Radar Cyber Security Lab

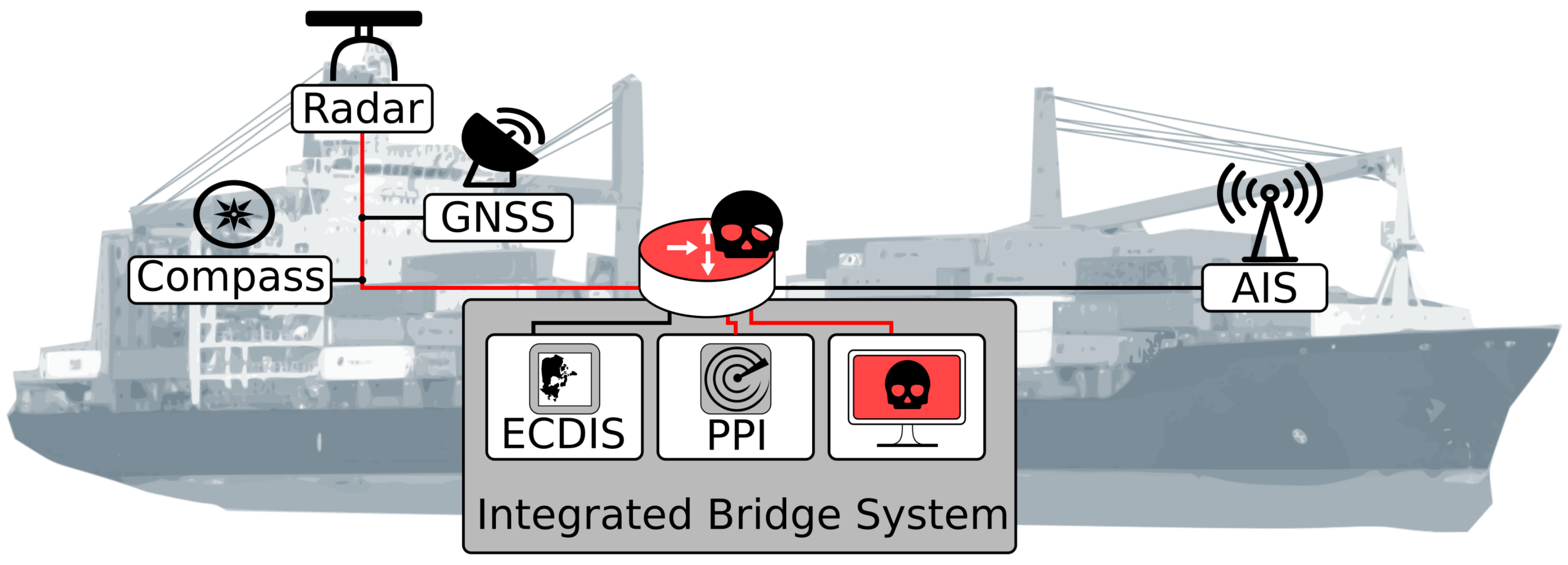
A Framework to Develop and Test New Defensive Solutions

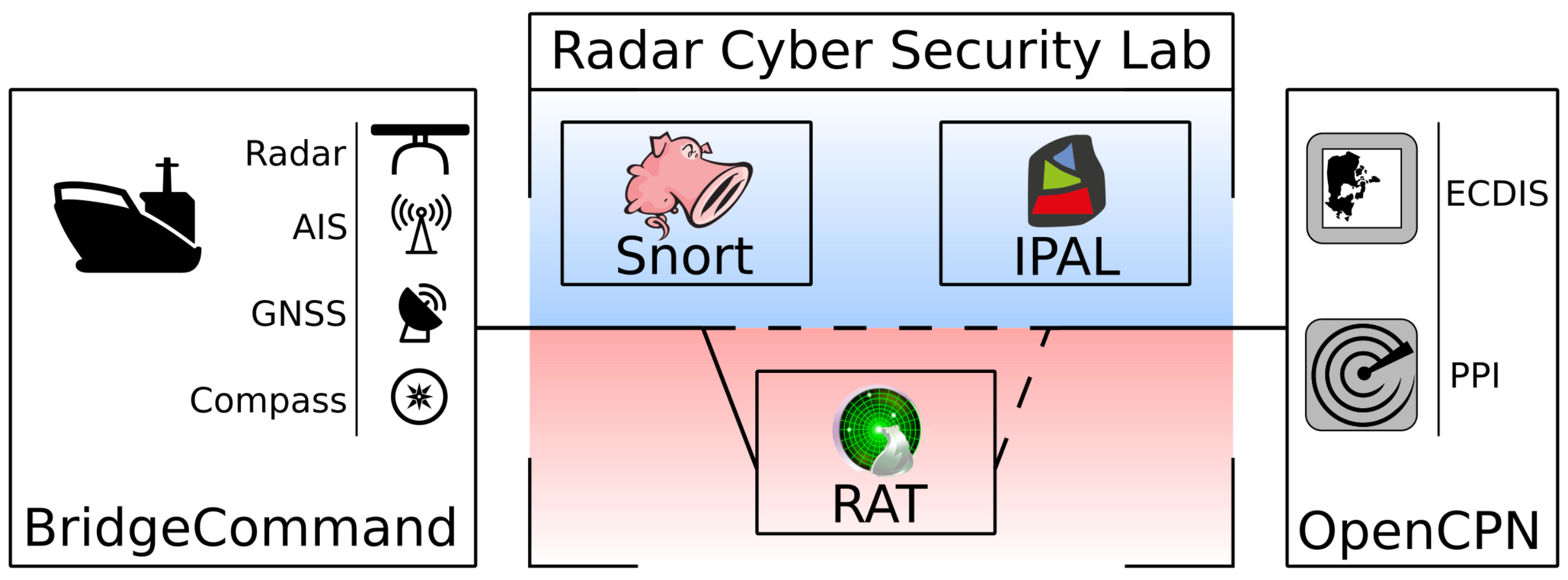
F. Basels, K. Wolsing, E. Padilla, J. Bauer

Fraunhofer FKIE

Maritime Radar Systems under Attack

Ship networks are built on maritime protocols with typically **no authentication** and **no encryption**. Without such security features, the doors are wide open for attackers to manipulate all kinds of systems on a bridge, including maritime radars. In narrow waterways or obscure situations, such targeted cyberattacks against these systems can lead to collisions or groundings of a ship that result in financial or physical harm.





Help is on the Way!

Our Radar Cyber Security Lab [3] is a framework for identifying, developing and testing new weaknesses and defensive solutions for maritime radar systems. It leverages a simulative environment and builds on actual maritime protocols to also directly interact with real bridge systems and their networks.

INJECT – The Radar Attack Tool

Our Radar Attack Tool (RAT) [1] performs network-based attacks against radar systems. In a Machine-in-the-Middle (MitM) or Machine-on-the-Side (MotS) setup, RAT can inject packets to interfere with the radar and performs various types of attacks. The effects visible on the radar screen can be categorized into three classes:

Denial of Service

Fill the screen

Blank the screen

Turn the radar off

Image Manipulation

Rotate the image

Scale the image

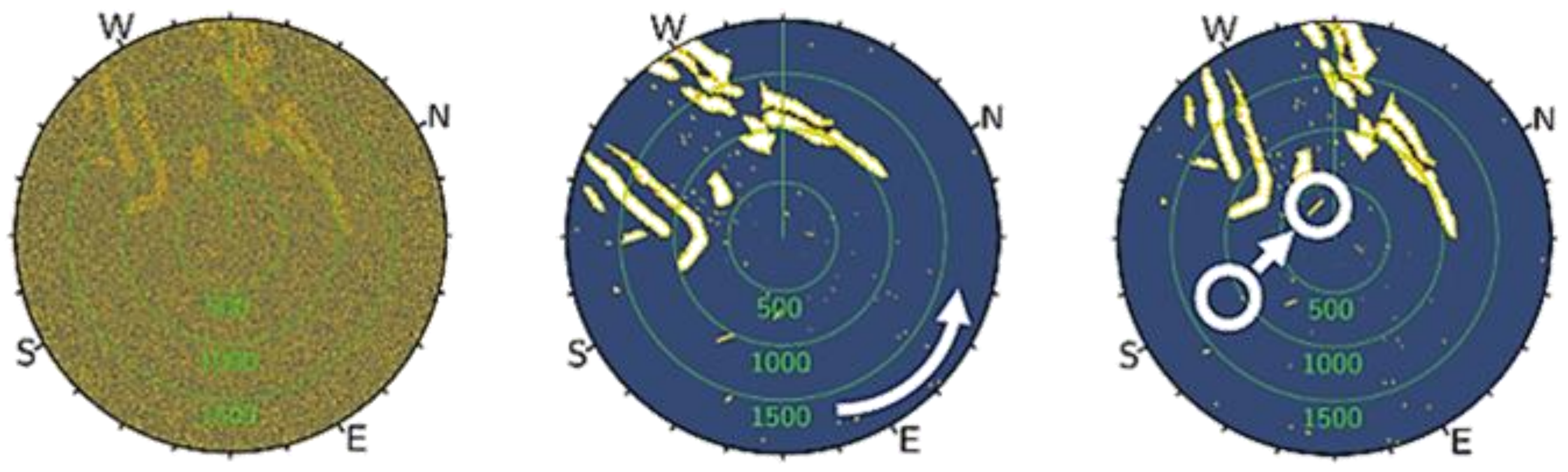
Translate the image

Object Manipulation

Add an object

Remove an object

Relocate an object



Detection Capabilities

The detection rates of the different IDSs depend heavily on the type of attack and position of the attacker. While all MotS attacks can be detected reliably by an analysis of the network traffic, object manipulation attacks in a MitM scenario can not be detected at all. A challenge in detecting this type of attack is the small number of manipulated pixels and a lack of ground truth for moving objects, i.e., other ships at sea.

	DoS	Image manipulation	Object manipulation
Snort	MotS	MotS	MotS
Image-Delta	(✓)	MitM	✗
Chart-Diff	(✓)	✓	✗

✓: reliable detection (✓): reduced detection rate ✗ : no detection

MotS|MitM: reliable detection in given scenario only

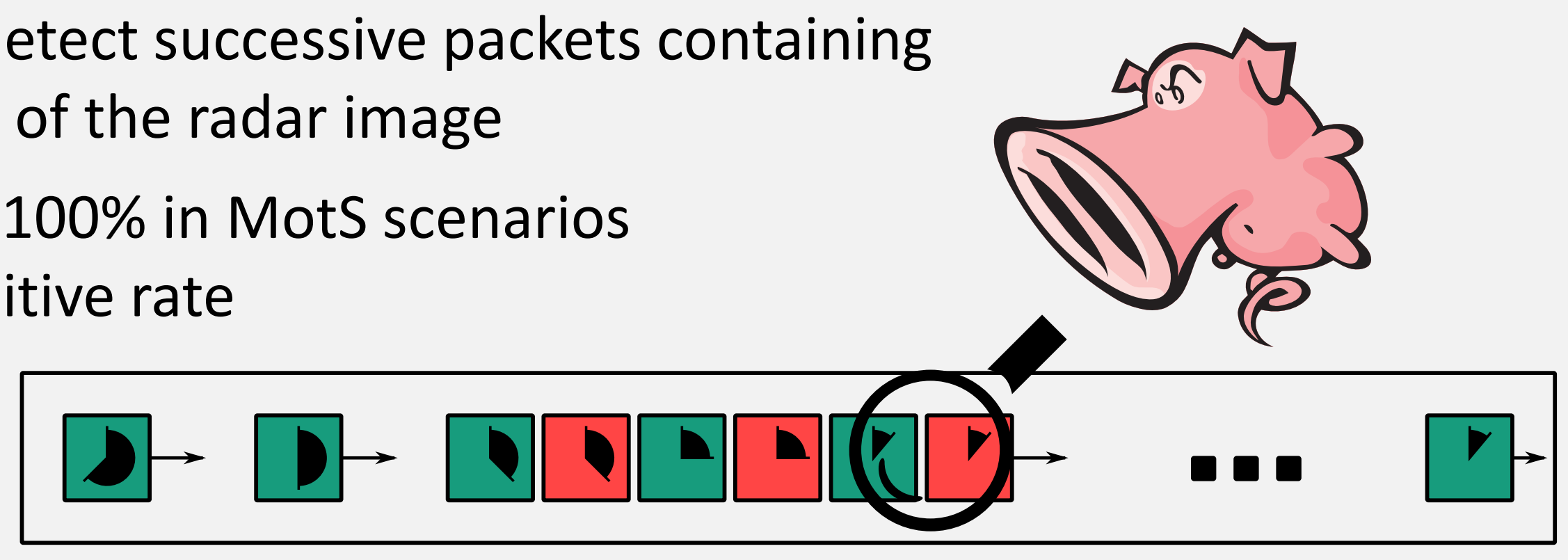
DETECT – Radar-Specific Intrusion Detection Systems

As long as manufacturers of maritime systems do not provide native solutions to prevent packet injection or manipulative attacks, Intrusion Detection Systems (IDSs) can be deployed to existing systems to detect attacks and inform the crew on the bridge [2].

Network Traffic Analysis:

Snort

- Custom rules to detect successive packets containing duplicated angles of the radar image
- Detection rate of 100% in MotS scenarios with 0% false-positive rate



Radar Image Analysis:

Image-Delta

- Validate successive radar images with movement of ship
- Limited to areas close to the coast

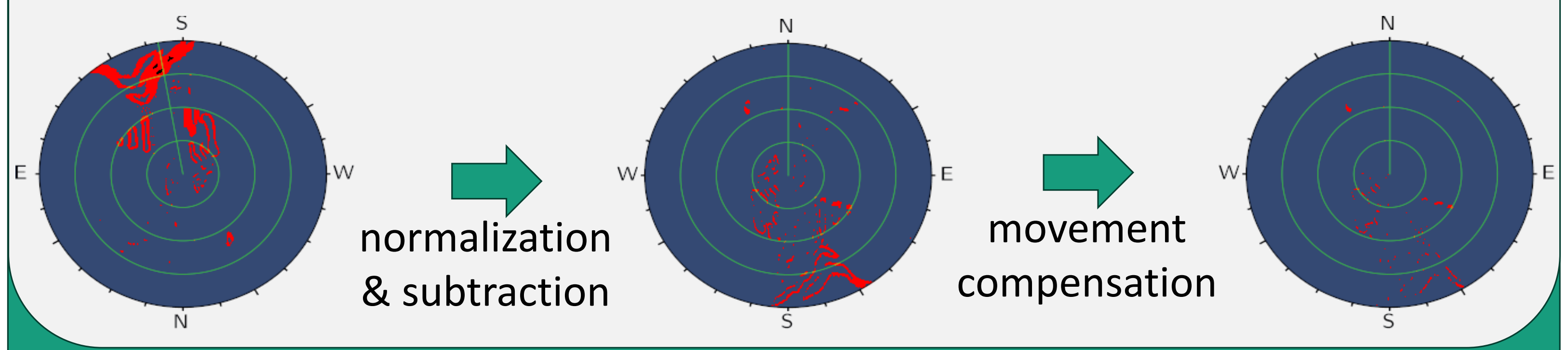
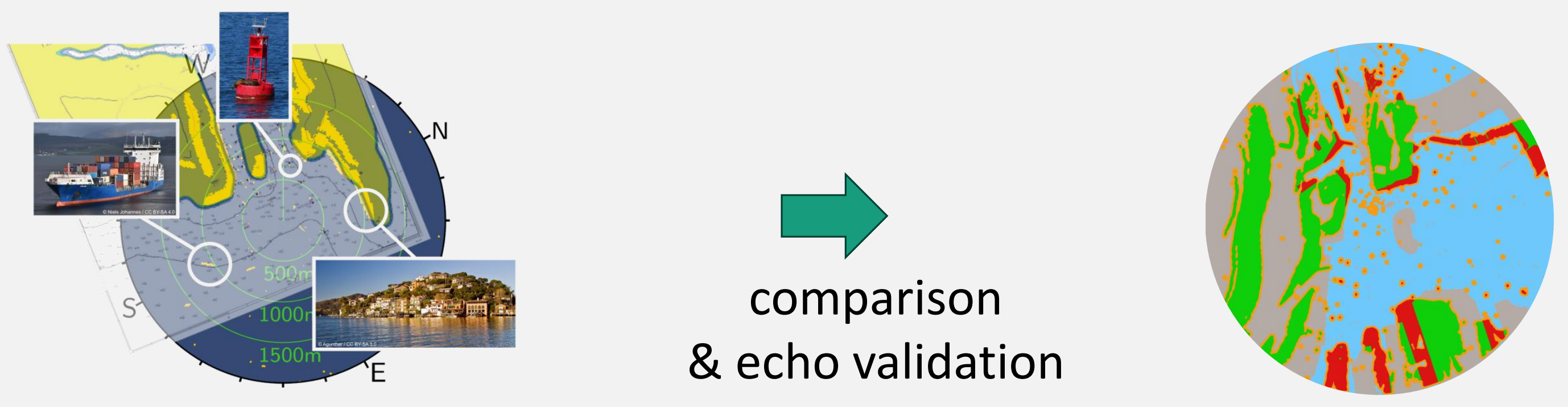


Chart-Diff

- Validate radar echos with objects on nautical chart
- Limited to areas close to the coast



Simulation Environment and RAT

[1] Wolsing *et al.*, “Network Attacks Against Marine Radar Systems: A Taxonomy, Simulation Environment, and Dataset”, LCN, 2022

[2] Saillard *et al.*, “Exploring Anomaly Detection for Marine Radar Systems”, CyberICPS, 2024

[3] Basels *et al.*, "DEMO: Maritime Radar Systems under Attack. Help is on the Way!", LCN, 2024