

Security-Informed Safety Educational Resource

Author: Dr Hossein Abroshan

Episode Title: Maritime GPS Spoofing and Navigation Integrity Failure (Novel Technologies and Resilience)

Associated Video: Episode 3 – Maritime GPS Spoofing and Navigation Integrity Failure

Prerequisites:

- Basic cyber security concepts
- Basic safety concepts
- Familiarity with cyber-physical systems (recommended)

1. Episode Overview

Purpose

Modern maritime navigation is heavily reliant on Positioning, Navigation, and Timing (PNT) information provided by Global Navigation Satellite Systems (GNSS). Maritime bridge systems for vessel position information include Electronic Chart Display and Information Systems (ECDIS), Automatic Identification Systems (AIS), route-monitoring functions, and track-control systems. These technologies increase the navigational accuracy and operational effectiveness of navigation, but also induce new dependencies on digital information.

Unlike most conventional safety risks, cyber incidents may be unrelated to damage to physical equipment. Instead, they can blur the validity of operational data and pose the danger of making unsafe decisions driven by inaccurate information.

GNSS spoofing is a major challenge in maritime environments. A successful spoofing attack can result in bridge systems that show a fake position for the vessel while appearing fully operable.

This episode deals with GNSS spoofing implications for navigational safety, how integrity loss caused by cyber-induced integrity failures can propagate through contemporary bridge systems, and robust navigation practices that can curtail danger.

2. Learning Outcomes

After completing this episode, students should be able to:

1. Explain the role of GNSS within modern maritime navigation systems.

2. Describe how ECDIS, AIS, radar, gyrocompass, speed logs, and echo sounders support vessel navigation.
3. Explain the difference between GNSS spoofing and GNSS jamming.
4. Analyse how compromised navigation information can influence operational decision-making.
5. Identify the relationship between information integrity and navigational safety.
6. Explain how cyber-induced integrity failures can propagate through cyber-physical systems.
7. Evaluate unsafe control actions associated with navigation information anomalies.
8. Describe resilience mechanisms used within mixed-trust sensor environments.
9. Explain the importance of human oversight during navigation uncertainty.
10. Apply Security-Informed Safety principles to maritime navigation systems.

3. Security-Informed Safety Focus

Core Principle

Cyber events become safety hazards when compromised information influences operational decisions and physical system behaviour.

Cyber-to-Physical Relationship

The attacker does not directly control the vessel.

Instead, the attack compromises a trusted source of navigation information.

The compromised information influences:

- Navigation displays.
- Route monitoring.
- Steering assistance.
- Human decision making.

The resulting hazard emerges from the interaction between technology, automation, and human operators.

Several unsafe control actions may contribute to escalation:

- Treating GNSS as the sole authoritative position source.
- Ignoring discrepancies between radar and ECDIS.
- Assuming AIS confirms own-vessel position.
- Continuing automated track control after navigation inconsistencies appear.
- Delaying manual intervention.

The scenario therefore highlights the importance of understanding both cyber vulnerabilities and operational safety responsibilities.

4. Suggested Teaching Plan

Introduction

Introduce:

- Maritime navigation systems
- GNSS and Positioning, Navigation and Timing (PNT)
- ECDIS
- AIS
- Navigation integrity
- Safe navigation corridors

Questions to ask:

- How does a vessel know where it is?
- What happens if navigation information becomes inaccurate?
- Why might a system appear normal while still creating safety risk?

Video Activity

Students watch the episode.

Encourage students to identify:

- Assets
- Threats
- Hazards
- Safety consequences
- Information dependencies
- Resilience mechanisms

Worksheet Activity

Students complete:

- Hazard–Threat Mapping
- Cyber-to-Physical Escalation Analysis
- Incident Response Exercise
- Mitigation Analysis

Discussion

Facilitate discussion around:

- Information integrity
- Mixed-trust sensor environments
- Human oversight
- Navigation resilience
- Security-Informed Safety implications

Debrief

Summarise key lessons.

Reinforce Security-Informed Safety concepts.

5. Discussion Questions

Technical Discussion

1. What role does GNSS play within modern bridge systems?
2. How does ECDIS use navigation information?
3. What is the difference between GNSS spoofing and GNSS jamming?
4. Why can navigation integrity failures become safety-critical?

Security-Informed Safety Discussion

1. Why does the attack remain difficult to detect initially?
2. How does compromised information influence operational decisions?
3. What unsafe control actions contribute to escalation?
4. Why is GNSS not sufficient as a sole source of navigation information?

Reflection Questions

1. Which navigation systems should be considered independent sources of verification?
2. What role does the bridge team play when navigation information becomes inconsistent?
3. How could resilience have been improved?
4. Why is human judgement still important in highly automated environments?
5. How does this scenario illustrate Security-Informed Safety?

6. Instructor Facilitation Notes

The worksheet activities are intended to support discussion and critical analysis rather than produce a single correct answer.

Students should be encouraged to:

- distinguish cyber events from hazards and harm
- identify cyber-to-physical escalation pathways
- consider both cyber security and safety perspectives
- evaluate trade-offs between operational, security, and safety objectives
- justify their decisions using evidence from the scenario

Instructors may adapt discussions and expected outcomes according to the background, experience, and level of the student cohort.

Many activities are intentionally open-ended and designed to encourage multidisciplinary reasoning rather than recall of specific facts.

7. Key Technical Concepts

- GNSS
- Positioning, Navigation and Timing (PNT)
- ECDIS
- AIS
- Radar and ARPA
- Gyrocompass
- Speed log
- Echo sounder
- Navigation integrity
- GNSS spoofing
- Information assurance
- Mixed-trust sensor environments
- Human oversight
- Security-Informed Safety

8. CyBOK Knowledge Area Mapping

Learning Activity	CyBOK Knowledge Area(s)
Hazard–Threat Mapping	Risk Management & Governance; Cyber-Physical Systems Security
Cyber-to-Physical Escalation Analysis	Cyber-Physical Systems Security
Incident Response Exercise	Security Operations & Incident Management; Cyber-Physical Systems Security

Mitigation Analysis	Cyber-Physical Systems Security; Physical Layer & Telecommunications Security
GNSS Spoofing and Navigation Integrity Discussion	Physical Layer & Telecommunications Security; Cyber-Physical Systems Security
Navigation Integrity and Cross-Sensor Validation Discussion	Cyber-Physical Systems Security; Physical Layer & Telecommunications Security
Human Oversight and Operational Decision-Making Discussion	Human Factors; Cyber-Physical Systems Security
Security-Informed Safety Discussion	Cyber-Physical Systems Security; Human Factors

9. Alignment with Security-Informed Safety

Key Message

This episode demonstrates that cyber attacks do not need to damage equipment or disrupt communications to create significant safety risks.

By compromising navigation data integrity, a GNSS spoofing attack can create a false understanding of vessel position while all bridge systems continue to appear operational.

The scenario highlights the importance of:

- Security-informed safety engineering.
- Independent verification of critical information.
- Human-centred resilience.
- Defence-in-depth for navigation systems.
- Mixed-trust sensor architectures.

Safe navigation depends not only on accurate sensors but also on the ability to recognise when trusted information can no longer be trusted.

10. Additional Resources

Relevant Standards and Guidance:

- International Maritime Organization (IMO) Guidance on Maritime Cyber Risk Management
- NISTIR 8323 – Foundational Positioning, Navigation, and Timing (PNT) Profile
- IEC 61162 Series – Maritime Navigation and Radiocommunication Equipment and Systems

- IALA Guidelines on Resilient Positioning, Navigation and Timing
- Security-Informed Safety

Instructor Notes

The primary objective is not to teach GNSS spoofing techniques.

The primary objective is to help students understand how cyber-induced integrity failures can influence physical operations and create navigational safety hazards.

Students should leave the session understanding the distinction between:

- Cyber event
- Information integrity failure
- Hazard
- Potential harm

and the importance of independent verification, diverse navigation sources, human oversight, and resilience in mixed-trust sensor environments.

The key Security-Informed Safety lesson is that trusted information can become untrusted while systems continue to appear fully operational.