner for a life cycle of 15 years for the autonomous ferry [1].

Specifications:

- On-demand passenger ferry
- Max 12 persons + bicycles
- Electrical propulsion, battery
- Inductive charging at quay

[1] Havdal, G., Heggelund, C. T., & Larssen, C. H. (2017). *Design of a Small Autonomous Passenger Ferry* (Master's thesis, NTNU).

Autoferry stand on Ocean Week 2019

Autoferry: Project Goals

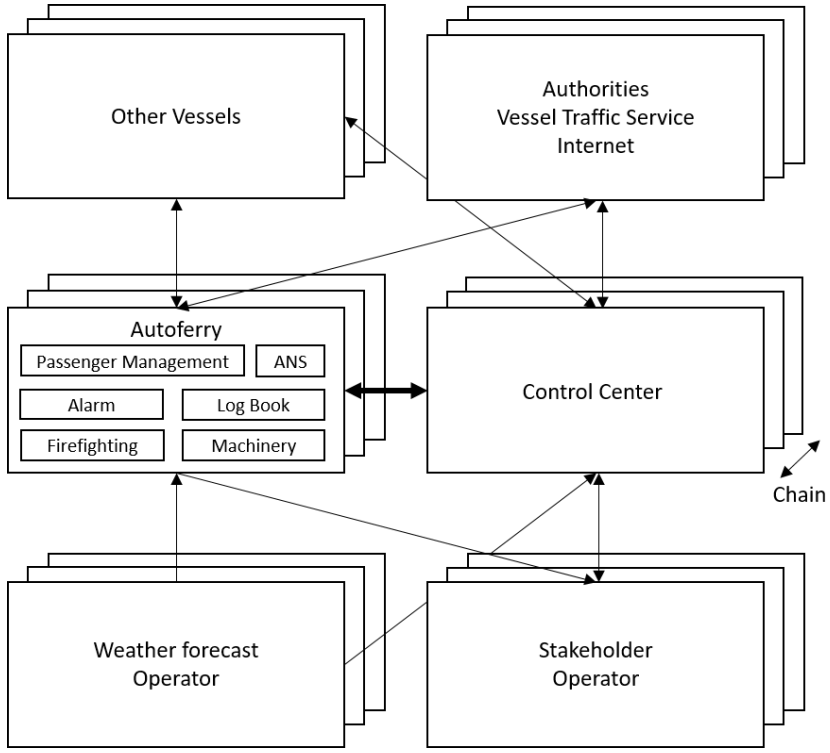
1. Define and implement a suitable communication architecture that:
    a. Complies with regulations and standards.
    b. Satisfies functionality, safety and cybersecurity requirements.
2. Apply a suitable risk assessment method in order to identify potential risks.
3. Elicit and integrate cybersecurity mechanisms required to enforce security policies.
4. Provide risk management capabilities through the design and implementation of a standard-aligned Integrated Ship Safety and Security Management System (IS3MS).

Related Work

- Autonomous vessel development
  - **Autoferry master project**: Shedding light on the Autoferry background and motivation.
  - **Autonomous vessel steering**: agent-based system distributing navigational rules between vessels and control center.
- Maritime communication
  - **MUNIN**: Relative deliverables, some requires to be adapted for urban transportation.
  - **NetBaltic** project: Design approach for non-satellite wireless communication system.
  - **Bureau Veritas**: Guidelines for autonomous shipping risk assessment, functions, and reliability.
- Maritime Cybersecurity
  - Maritime specific PKI, CySiMS, mIBC and MMSI.
  - NIST Implementation by United States Coast Guard and BIMCO.
  - **MaCRA**: model-based risk assessment framework was developed to assess risks related to autonomous vessels.
  - No work published yet on IS3MS for autonomous vessels.

Autoferry: Communication Architecture

- Development of a heterogeneous communication network with suitable hierarchy, modular and flexible design, to achieve reliability and resiliency.
- Influenced by on MUNIN's communication architecture and Cisco network design principles.
- Complies with regional and international regulations and standard. Such as the International Maritime Organization **IMO**, and Norwegian Maritime Authorities **NMA**.
- Satisfies Bureau Veritas and DNV-GL functionality and reliability requirements for vessel operators and manufacturers.



Communication Flow Diagram

Autoferry: Cybersecurity Mission Objectives

- With increased connectivity comes increased cyber threats.
- Targeted cybersecurity mission objectives:

1. **Maintain Cyber Situational Awareness**: the understanding and assessment of cyber risks and threats, in addition to maintaining system parameters within the operational norms.
2. **Maintain Secure Communications**: most of the operational requirements of safe and autonomous navigation require the availability of reliable and secure communication.
3. **Maintain Secure Trip Management**: Secure coordination between several entities is required for route and passenger management.
4. **Maintain Regulatory Compliance**: Sustaining reliable operational activities whilst complying with relevant regulation must be achieved.

Autoferry: NIST Framework Profile

United States Coast Guard maritime NIST profiles:

1. Maritime Bulk Liquids Transfer.
2. Offshore Operations.
3. Passenger Vessel.

23 108

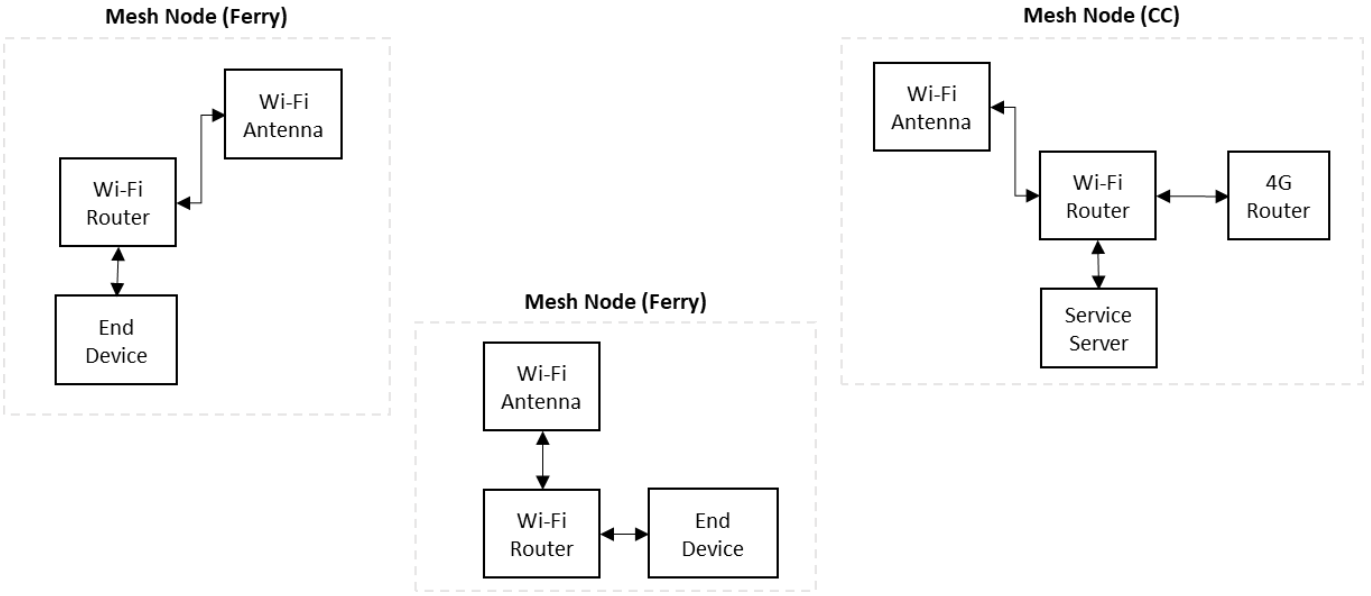
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

Content for USCG NIST implementation can be found in http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/.

Communication and Cybersecurity Testbeds for Autonomous Vessels

1. **Wireless Communication testbed**: to evaluate the communication architecture against the operational requirements in several scenarios, a testbed will be implemented, that will provide measurements related to wireless communication coverage, bandwidth, latency, etc.



Communication and Cybersecurity Testbeds for Autonomous Vessels

2. **Cybersecurity testbed**: to evaluate overall system cybersecurity preparedness against selected attack scenarios another testbed will be implemented by emulating autonomous ship and control center interconnected components.

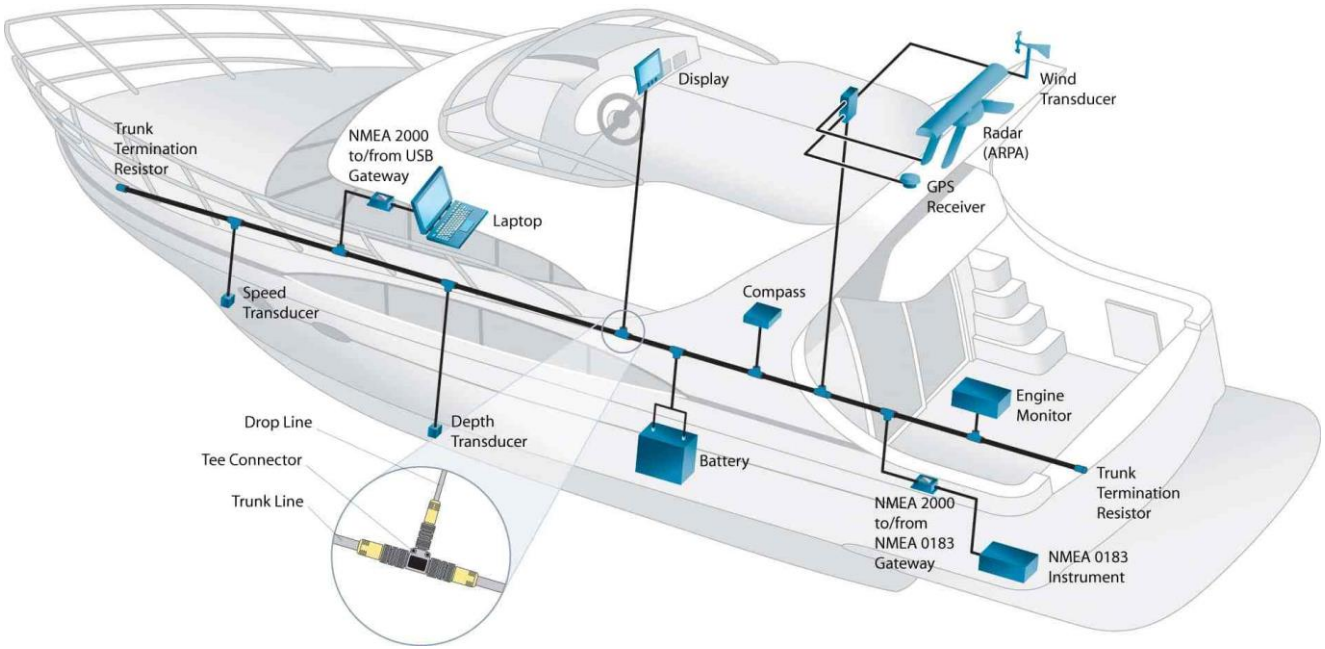


Image source [link]

Progress

Tasks	Start	Duration (months)	Year 1				Year 2				Year 3				Year 4			
			Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Work Package 1																		
State-of-the-art	1	6																
Work Package 2																		
Design and Implementation of Autoferry Communication Architecture	7	6																
Design and Implementation of Wireless Communication testbed	13	3																
Work Package 3																		
Cybersecurity related assets and risk assessment	16	3																
Cyber Security Protection mechanisms, and Attack modeling	19	3																
Cyber Security Detect, Response, and Recovery Mechanisms	25	6																
Implementation of Cybersecurity testbed and Attack Scenarios	31	6																
Validaion of results	34	3																
Work Package 4																		
Implementation of the IS3MS	37	6																
Evaluation of the IS3MS	43	3																
Work Package 5																		
Thesis write-up	46	3																

Thank you!
Questions?

ntnu.edu/autoferry