update:me, 09. September 2024

Fraunhofer CML

Fraunhofer FKIE

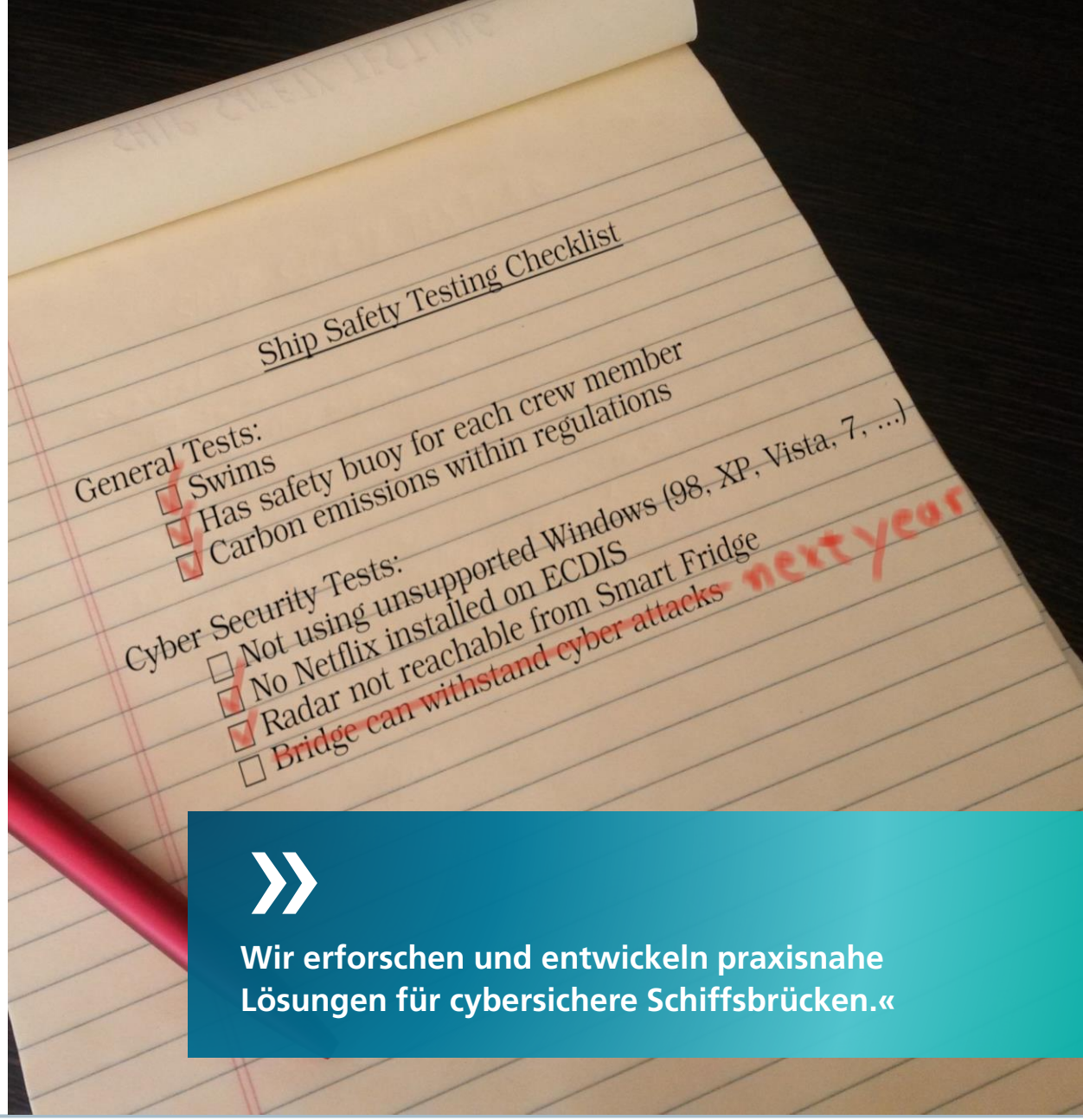
Cybersicherheit für die Schifffahrt

Mit einer Schiffsbrücke als Test- und Entwicklungslabor

Philipp Sedlmeier, Fraunhofer CML

Cybersicherheit für die Schifffahrt

Inhalt



»Wir erforschen und entwickeln praxisnahe Lösungen für cybersichere Schiffsbrücken.«

1

Cybersicherheit im maritimen Umfeld

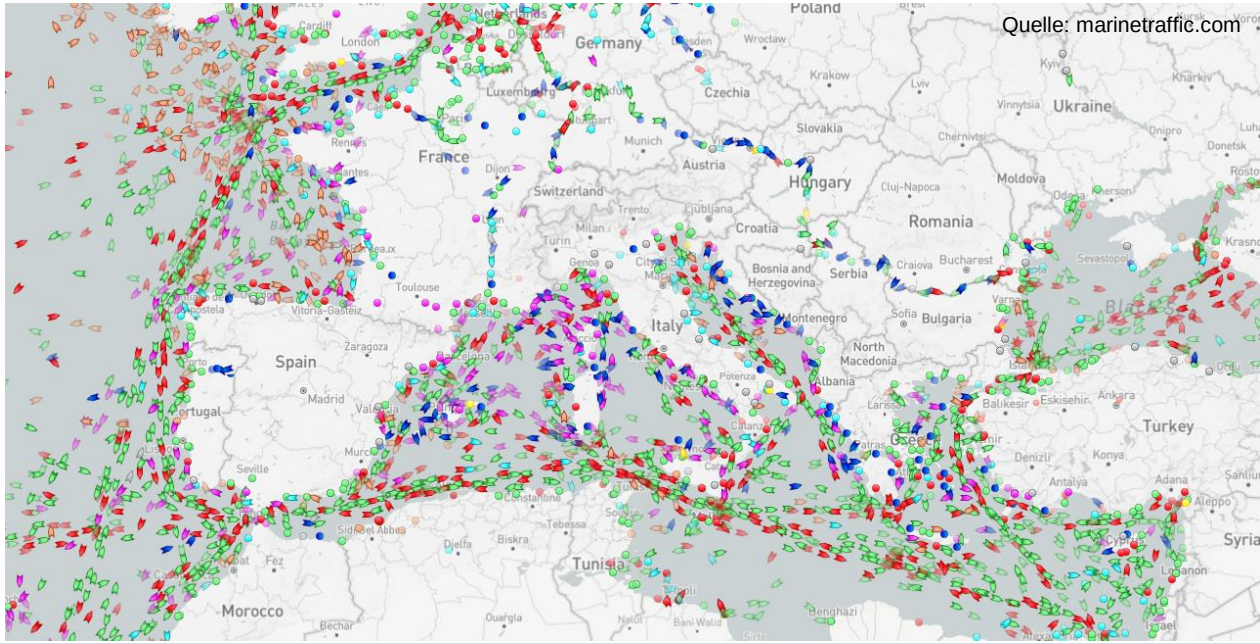
Fraunhofer

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



Quelle: marinetraffic.com

Fraunhofer

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 ≠ Cyberexperten

Source: tagesschau.de / epa

© Fraunhofer CML

Fraunhofer

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

© Adobe Stock

Fraunhofer

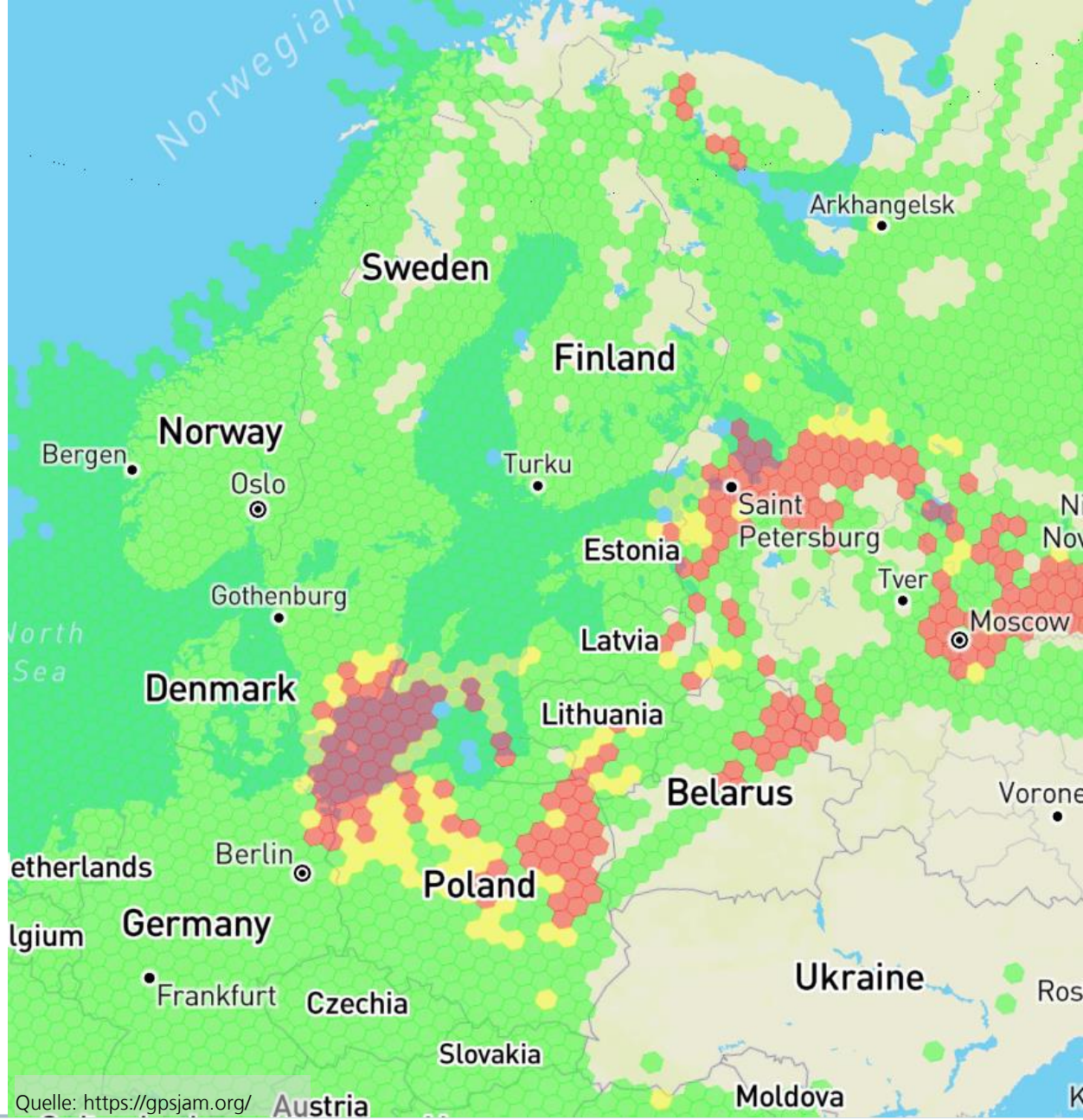
2

Bedrohungslage und Angriffsszenarien

Bedrohungslage u. Angriffsszenarien

Maritime Cybervorfälle

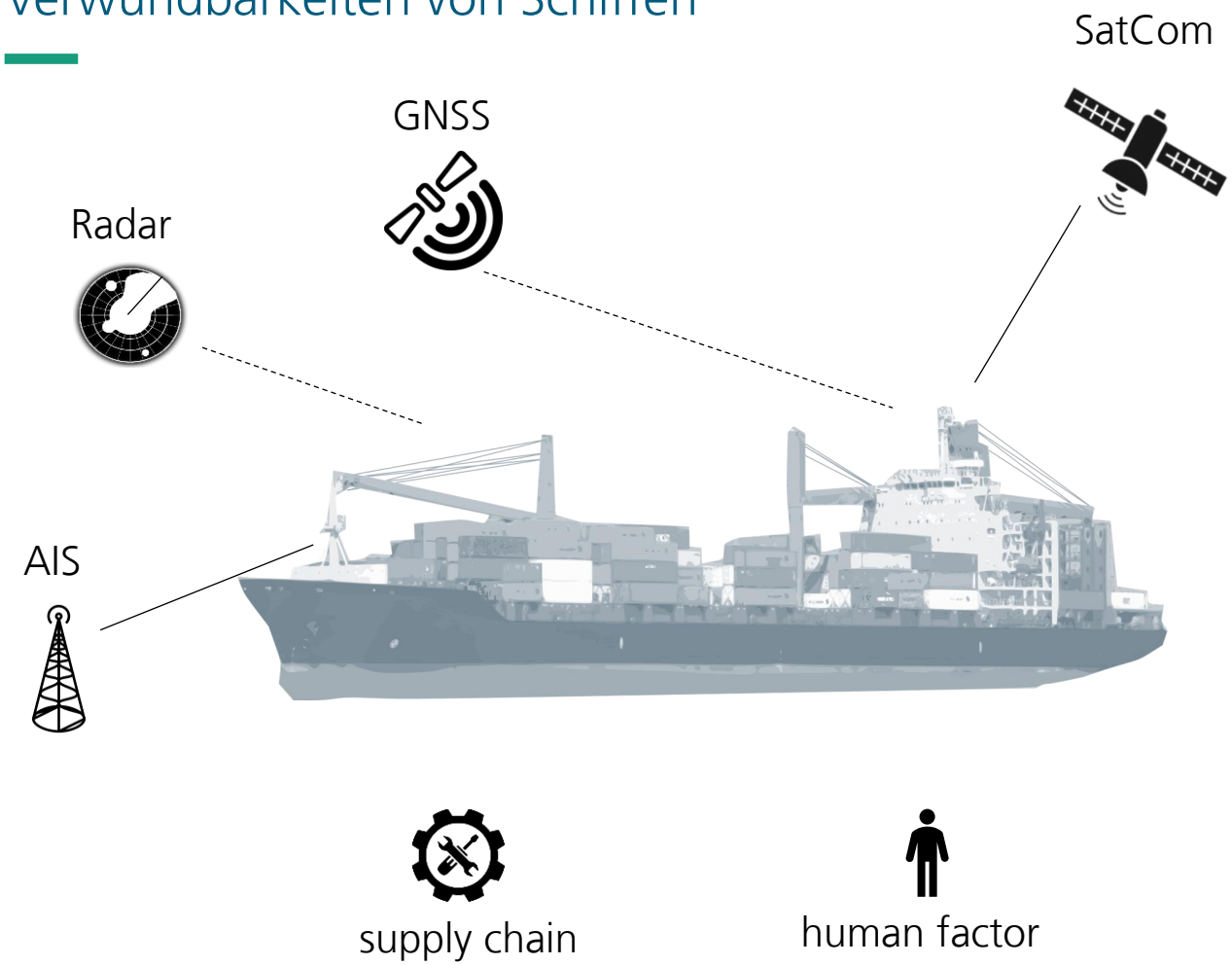
- Vermutlich hohe Dunkelziffer
- Häufig ungezielte Angriffe durch Viren/Malware
- Gezielte Angriffe auf GNSS und AIS



Fraunhofer

Bedrohungslage u. Angriffsszenarien

Verwundbarkeiten von Schiffen



Quelle: Maritime Cyber Threat Research group, University of Plymouth

Quelle: wired.co.uk / Gunva Le Meur

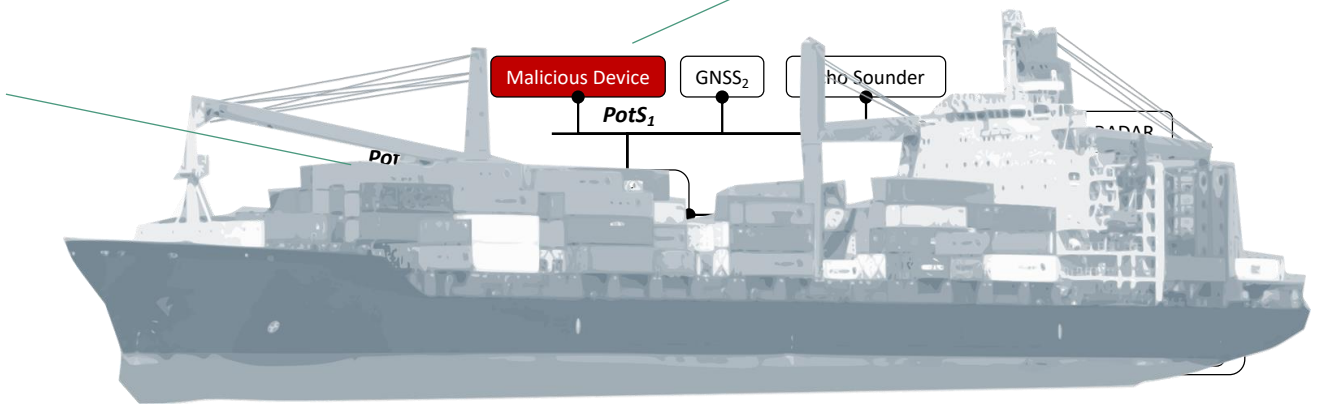
Fraunhofer

Bedrohungslage u. Angriffsszenarien

Fokus auf integrierte Brückensysteme

Malware (human factor, supply chain, SatCom)

Malicious hardware
(infiltriertes Gerät)



- Im Netzwerk

Ethernet header	IP header	UDP header	IEC 61162-450	Ethernet CRC32

IEC 61162-450 header		Payload
Token	TAG blocks	NMEA 0183 sentence

- NMEA Beispiel

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

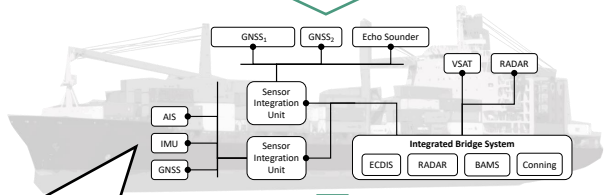
3

Test- und Entwicklungsumgebung

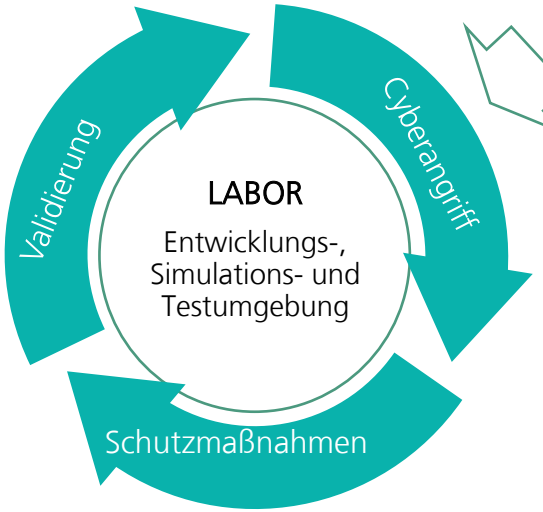
Fraunhofer

Test- und Entwicklungsumgebung

Vorgehen



Systemmodell



Bedrohungsmodell

Quelle: BSH

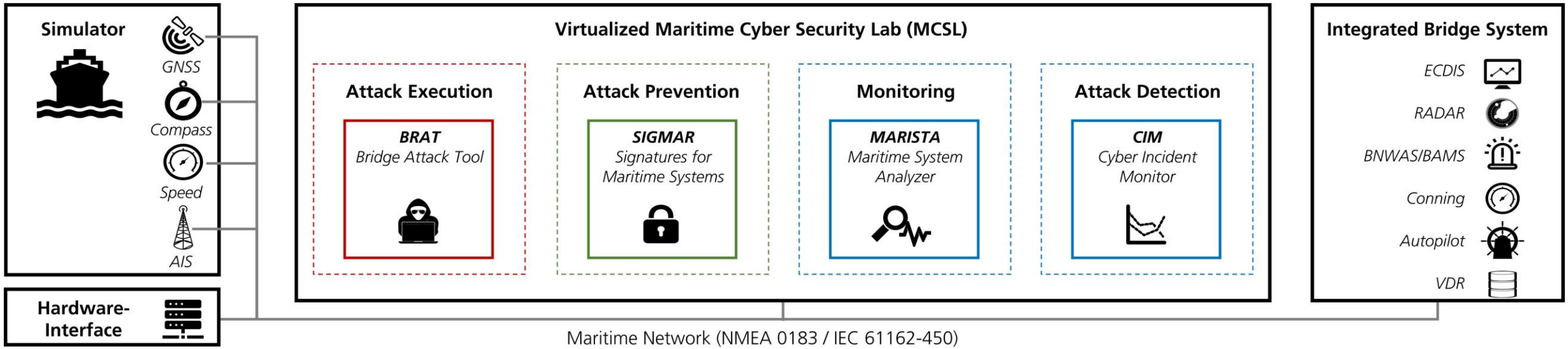
Praxis-Transfer

- Fraunhofer @ SMM 2022 in Hamburg

Fraunhofer

Test- und Entwicklungsumgebung

Softwarelösungen

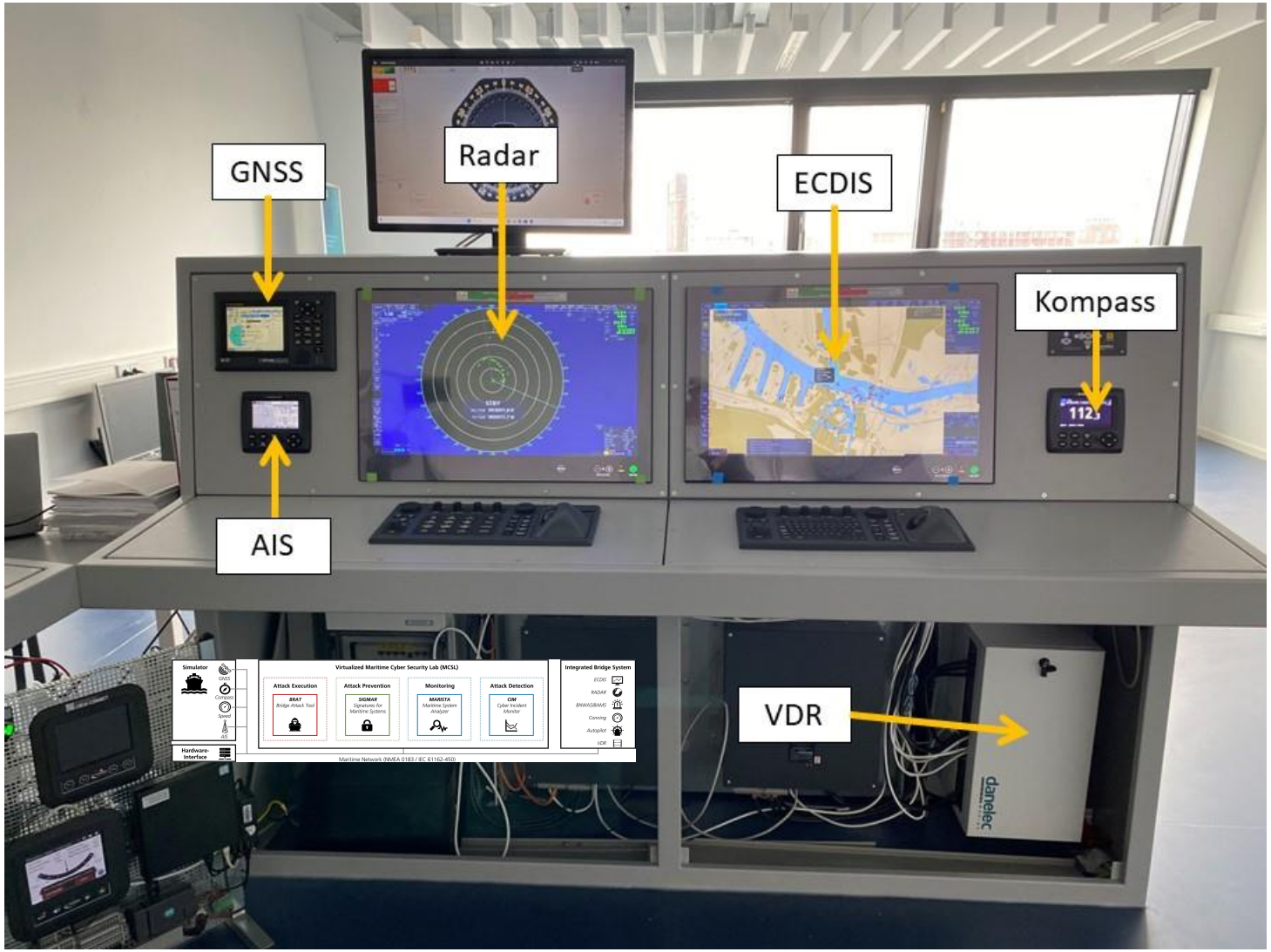


Fraunhofer

Test- und Entwicklungsumgebung

Brückenlabor

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

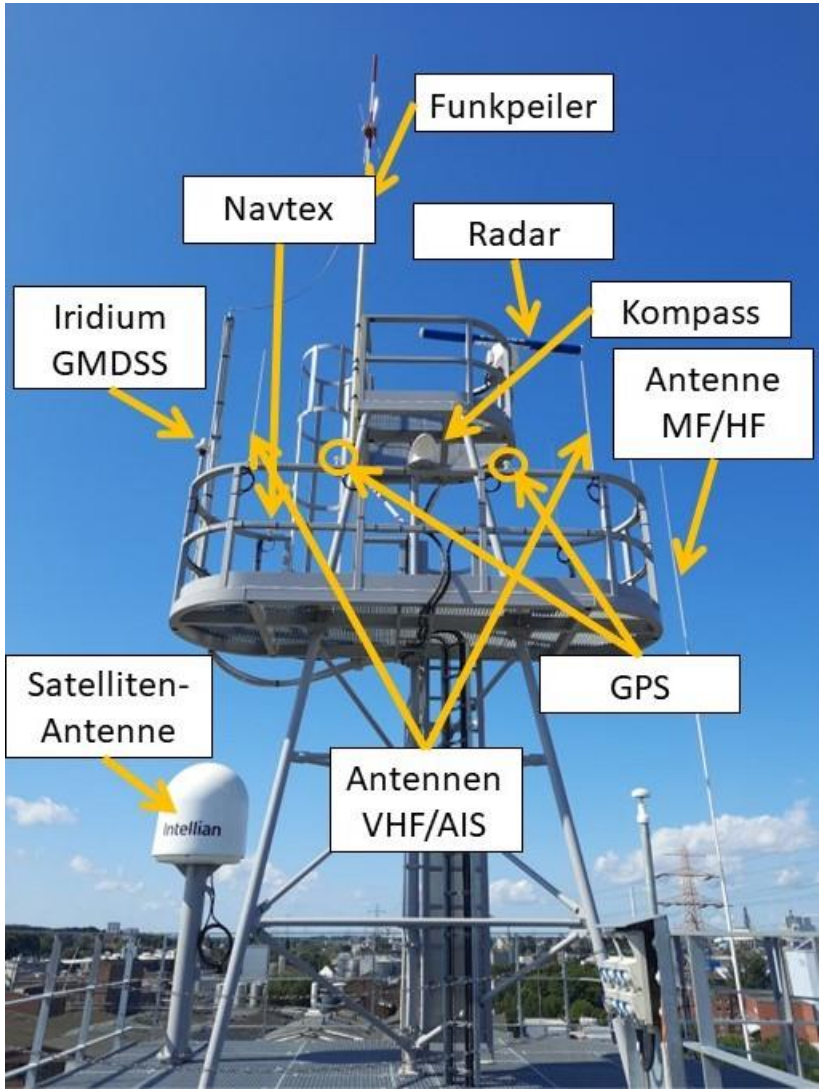


Fraunhofer

Test- und Entwicklungsumgebung

Antennenplattform

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



Fraunhofer

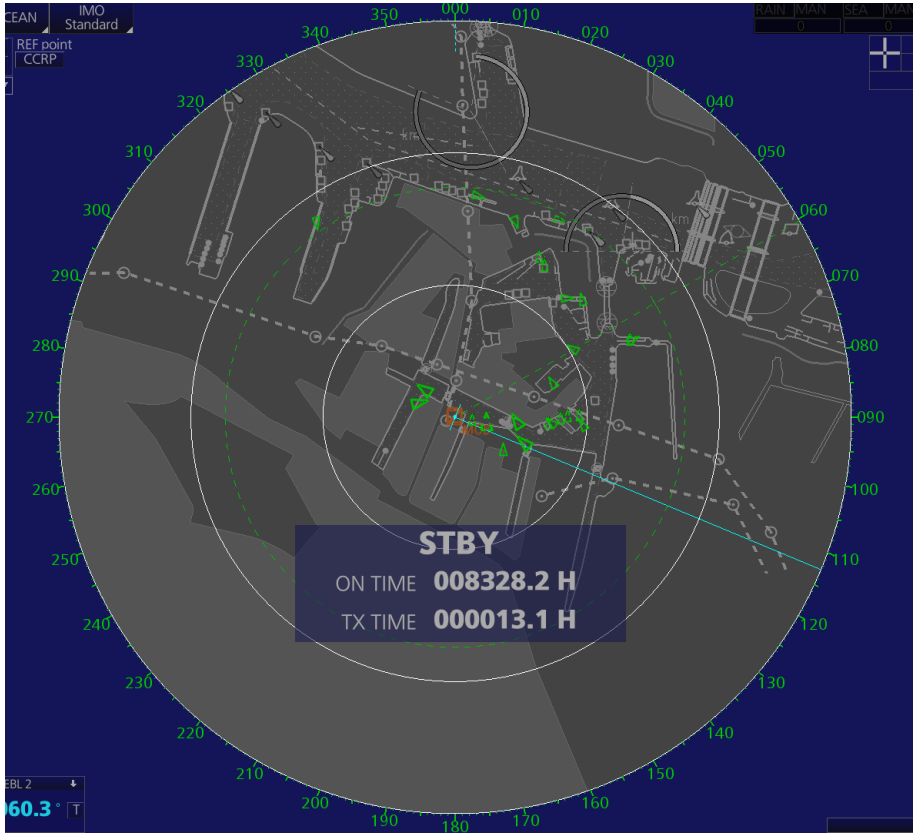
4

Experimente und Ergebnisse

Fraunhofer

Experimente und Ergebnisse

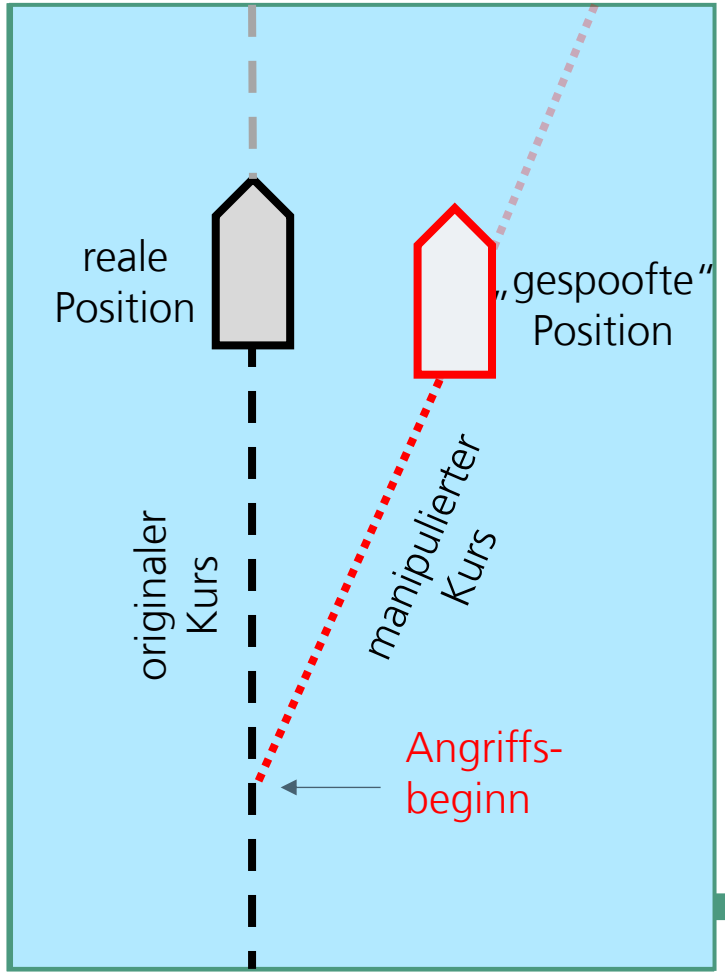
AIS-Flooding-Angriff

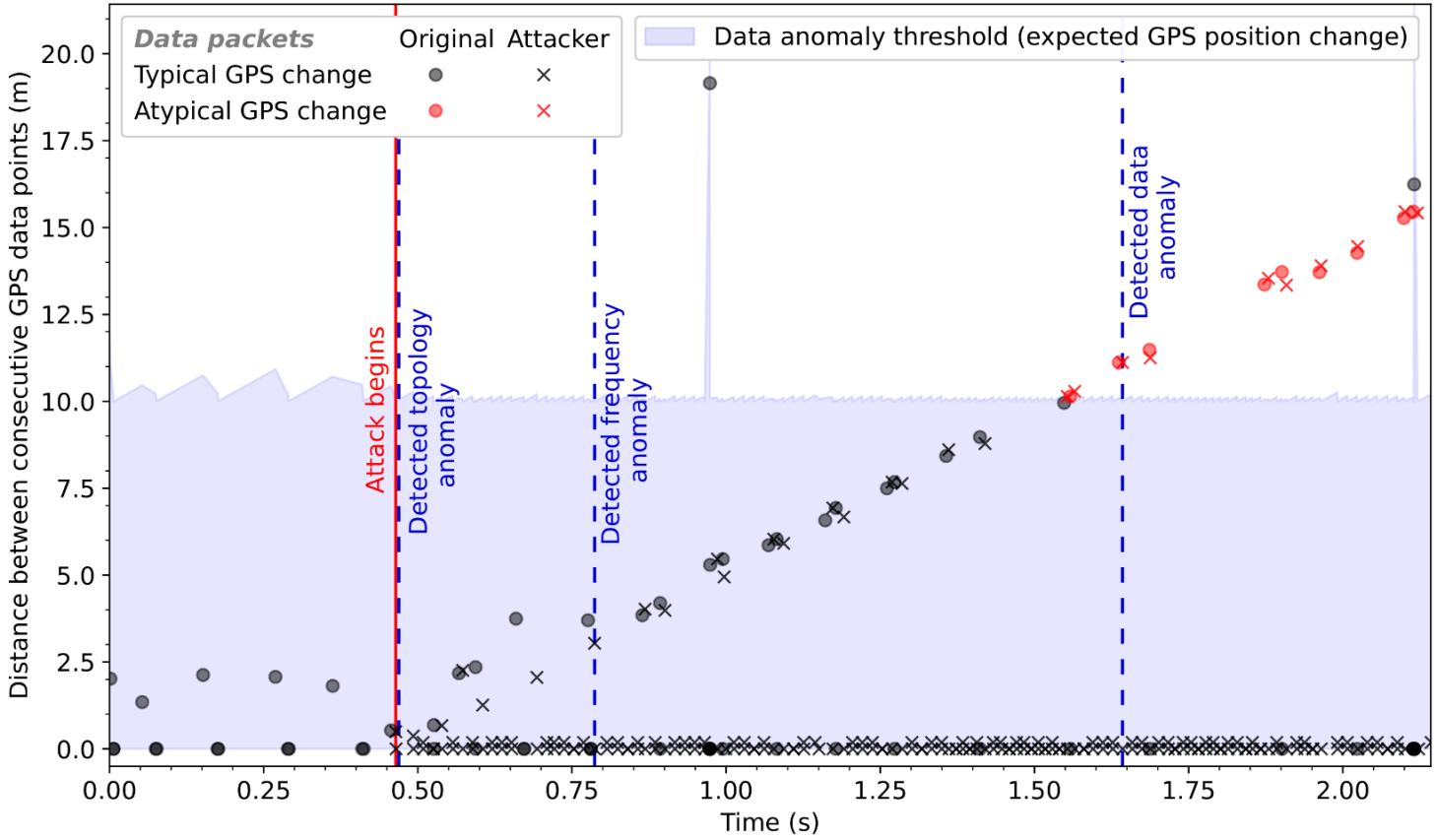


Fraunhofer

Anomalie-Erkennung

Maritimes Intrusion Detection System





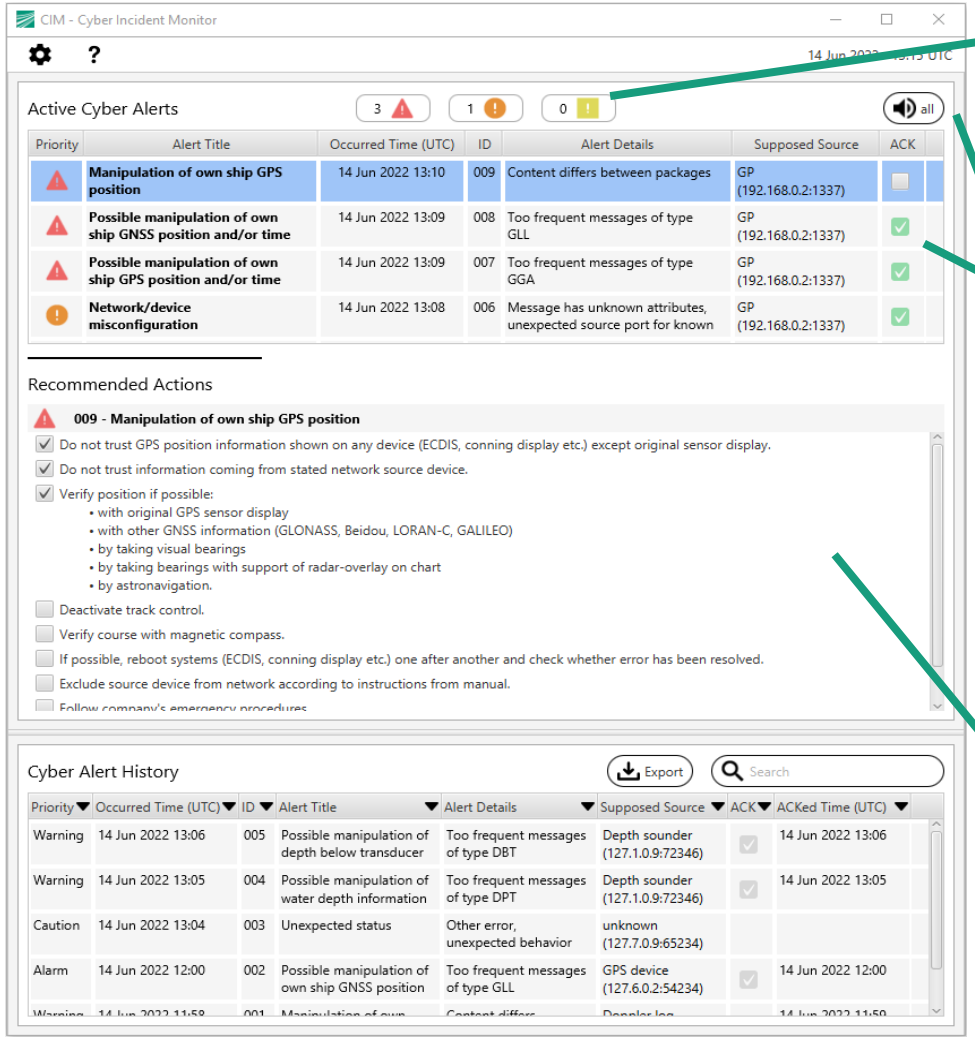
Fraunhofer

Cyber Incident Monitor

Ergonomische Mensch-Maschine-Schnittstelle

Aktive Cyber-Alarme

Alarm-Historie



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

Stumm- und Bestätigungsfunktionalität*

Checklist als Entscheidungsunterstützung

* gemäß IMO Performance Standards MSC.302(87)

Fraunhofer

Fraunhofer CML

Fraunhofer FKIE

Kontakt

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

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