Frederik Basels, Philipp Sedlmeier, Elmar Padilla, Jan Bauer

Seeing is Believing
- A Practical Study of Cyber Attacks on a Ship Navigation Bridge

A Known Threat to Unprepared Seafarers

Digitalization enables cyber attacks on modern vessels

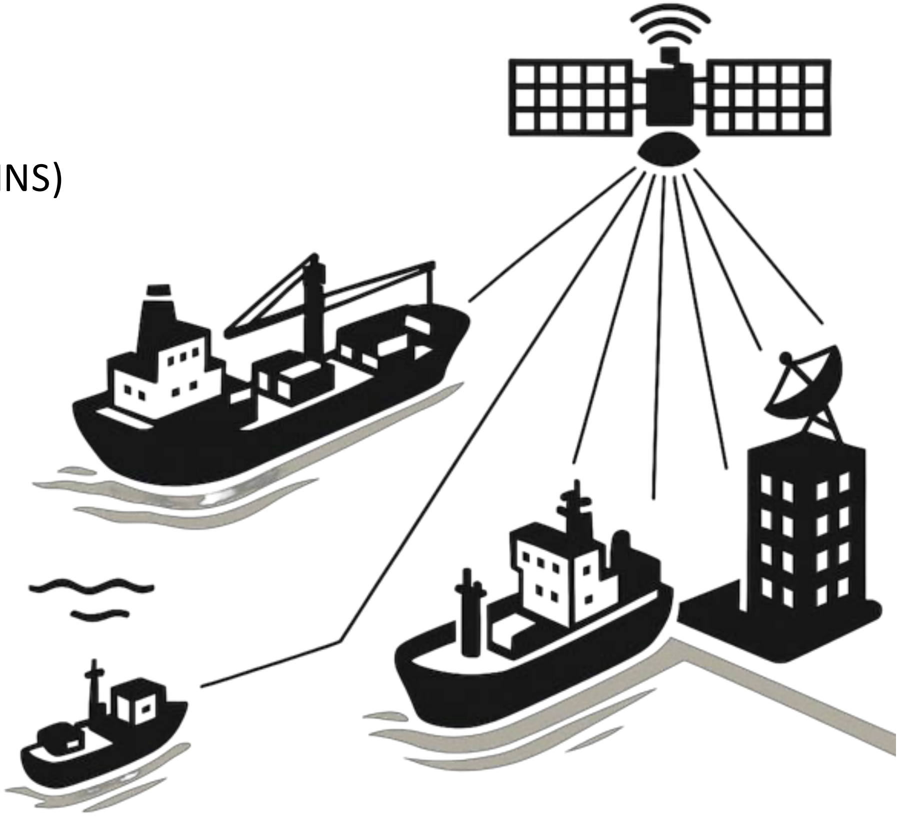
- Ships are no longer air-gapped systems
- Sensors and terminals all interconnected on Integrated Navigation Systems (INS)

Known threat for all kind of maritime personnel

- Cyber security now included in regulations and standards
- Shipyards and owners claim to be aware of the importance
- **However:**
  - Lack of secure-by-design products
  - 93% of crewmember feel unprepared to handle cyber incidents[1]

Practical demonstrations on real-world environments necessary

- Improve training of maritime personnel
- Motivate development of cyber secure products



Demonstrated Attacks

Exploitation-/Malware-based Attacks

e.g.,

- Manipulation of received data by malware[2,3]
- Reconfiguration via vulnerable interfaces[4]

➔ Manipulation of single device

Network-based Attacks

e.g.,

- Injection of network packets as MotS[5,6]
- Manipulation of intercepted packets as MitM[7]

➔ Manipulation of all systems on network

Our Goal:

1. Study feasibility of network-based attacks
2. Report our lessons learned

Hardware Systems

Simulators

IEC 61162-450

Chart Plotter / ECDIS

Simulative Environments

Our Real-World Bridge

Stationary INS with real marine equipment

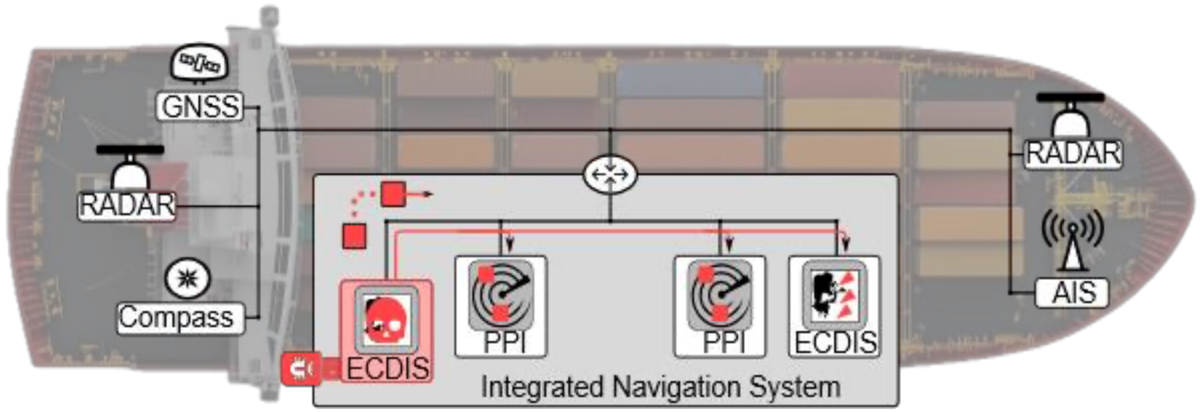
- Resembles bridge of actual container ship
- Antenna platform on the roof provides realistic sensor data

Installed and configured according to regulations

- Installed systems, among others:
  ECDIS, Chart RADAR, GNSS, satellite compass, AIS transponder
- Interconnected via NMEA 0183 and IEC 61162-450 networks

- Missing:
  - Information on depth, rudder and propulsion
  - Redundancies in sensors

From Simulator to Bridge
– Performed Attacks



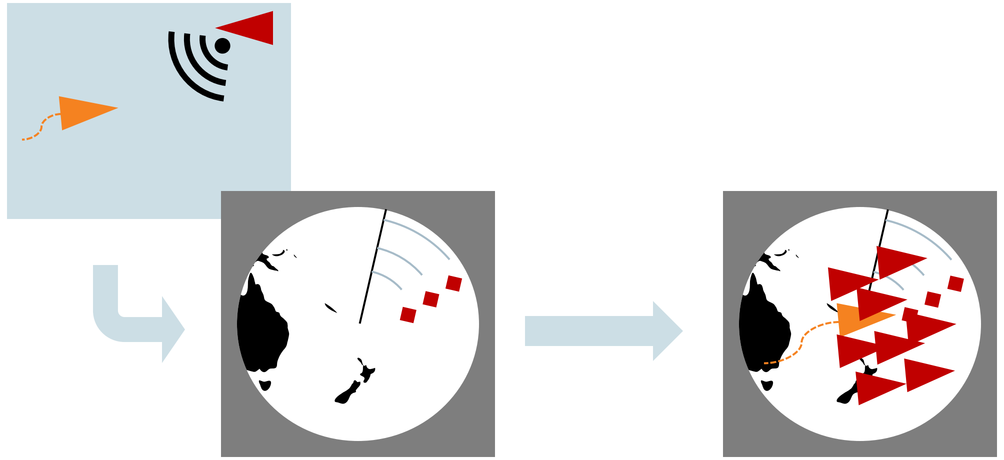
Scenario:

Attacker infected one device on an arbitrary INS

- Laptop connected to network switch
- Little knowledge about the bridge and its configuration
- No change of configuration

Network-based attacks

- Bridge Attack Tool (BRAT) to manipulate displayed sensor data
- Radar Attack Tool (RAT) to manipulate displayed RADAR image



Triggering via Covert Channel

- Reimplemented approaches from literature
  - E.g. RADAR based attack triggering

Fraunhofer FKIE

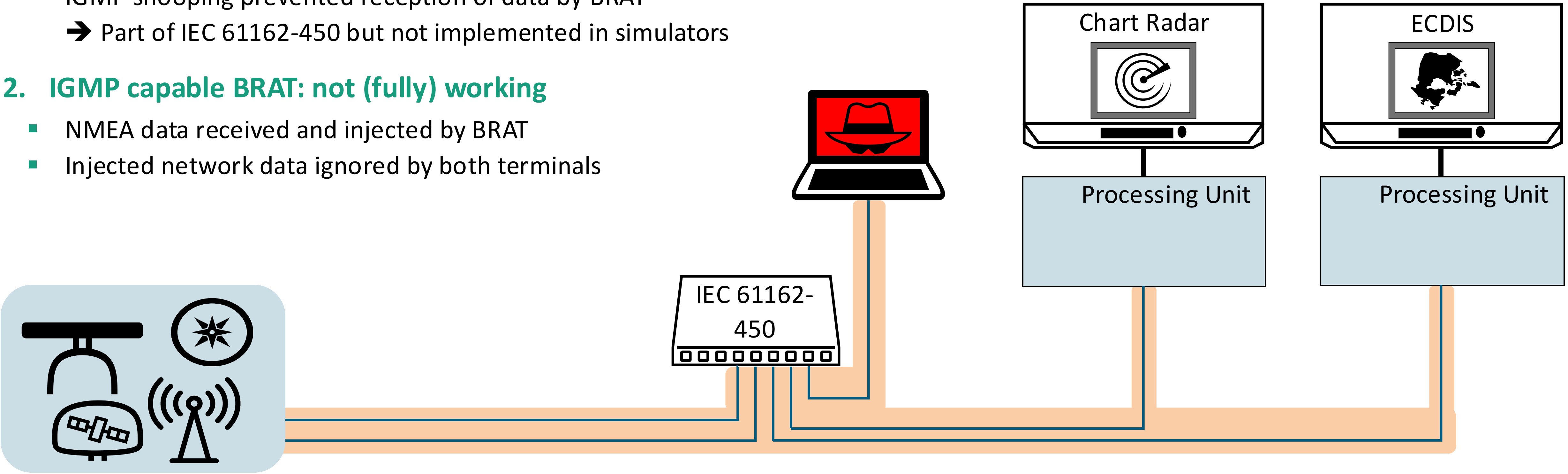
Network-based Attacks
– Expectations

1. BRAT out of the box: not working

- NMEA data only shared in IP-multicast groups managed via IGMP
- IGMP snooping prevented reception of data by BRAT
  ➔ Part of IEC 61162-450 but not implemented in simulators

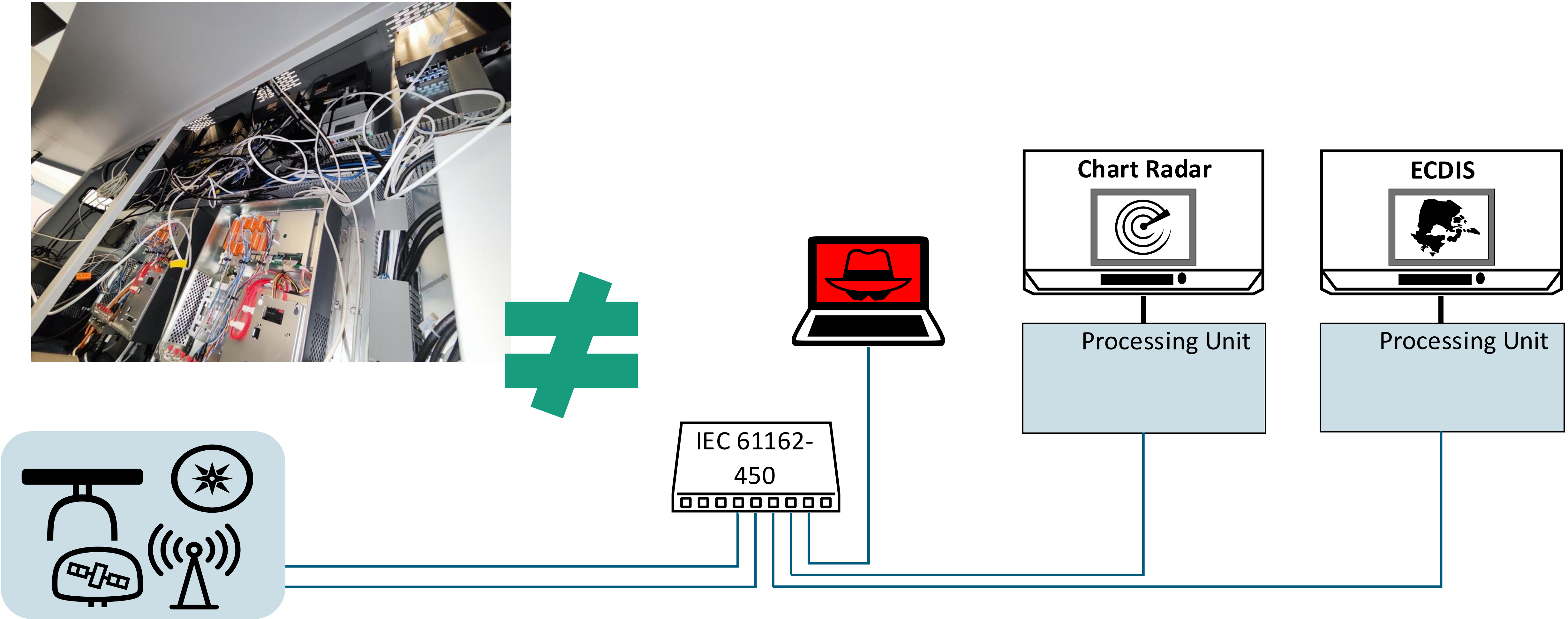
2. IGMP capable BRAT: not (fully) working

- NMEA data received and injected by BRAT
- Injected network data ignored by both terminals



Network-based Attacks

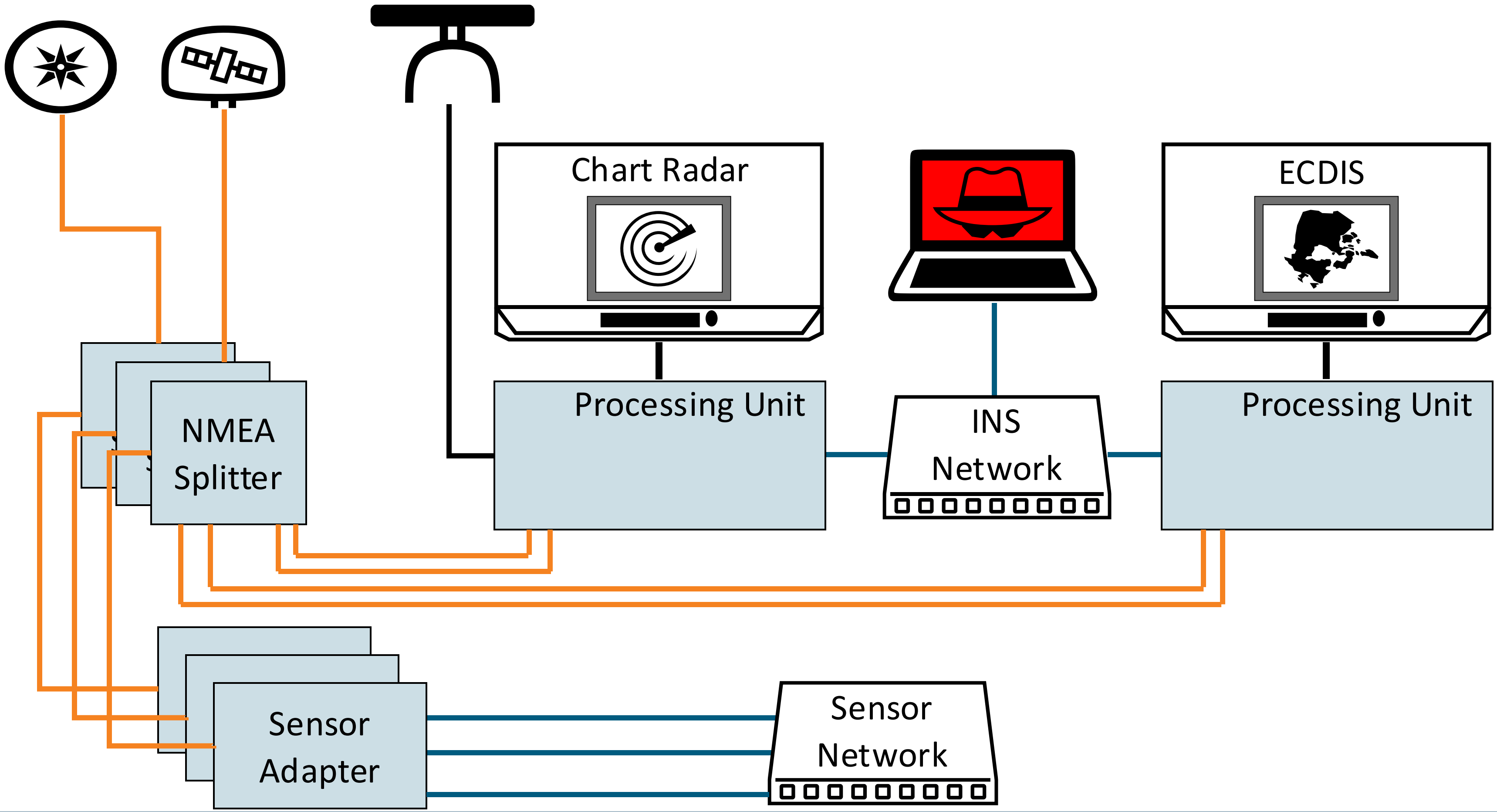
– Reality



Network-based Attacks
– Reality

Existing INS networks:

- Serial network
  - NMEA 0185
  - ➔ Main and prioritized data source
- Sensor network
  - Mainly IEC 61162-450
  - Terminals not participants
  - ➔ Actual purpose unknown
- INS network
  - IEC 61162-450 and others
  - Sensors not participants
  - ➔ Share terminal settings,
  - ➔ Backup for sensor data



Network-based Attacks
– Results

3. BRAT with IGMP and interrupted serial connections:

- Arbitrary manipulations possible on:
  - Position
  - Heading
  - Speed
  - AIS signals
- Sudden or continuous (stealthy)
- Triggering of alerts possible

Limitation:

- Manipulations only possible on when serial connection interrupted

Safety measurements (i.e., redundancies) can prevent network-based attacks

➔ Reconnaissance and reconfiguration of each terminal might be necessary

RADAR Overlay Manipulation
– Results

Prior work necessary:
- Understand and implement proprietary network protocol

1. RAT out of the box:
successful on ECDIS
- Arbitrary manipulations possible:
  - Changing azimuth field to rotate image
  - Add echoes
  - Remove echoes

Limitations
- Fragments of image visible due to Man-on-the-Side attack
- Fields in network protocol not changeable
  e.g., constant redrawing when changing range field

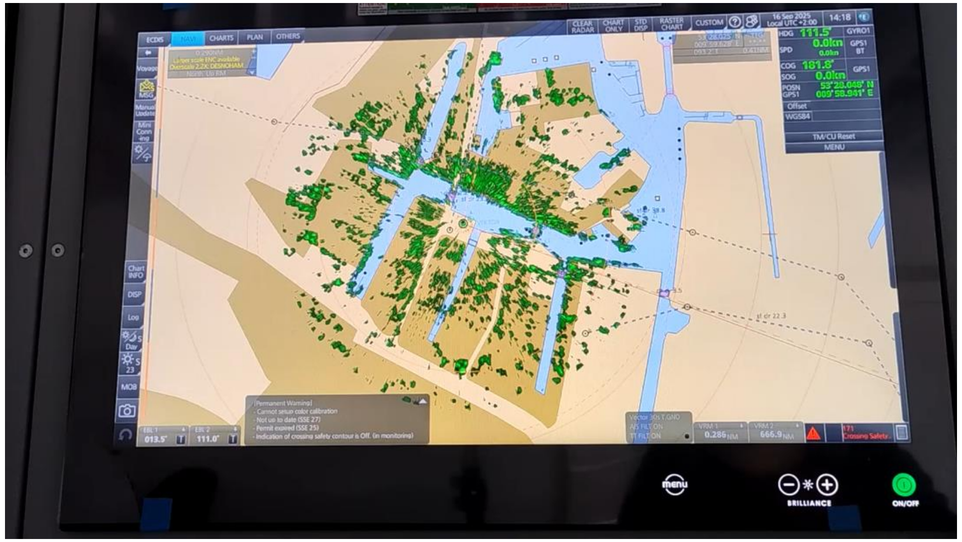


Chart RADAR Manipulation

– Expectation vs. Reality

Expectation:

No manipulation possible

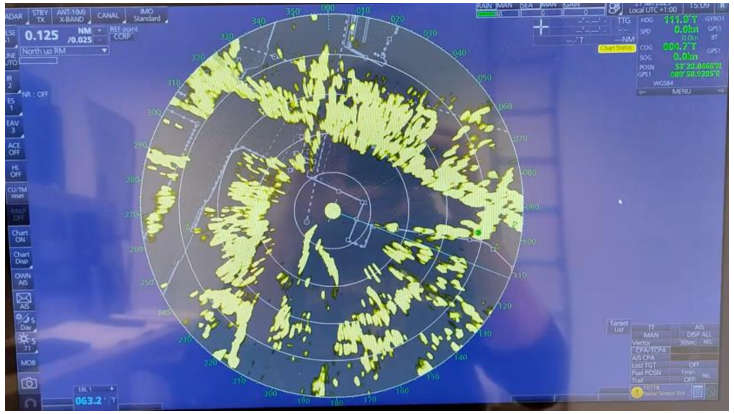
- Direct connection via (apparently) LAN cable from RADAR antenna to processing unit
- However, second spoke visible while replay of network data

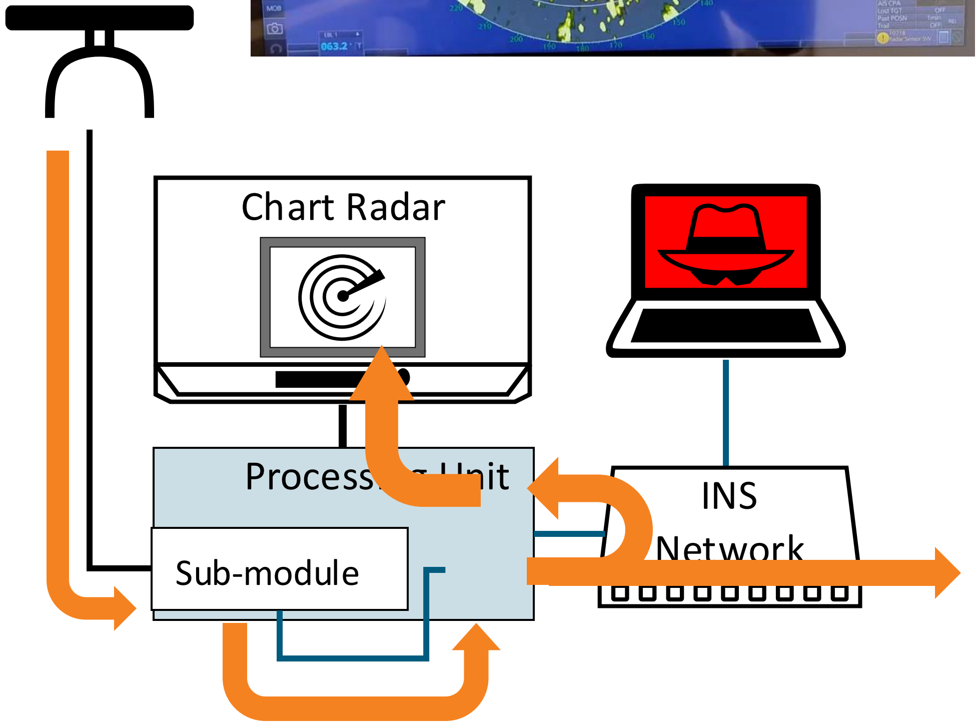
Reality:

Image data enters network before being processed

- Sub-module forwards data to processing unit

- Speculations:
  - Sub-module encodes raw video data from RADAR antenna
  - Routing through network simplified implementation





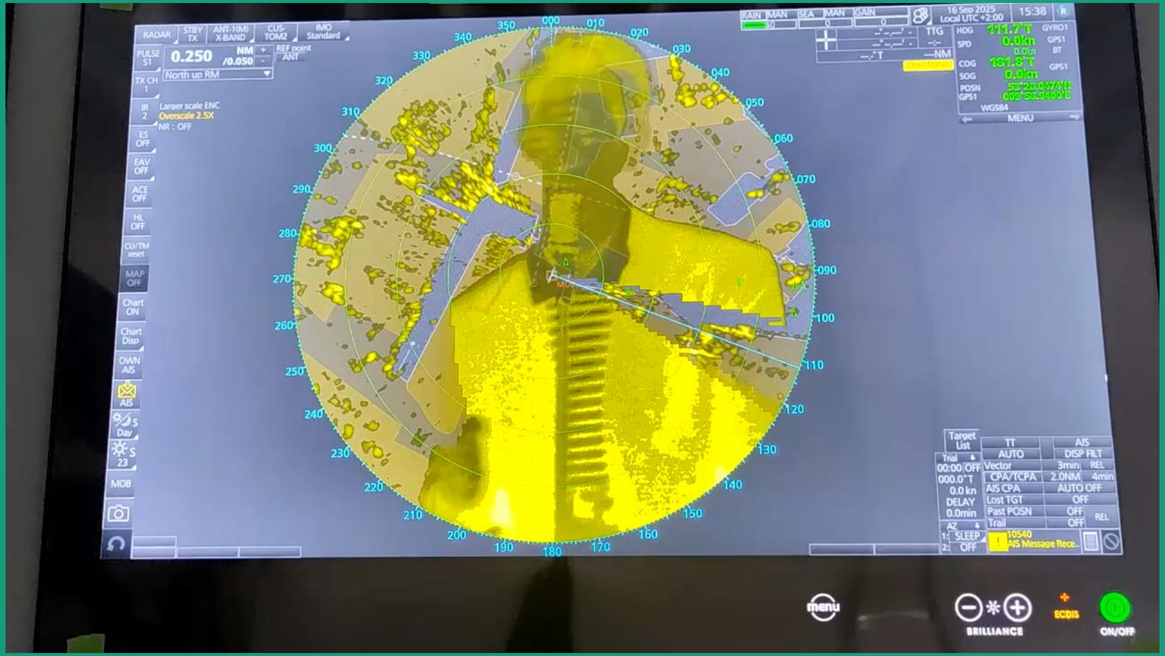
Fraunhofer FKIE

Chart RADAR Manipulation
– Results

Arbitrary manipulations of Chart RADAR image possible:

- Possible manipulations:
  - Change position of echoes
  - Add echoes
  - Remove echoes
  - Change Echo color
    → blue echoes indicate past echoes of a moving target
- Manipulations without fragments

Only nondisclosure of protocol prevent arbitrary manipulation of RADAR image
Nice!



Limitations:

- Fields in network protocol not changeable
  e.g., constant redrawing when changing range field

Remote Triggering
– Results

Limitations in tests:

- Proximity of local harbor prevented transmission of fake signals
  ➔ RADAR trigger tested by message injection
  - Encoded triggering RADAR echoes according protocol

Network traffic has no effect on trigger functionality, but

- RADAR tuning can influence trigger behavior
  - Noisy near harbor or land
  - Noise level dependent on tuning
    e.g., gain, rain-, sea suppression

RADAR tuning and environment can lead to false triggering

More complex trigger patterns or pattern detection necessary

From Simulator to Bridge
– Performed Attacks

Attack Type 2:

Covert control channel to trigger attacks

- Reimplemented approaches from literature

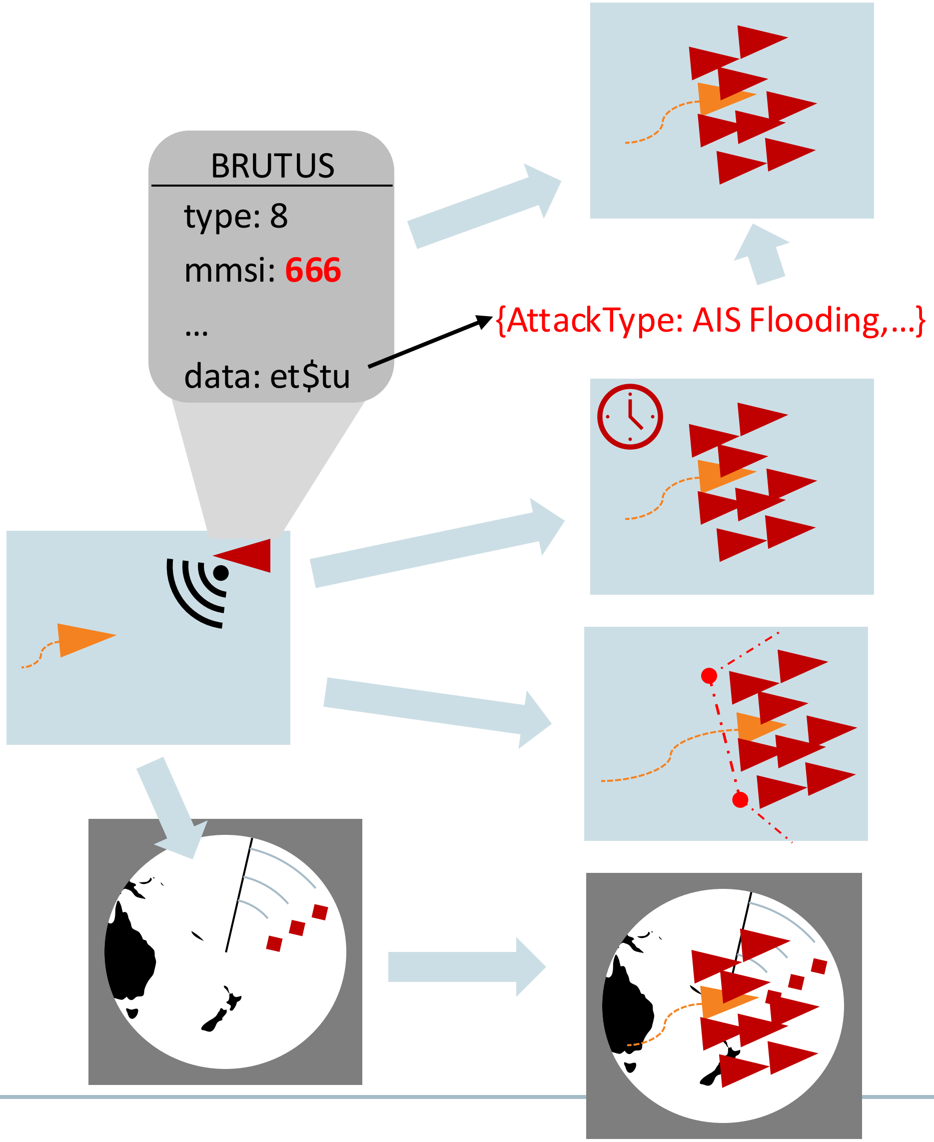
Environmental information

- GNSS based trigger agent reacting to
  - Time
  - Location (= Geofencing)

One-directional communication via RF signals

- AIS based trigger agent reacting to
  - Received MMSI
  - Payload in AIS message[8]

- RADAR based trigger agent reacting to echo patterns[9]



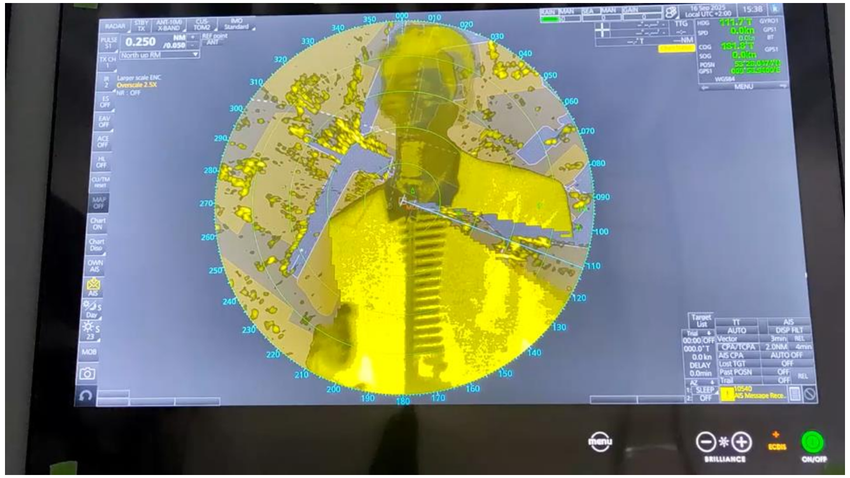
Fraunhofer FKIE

Takeaways & Conclusion

Studied cyber attacks on stationary real-world INS

- Attacks in maritime environment needed for training and awareness
- Focus on network-based cyber attacks

  ➔ Demonstrated some limitations of proposed cyber threats



Sensor manipulations not trivial

- Redundant and prioritized networks

  → Access to network does not grand full control
- Reconfiguration might ne necessary
  - Unnoticed physical access unlikely, as casings are hard to access and sealed

INS-wide RADAR manipulation possible

- Only protected by nondisclosure of proprietary network protocols

Reception via covert-channels possible, but

- Detection of pattern in RADAR image not trivial
- Depends on environment and tuning of RADAR

Target	Position	AIS	Heading	SOG	RADAR
ECDIS	◖	◖	●	◖	●
Chart RADAR	◖	◖	◖	◖	●
Attack Trigger	●	●	–	–	◕

References

[1] F. Macdonald, “The Lifecycle Dilemma: Navigating cybersecurity risks across designing, constructing and operating a vessel.” [Online].

[2] M. S. Lund, O. S. Hareide, and Ø. Jøsok, “An Attack on an Integrated Navigation System,” Necesse, vol. 3, no. 2, 2018.

[3] V. Wee, “Naval dome exposes vessel vulnerabilities to cyber attack,” Seatrade Maritime News, 2017. [Online].

[4] K. Munro, “Hacking, tracking, stealing and sinking ships,” PenTestPartners, 2018. [Online].

[5] C. Hemminghaus, J. Bauer, and E. Padilla, “BRAT: a Bridge Attack Tool for Cyber Security Assessments of Maritime Systems,” TransNav, vol. 15, no. 1, 2021.

[6] G. Longo, E. Russo, A. Armando, and A. Merlo, “Attacking (and Defending) the Maritime Radar System,” IEEE Transactions on Information Forensics and Security, vol. 18, 2023.

[7] K. Wolsing, A. Saillard, J. Bauer, E. Wagner, C. van Sloun, I. B. Fink, M. Schmidt, K. Wehrle, and M. Henze, “Network Attacks Against Marine Radar Systems: A Taxonomy, Simulation Environment, and Dataset,” in Proc. of the 47th IEEE Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 2022.

[8] A. Amro and V. Gkioulos, “From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks,” in Proc. of the 27th European Symposium on Research in Computer Security (ESORICS), Copenhagen, Denmark, 2022.

[9] W. C. Leite Junior, C. C. de Moraes, C. E. de Albuquerque, R. C. S. Machado, and A. O. de Sá, “A Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems,” Sensors, vol. 21, no. 9, p. 3195, 2021.