Fraunhofer
CML

Fraunhofer Center for Maritime
Logistics and Services CML

Maritime Cybersecurity Lab (MaCy)

Testing Cybersecurity Safely in the Laboratory

© Fraunhofer CML

Maritime Cybersecurity Lab at Fraunhofer CML

Cyber risk in shipping has increased dramatically in recent years. In addition to the security of the individual components on board, the network topology also has a significant impact on the cybersecurity of a ship.
Due to limited resources, it is a major challenge for both integrators and shipping companies to conduct cybersecurity tests for different topologies and components.

For existing systems, for example, the following questions arise:

How can I ...

... identify individual security risks in each system?

... assess the overall cyber resilience of the ship?

... assess the cybersecurity of a new device or its configurations?

... test the functionality and security of different network topologies?

... develop best practices and test them immediately?

The new CML research building with antenna system

The new research building of the Fraunhofer CML in Harburg's inland harbour is also called a "stone ship" because of its external appearance.
In fact, it also has characteristics of a real ship due to its unique technical features.

The radio laboratory replicates an actual ship bridge that is connected to an antenna platform providing real-time data – with a design that is found on about 70 percent of seagoing vessels.

In the CML radio and bridge laboratory, we do not simulate, but work and research with real data

Potential customers such as device manufacturers and software developers can use this laboratory, for example, to have their products tested for cybersecurity:

This way, you can have your software attacked "safely" – without the risk of compromising your own data.

Our approach:

- Lab with key bridge components, a configurable network and real-time data software-based tools to simulate different attacks
- Identification of technological, regulatory and procedural needs
- Development of a structured methodology for maritime cyber risk assessment
- Creation, testing and validation of holistic cybersecurity concepts for individual components or bridge systems

Our offer

- Cybersecurity assessment
- Response & Recovery Plans
- Policy Development
- Personell Training

This is possible with our radio and bridge laboratory, which combines an antenna platform with complete and certified bridge equipment. With this, we offer in detail:

- Restoration of on-board configuration in our bridge lab
- Tests of current equipment and network topology
- Tests of new devices or different network topologies
- Systems to carry out cyber attacks in an automated and user-friendly way
- Carrying out penetration tests
- Incident detection
- Role definitions
- Response plans and trainings

... and all this without having to dock the ship yourself.

Contact

Dr.-Ing. Anisa Rizvanolli
anisa.rizvanolli@cml.fraunhofer.de
+49 40 271 6461 - 1401

M. Sc. Philipp Sedlmeier
philipp.sedlmeier@cml.fraunhofer.de
+49 40 271 6461 - 1413

Fraunhofer CML

Fraunhofer Center for Maritime Logistics and Services CML

Blohmstr. 32
21079 Hamburg
Germany

info@cml.fraunhofer.de
www.cml.fraunhofer.de