

update:me, 09. September 2024



Cybersicherheit für die Schifffahrt

Mit einer Schiffsbrücke als Test- und Entwicklungslabor

Philipp Sedlmeier, Fraunhofer CML

Cybersicherheit für die Schifffahrt

Inhalt

1

Cybersicherheit im maritimen Umfeld

2

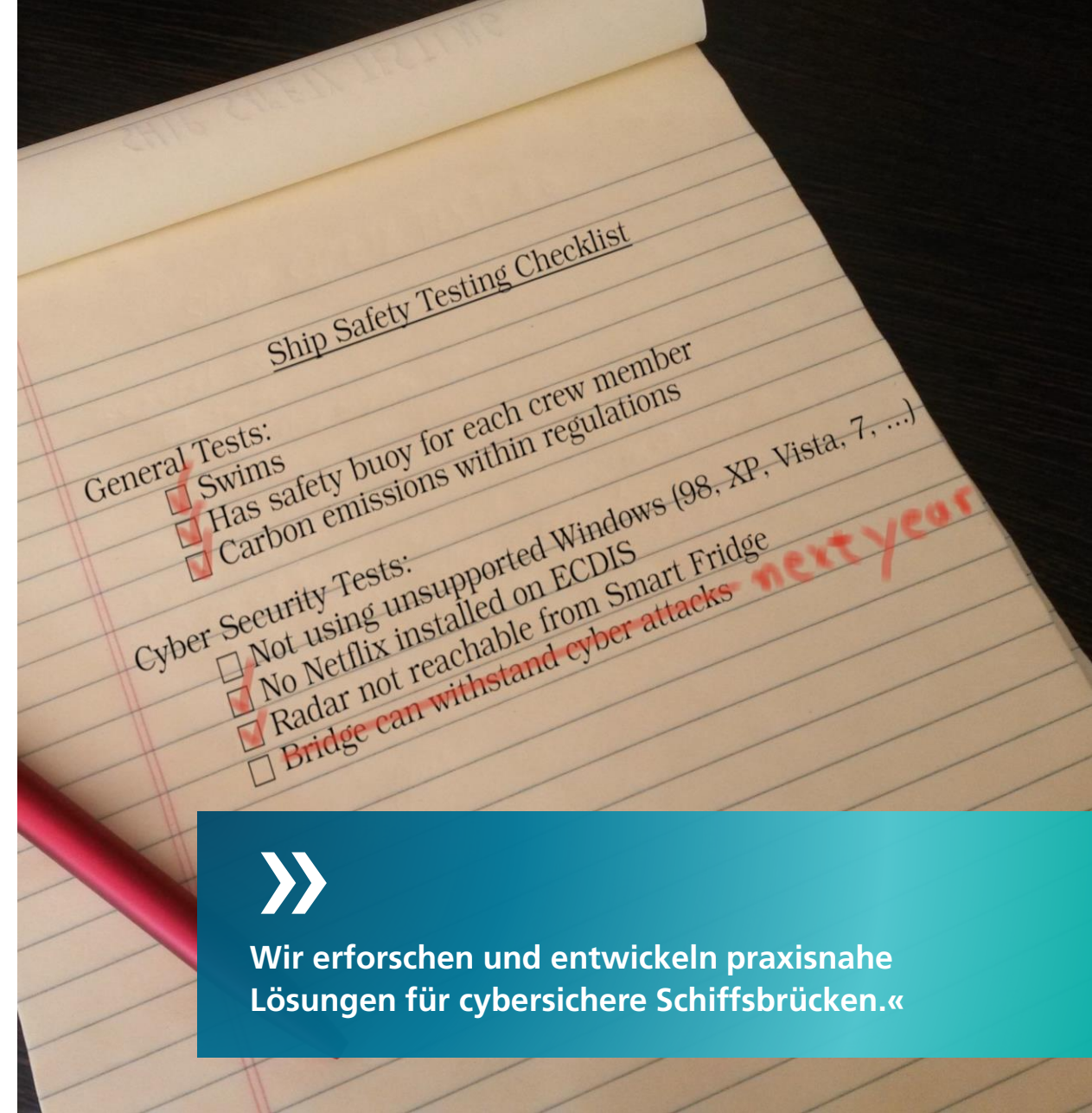
Bedrohungslage und Angriffsszenarien

3

Test- und Entwicklungsumgebung

4

Experimente und Ergebnisse



1

Cybersicherheit im maritimen Umfeld

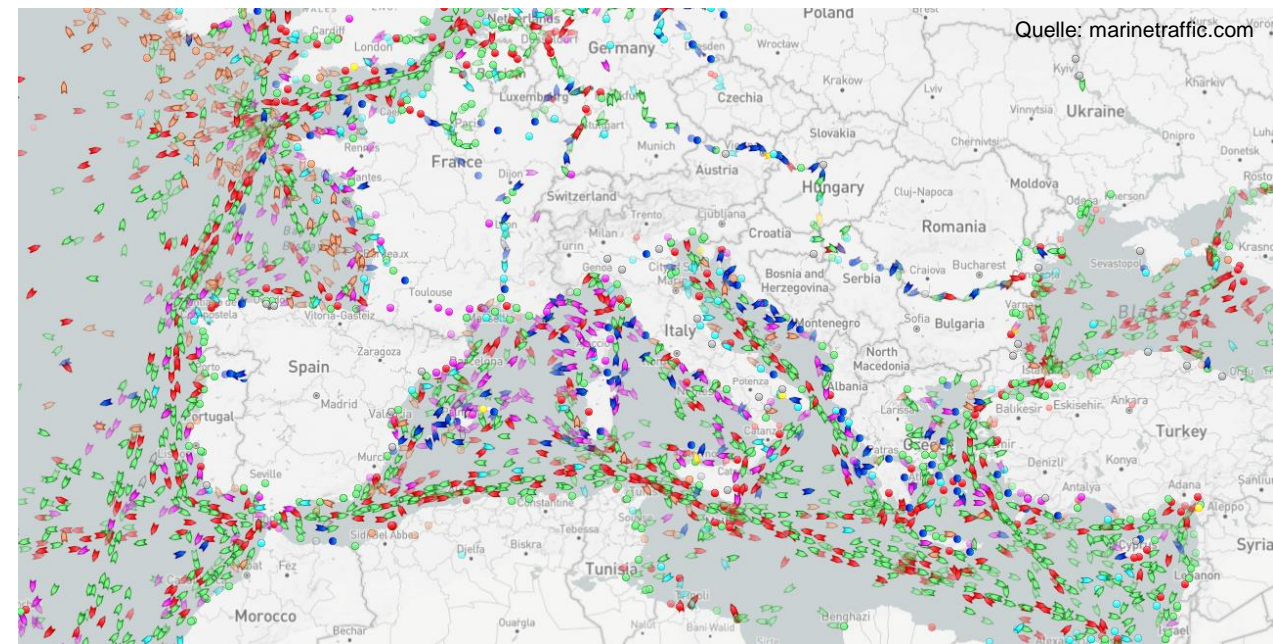
Cybersicherheit im maritimen Umfeld

Maritime Trends

- Die globale Lieferkette ist maritim
- UNCTAD's Review of Maritime Transport 2023:
- >80% des internationalen Handelsvolumens
- >12 Mrd. Tonnen pro Jahr
- 2% jährliches Wachstum bis 2028
- > 105.000 Schiffe mit über 2 Mrd. dwt Tragfähigkeit



© kees torn CC BY-SA 2.0



Cybersicherheit im maritimen Umfeld

Maritime Trends

- Abhängigkeit der Lieferketten vom maritimen Sektor
- Fortschreitende digitale Vernetzung
- Lange Lebensdauer der Schiffe
- Trend zu autonomen Systemen
- Menschlicher Faktor: Nautiker \neq Cyberexperten



Cybersicherheit im maritimen Umfeld

Regeln und Vorschriften

- Berücksichtigung von Cyberrisiken in Safety Management Systems
- Klassifizierungsvorschriften für Schiffsneubauten (UR E26 & E27 der IACS)
- Keine Abdeckung durch Versicherungen
- Momentan: Überarbeitung der Richtlinien für Maritime Cyber Risk Management durch IMO



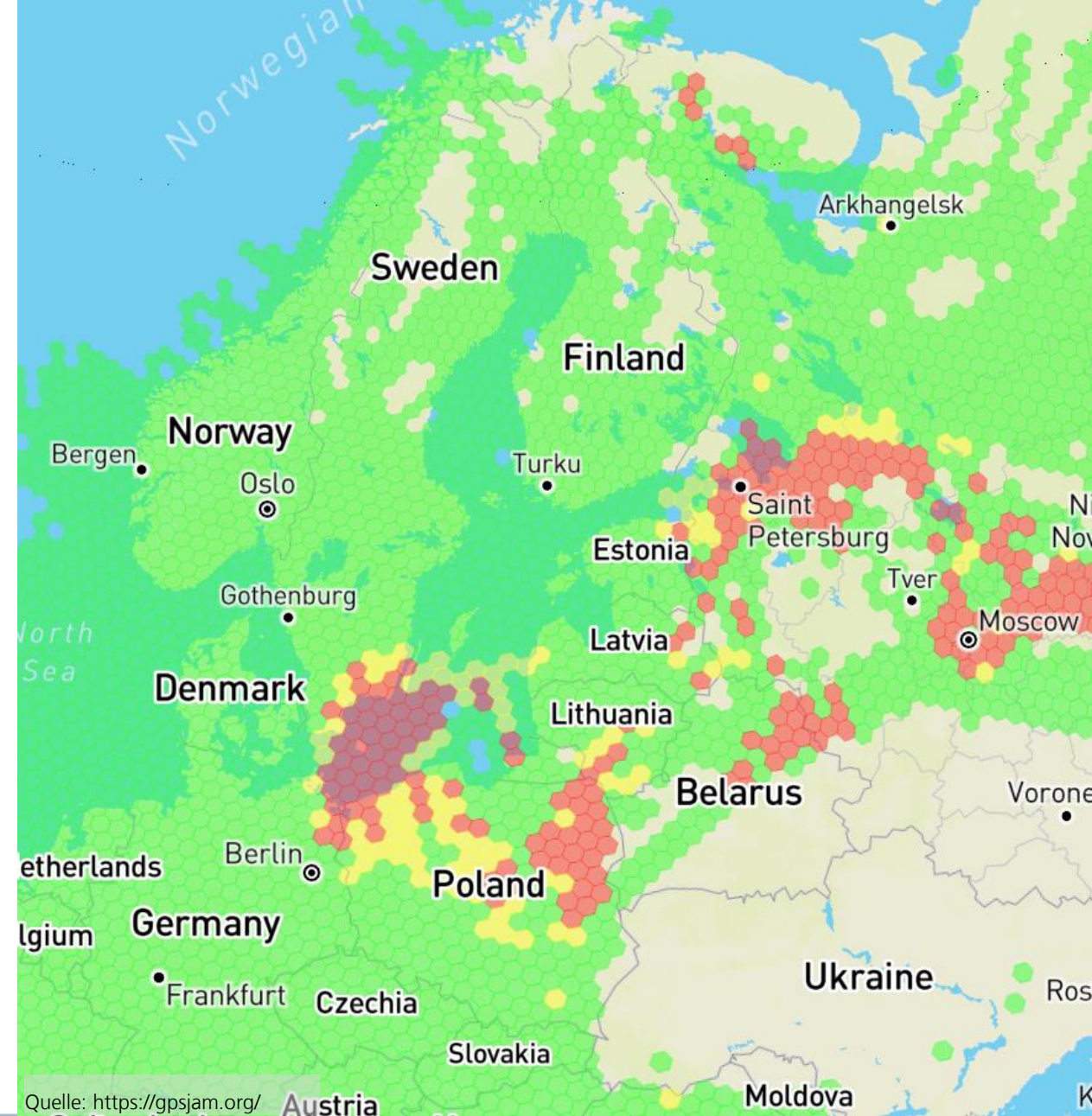
2

Bedrohungslage und Angriffsszenarien

Bedrohungslage u. Angriffsszenarien

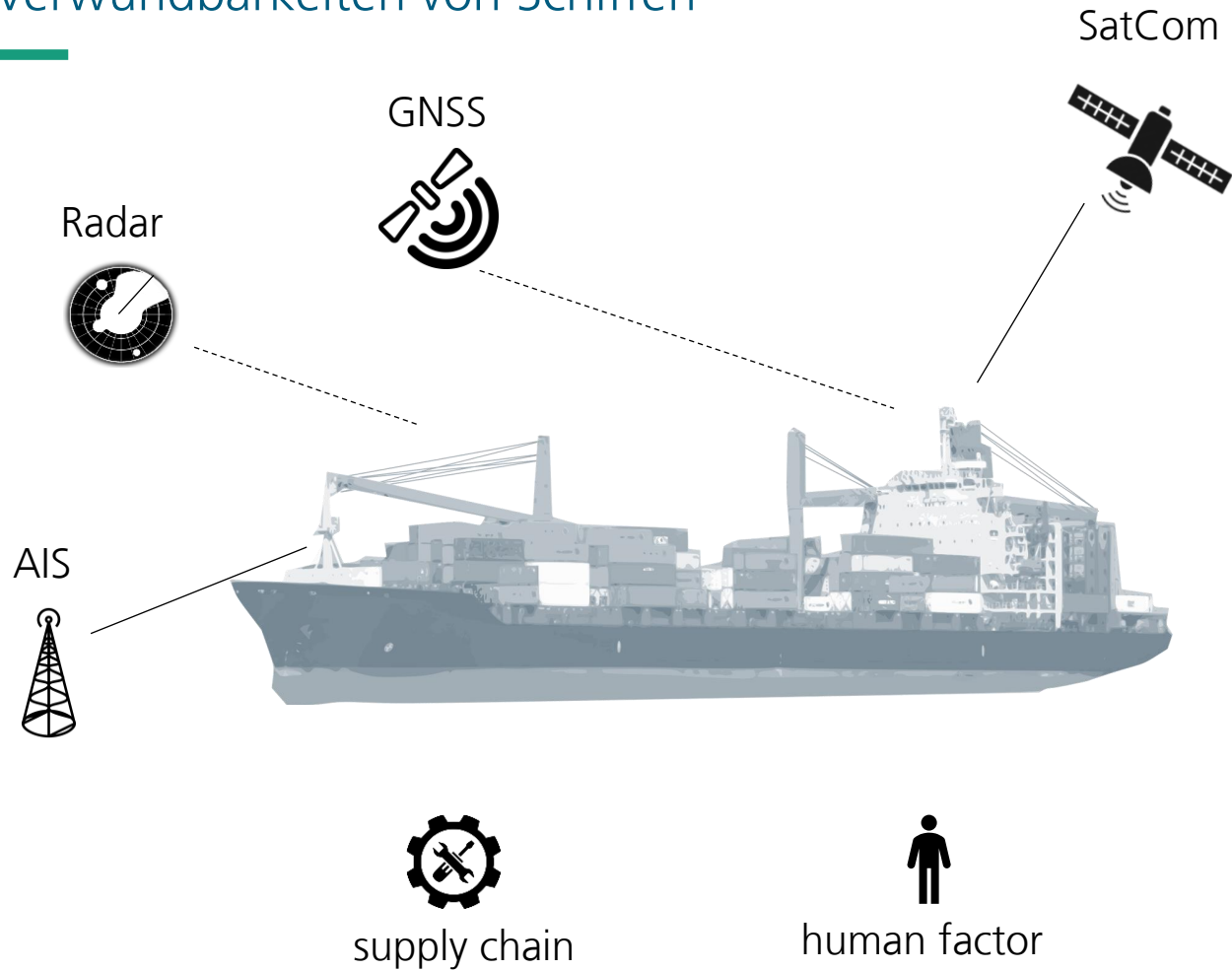
Maritime Cybervorfälle

- Vermutlich hohe Dunkelziffer
- Häufig ungezielte Angriffe durch Viren/Malware
- Gezielte Angriffe auf GNSS und AIS



Bedrohungslage u. Angriffsszenarien

Verwundbarkeiten von Schiffen



Quelle: Maritime Cyber Threat Research group, University of Plymouth



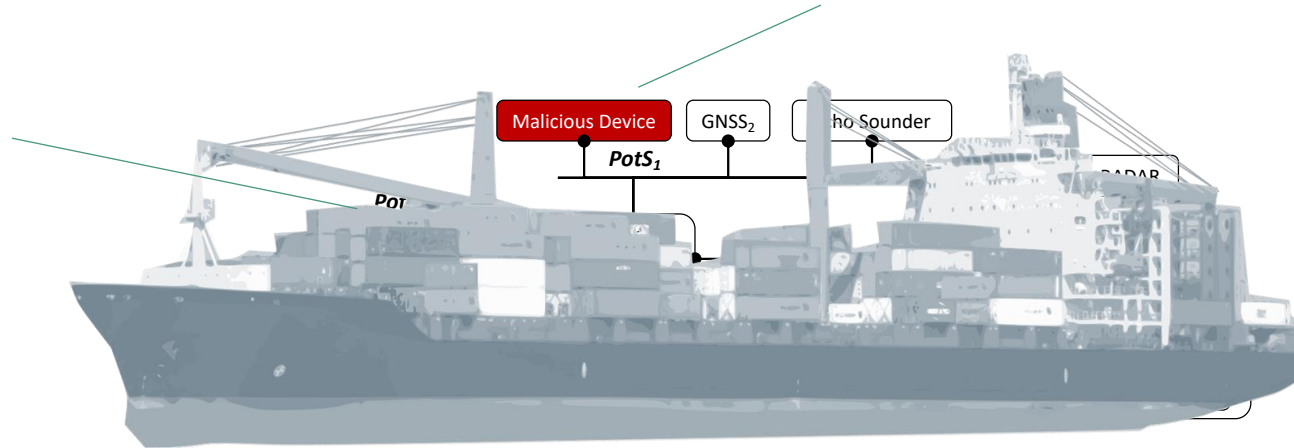
Quelle: wired.co.uk / Gurva Le Meur

Bedrohungslage u. Angriffsszenarien

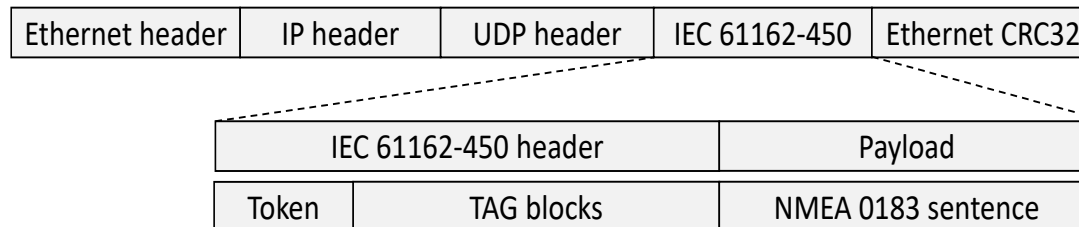
Fokus auf integrierte Brückensysteme

Malicious hardware
(infiltriertes Gerät)

Malware (human factor, supply chain, SatCom)



- Im Netzwerk



- NMEA Beispiel

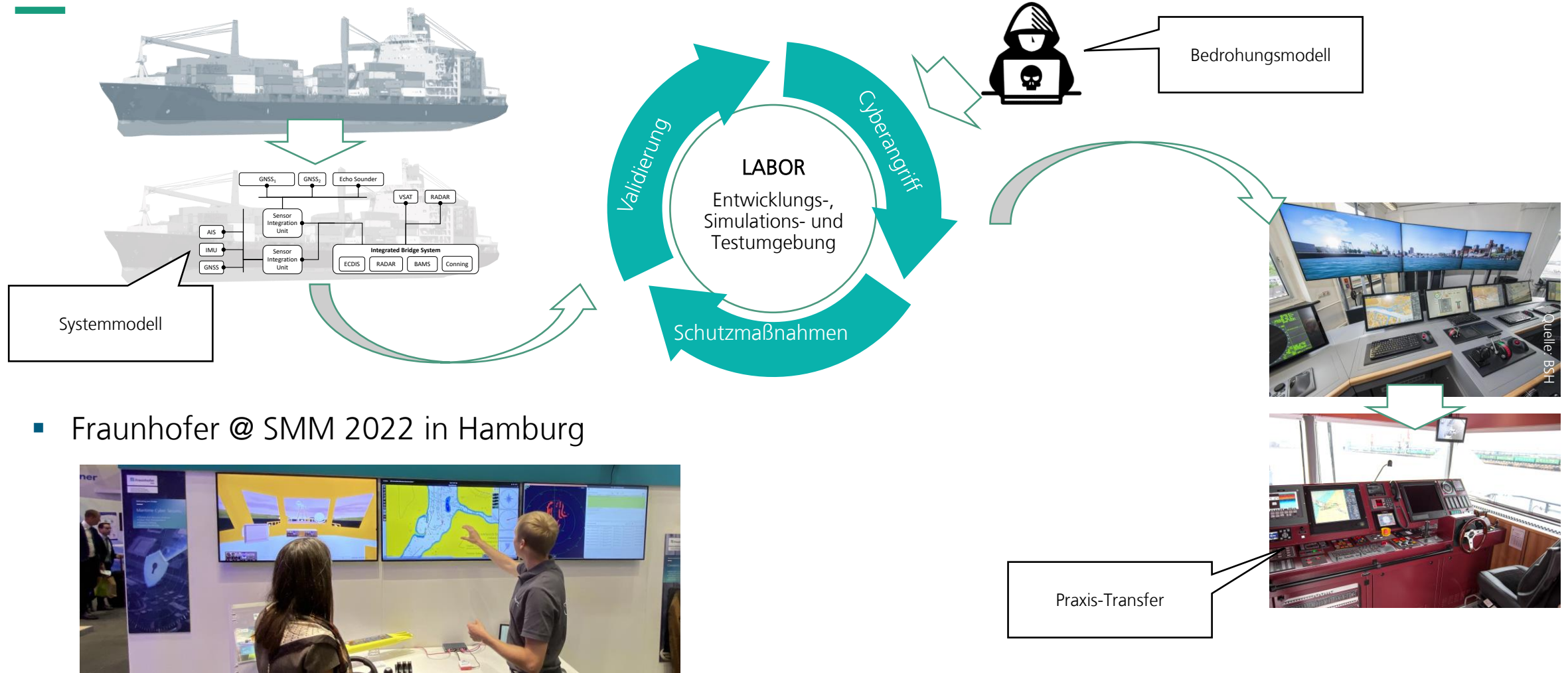
\$GPAPA,A,A,0.10,R,N,V,V,011,M,DEST,011,M*82

3

Test- und Entwicklungsumgebung

Test- und Entwicklungsumgebung

Vorgehen

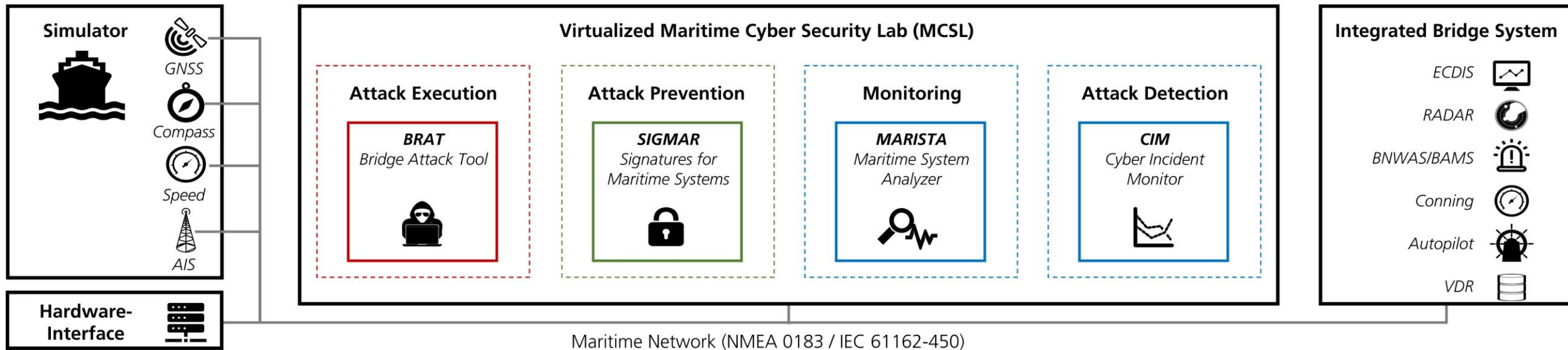


- Fraunhofer @ SMM 2022 in Hamburg



Test- und Entwicklungsumgebung

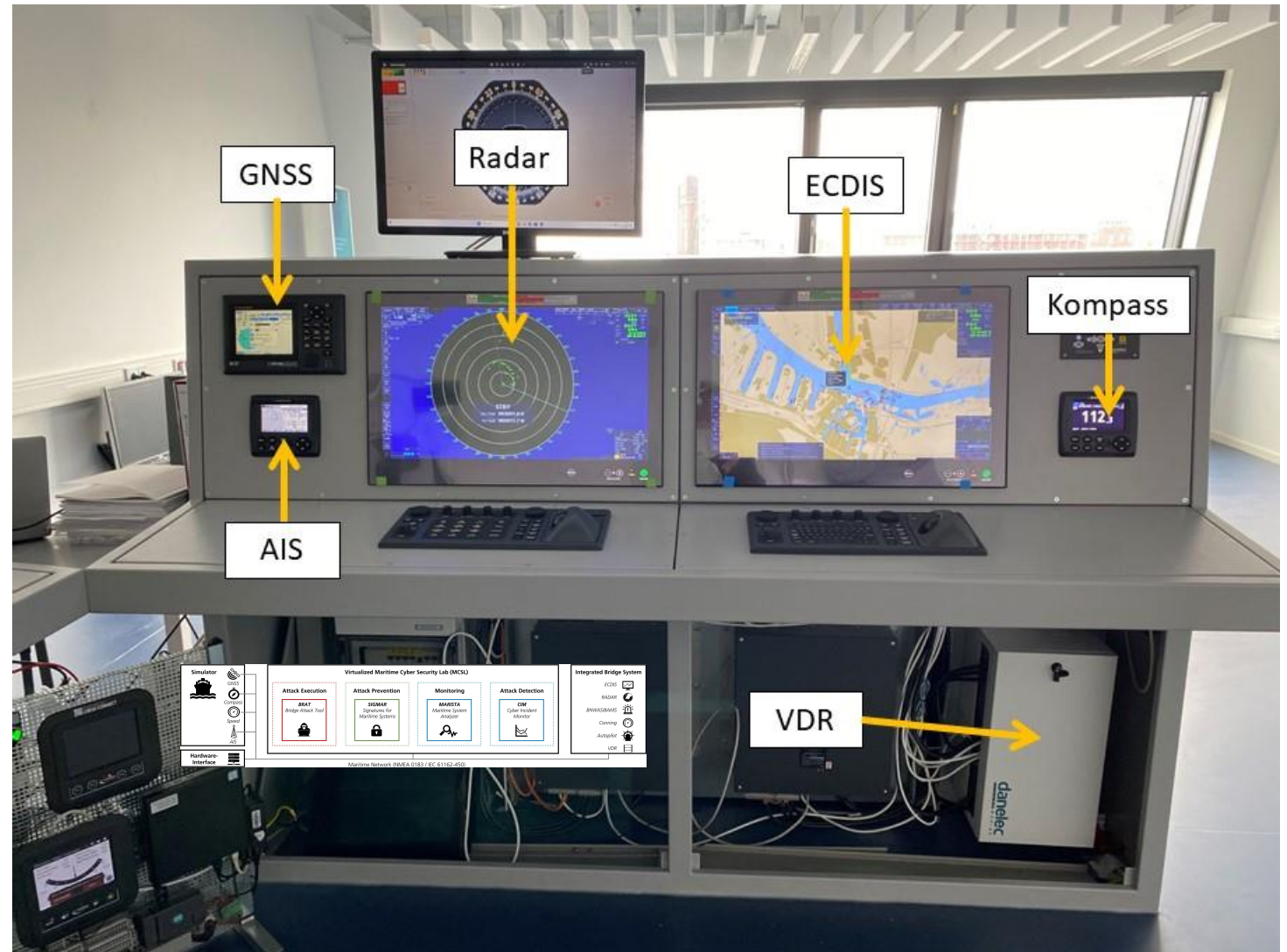
Softwarelösungen



Test- und Entwicklungsumgebung

Brückenlabor

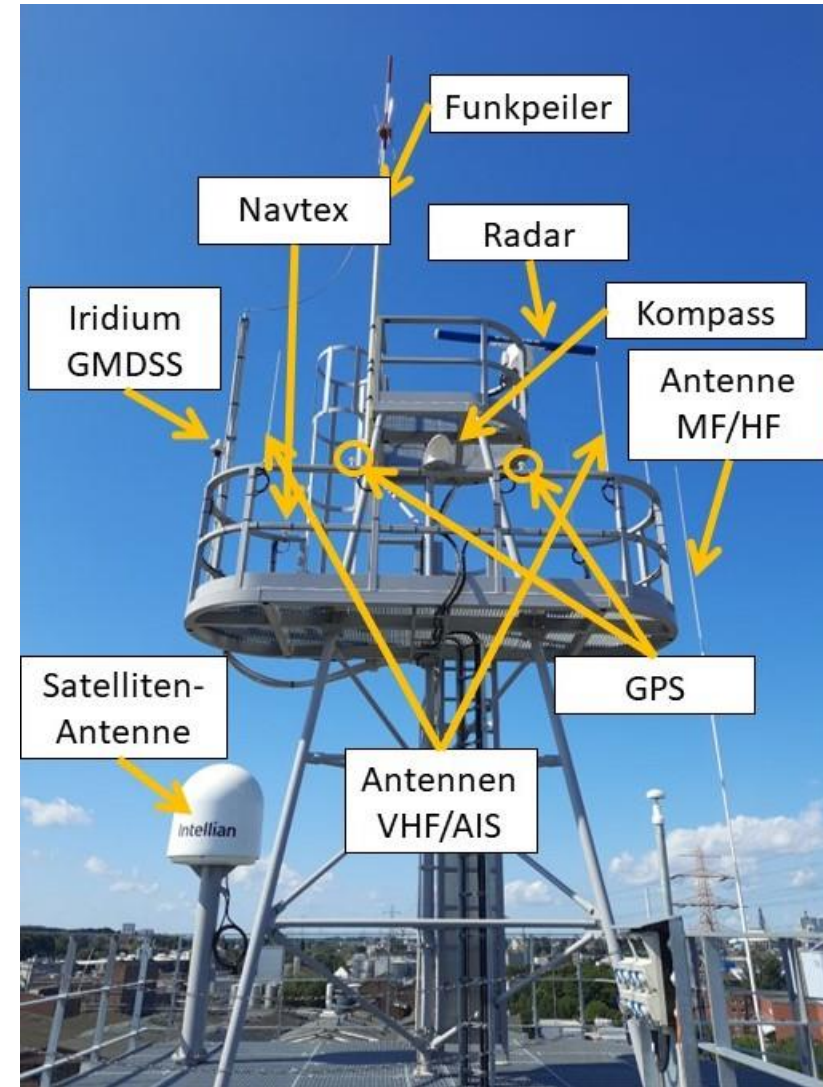
- Labor in realistischer Umgebung
- Austausch mit Nautikern
- Erprobung von Handlungsempfehlungen
- Feedback fließt direkt in Entwicklung ein
- Brückenlabor als Trainingsfazilität



Test- und Entwicklungsumgebung

Antennenplattform

- Jederzeit verfügbare Signale
- Verknüpfung zusätzlicher Geräte mit Antennenplattform
- Validierung von Strategien und Technik durch echte Daten



4

Experimente und Ergebnisse

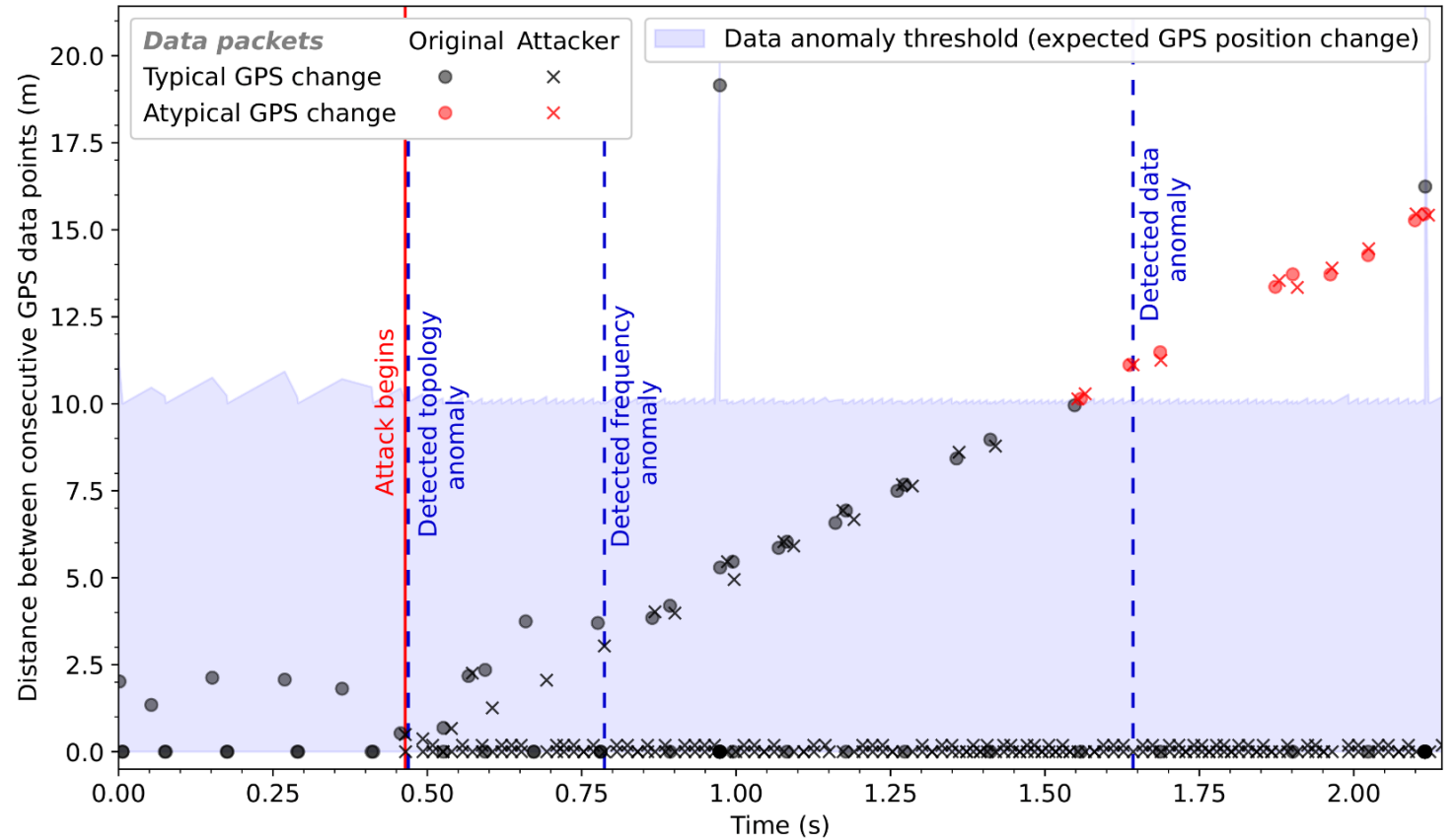
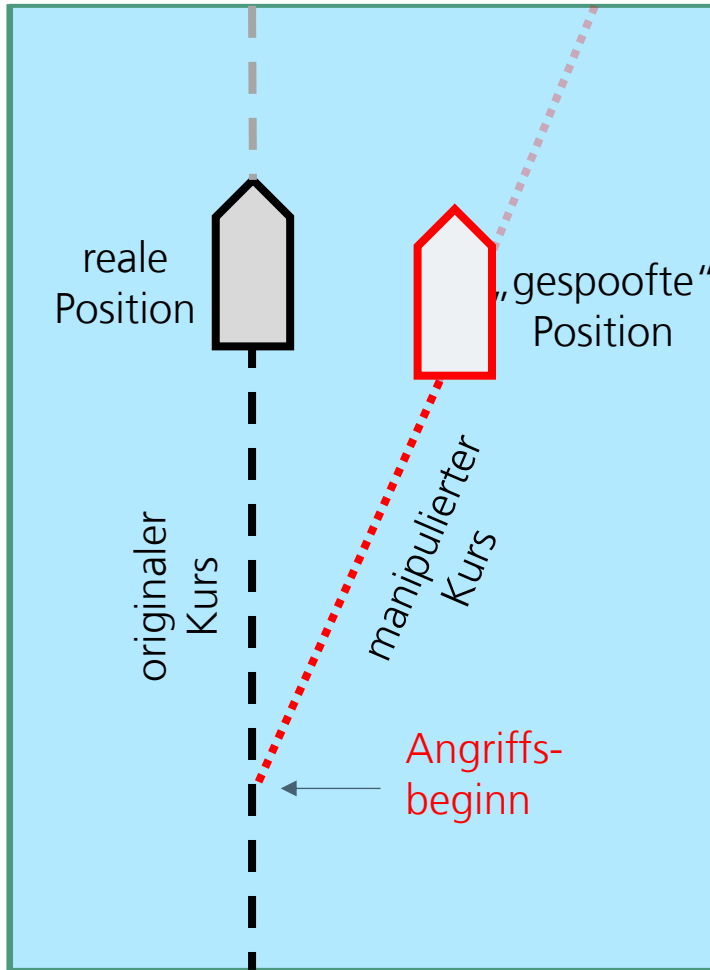
Experimente und Ergebnisse

AIS-Flooding-Angriff



Anomalie-Erkennung

Maritimes Intrusion Detection System



Cyber Incident Monitor

Ergonomische Mensch-Maschine-Schnittstelle

Aktive Cyber-Alarme

Alarm-Historie

The screenshot shows the 'Active Cyber Alerts' section of the CIM interface. At the top, there are three status indicators: 3 red triangles (alarms), 1 orange triangle (warning), and 0 green triangles (cautions). Below this is a table of active alerts:

Priority	Alert Title	Occurred Time (UTC)	ID	Alert Details	Supposed Source	ACK
Alarm	Manipulation of own ship GPS position	14 Jun 2022 13:10	009	Content differs between packages	GP (192.168.0.2:1337)	<input type="checkbox"/>
Alarm	Possible manipulation of own ship GNSS position and/or time	14 Jun 2022 13:09	008	Too frequent messages of type GLL	GP (192.168.0.2:1337)	<input checked="" type="checkbox"/>
Alarm	Possible manipulation of own ship GPS position and/or time	14 Jun 2022 13:09	007	Too frequent messages of type GGA	GP (192.168.0.2:1337)	<input checked="" type="checkbox"/>
Warning	Network/device misconfiguration	14 Jun 2022 13:08	006	Message has unknown attributes, unexpected source port for known	GP (192.168.0.2:1337)	<input checked="" type="checkbox"/>

Below the table is a 'Recommended Actions' section for alert ID 009:

- Do not trust GPS position information shown on any device (ECDIS, conning display etc.) except original sensor display.
- Do not trust information coming from stated network source device.
- Verify position if possible:
 - with original GPS sensor display
 - with other GNSS information (GLONASS, Beidou, LORAN-C, GALILEO)
 - by taking visual bearings
 - by taking bearings with support of radar-overlay on chart
 - by astronavigation.
- Deactivate track control.
- Verify course with magnetic compass.
- If possible, reboot systems (ECDIS, conning display etc.) one after another and check whether error has been resolved.
- Exclude source device from network according to instructions from manual.
- Follow company's emergency procedures.

At the bottom, the 'Cyber Alert History' section shows a list of past alerts with columns for Priority, Occurred Time (UTC), ID, Alert Title, Alert Details, Supposed Source, ACK, and ACKed Time (UTC).

Übersicht über aktive **alarms**, **warnings** und **cautions** (Prioritäten)*

Stumm- und Bestätigungsfunktionalität*

Checklist als Entscheidungsunterstützung

* gemäß IMO Performance Standards MSC.302(87)

Kontakt

Dr. rer. nat. Jan Bauer
jan.bauer@fkie.fraunhofer.de

Philipp Sedlmeier, M.Sc.
philipp.sedlmeier@cml.fraunhofer.de



Fraunhofer
CML



Fraunhofer
FKIE