Fraunhofer CML

Fraunhofer Center for Maritime Logistics and Services CML

Cybersecurity Testing & Training with Bridge Equipment in a Lab

Dr.-Ing. Anisa Rizvanolli
December 7, 2023

The Fraunhofer Society and the Fraunhofer CML

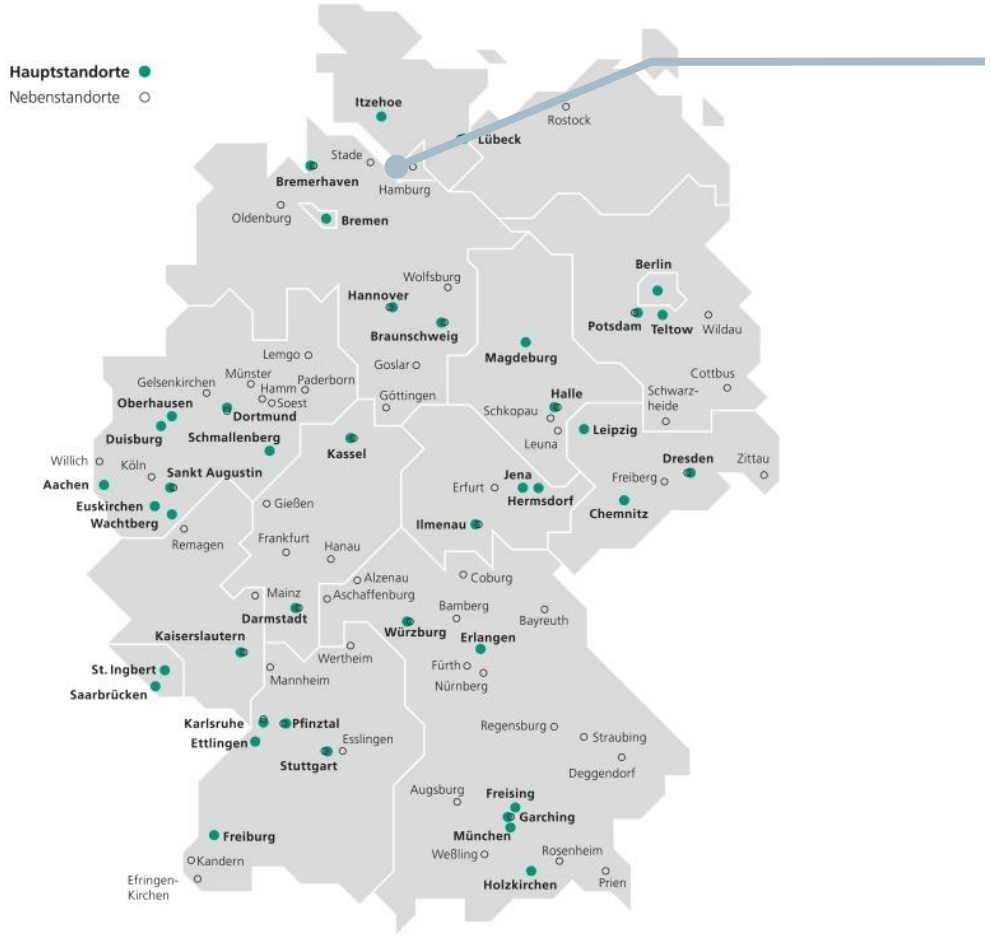
Applied Research for Economy and Society

Fraunhofer Society

30.000
Staff

76 Institutes
and research units

2,9 Bio. €
Financial volume



Fraunhofer CML, Hamburg

2010
Foundation in Hamburg

Focus on application-oriented research for the maritime industry

Cooperation with Institute of Maritime Logistics of TUHH

Fraunhofer CML: Innovating the Maritime Sector

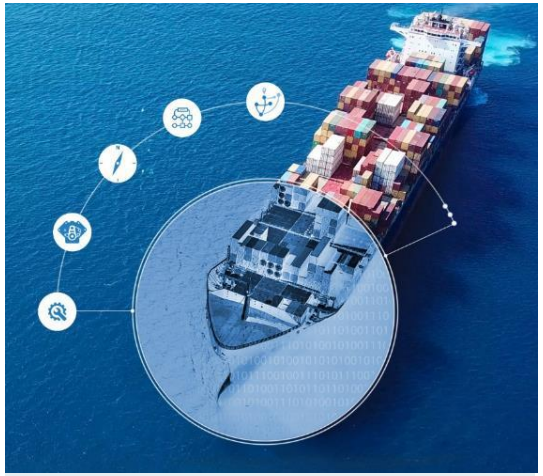
Fields of Research

Ports and Transport Markets

Analysis and optimization of nodes in the maritime supply chain

Sea Traffic and Nautical Solutions

Technologies for autonomous systems and nautical assistance systems



Ship and Information Management

Software development with focus on digital solutions for fleet management, ship operation and maritime services

Port Technologies

Mobile robotics and AI for new application areas in port operations

Background

Why Cybersecurity?

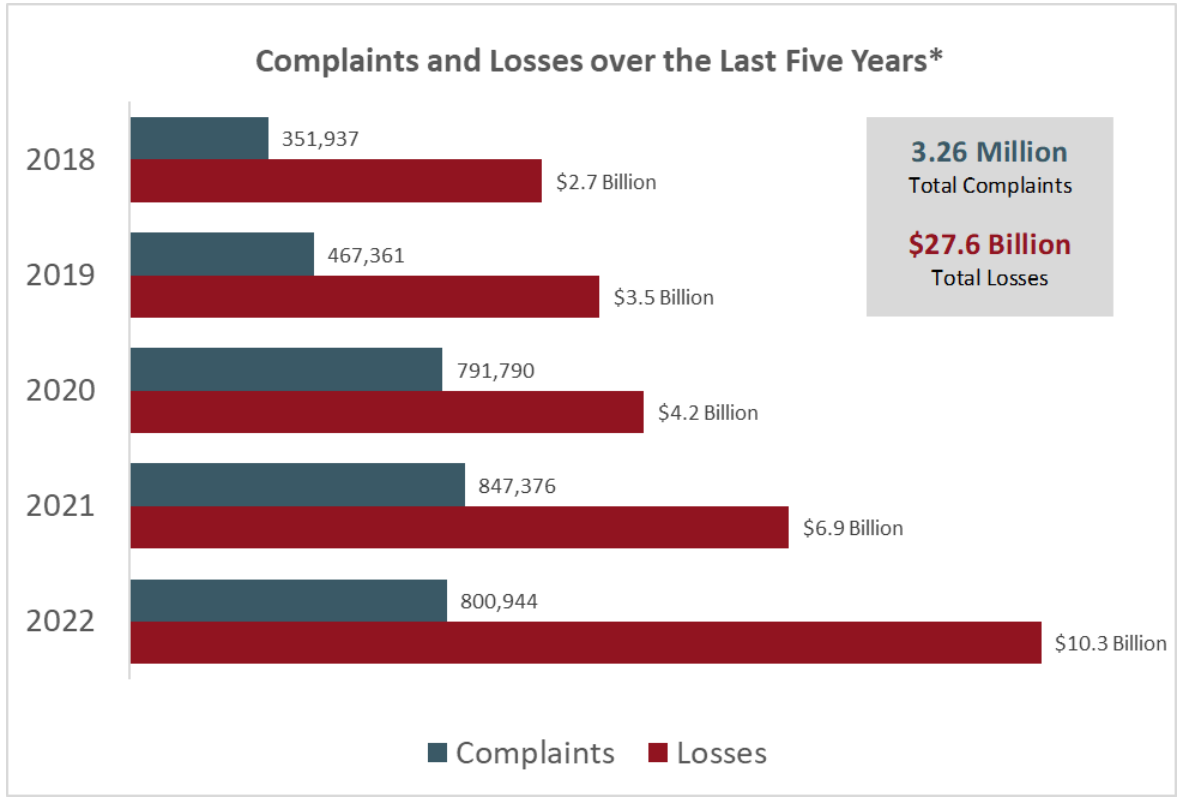
Fraunhofer CML

Why Cybersecurity?
Recent Developments

Growing number of interconnected devices
- LEO: internet fast and available
- Bring your own device
- Operational technology (OT) + IT

Higher automatization
- Machinery: optimization through software
- IP and serial networks together
- Moving toward decision support systems and unmanned shipping

Cyber attacks increasing in total
- Higher frequency and more costly
- Ransomware: largest threat
- Ships often hit "on accident"
- No insurance coverage
- Ships have a relative long life-time



FBI, Internet Crime Complaint Center, Internet Crime Report 2022

Fraunhofer CML

Why Cybersecurity?
Regulatory Requirements

IMO : Safety Management Systems
- Include cyber security measures into the SMS
- Main target: existing ships
- Operative measure
- Still lack of awareness among seafarers

IACS: Uniform Requirements E26/E27
- Minimum set of req. for cyber resilience capabilities
- Target: new ships and system manufacturers
- New builds after July 1st 2024
- E26: focus on 5 central requirement categories

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Current Situation
- Regulations describe **What to do**
- But not **How to**

The Bridge Laboratory

Implement Cybersecurity

Protect Against Cyber Incidents

Test your protection strategy

- Install new devices
- Change network topology
- Develop new approaches

Risk assessment

- Perform attacks
- Analyze system behavior

Validate awareness

- 81% of the seafarers feel they need training on advanced digital technologies
- Enable training in real-world environment
- Higher impact and focus on the most relevant topics

Fraunhofer CML

Detect & Respond to Cyber Incidents

System monitoring

- Based on risk assessment
- Intrusion detection systems
- Detect differences between normal behavior and incident

Enhanced alarms systems

- Providing the right information
- Not overloading the system
- Minimizing stress for the seafarer

Real data for

- Better monitoring
- Validation of the respond approaches
- Conducting test and preparing for the worst case

Fraunhofer CML

Fraunhofer CML

Fraunhofer Center for Maritime Logistics and Services CML

Contact

Dr.-Ing. Anisa Rizvanolli
Ship and Information Management
Tel. +49 40 2716461-1401
anisa.rizvanolli@cml.fraunhofer.de