

Security-Informed Safety Educational Resource

Author: Dr Hossein Abroshan

Episode Title: Railway Signalling Patch Leading to Near-Collision (Patching, Safety Cases and Security-Informed Safety)

Associated Video: Episode 2 - Railway Signalling Patch Leading to Near-Collision

Prerequisites:

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

1. Episode Overview

Purpose

This episode explores a real-world scenario in which an emergency cyber security patch is deployed within an ETCS Level 2 signalling environment. While this update manages to alleviate a cyber security issue, lack of safety validation presents a unique potential operational risk. The resulting signalling degradation reduces train separation margins and creates a near-collision situation that is ultimately prevented by onboard ETCS protection.

This episode is an example of a foundational tenet of Security-Informed Safety:

Improving cyber security does not automatically improve safety. Operational railway systems that require change to achieve security objectives should be evaluated along with safety objectives.

2. Learning Outcomes

After completing this episode, students should be able to:

1. Describe the purpose of railway signalling systems.
2. Explain the operation of ETCS Level 2.
3. Describe the roles of the Radio Block Centre (RBC), electronic interlocking and onboard ETCS equipment.
4. Explain how Movement Authorities are generated and enforced.
5. Understand the purpose of railway safety cases.
6. Explain why software changes require safety assurance.
7. Analyse how emergency cyber security actions can create safety risks.

8. Identify unsafe change-management practices.
9. Explain how ETCS protection mechanisms prevent hazardous situations.
10. Apply Security-Informed Safety principles to railway environments.

3. Security-Informed Safety Focus

Core Principle

Improving cyber security does not automatically improve safety.

Operational railway systems that require change to achieve security objectives should be evaluated along with safety objectives.

Cyber-to-Physical Relationship

The progression from cyber security action to physical risk occurs through a sequence of linked events.

Security Vulnerability Identified → Emergency Patch Deployment → Incomplete Safety Validation → Unexpected Software Timing Behaviour → Delayed Movement Authority Updates → Reduced Train Separation Margin → Near-Collision Hazard

The scenario demonstrates that hazards may emerge even when cyber security actions are well intentioned.

The problem is not malicious activity.

The problem is insufficient understanding of how cyber security decisions influence safety-critical behaviour.

4. Suggested Teaching Plan

Introduction

Introduce:

- Railway signalling systems
- ETCS Level 2
- Movement Authorities
- Train separation
- Safety-critical railway operations
- Railway safety cases

Questions to ask:

- Why must trains remain safely separated?
- What happens if signalling information becomes inaccurate or delayed?

- Why are software changes treated differently in safety-critical systems?

Video Activity

Students watch the episode.

Encourage students to identify:

- Assets
- Threats
- Hazards
- Safety consequences
- Cyber security controls
- Safety controls

Worksheet Activity

Students complete:

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

Discussion

Facilitate discussion around:

- Security-Informed Safety implications
- Emergency patch governance
- Safety assurance
- Operational change management
- Independent protection mechanisms

Debrief

Summarise key lessons.

Reinforce Security-Informed Safety concepts.

5. Discussion Questions

Technical Discussion

1. What role does the Radio Block Centre play in train separation?
2. Why is Movement Authority critical to railway safety?

3. What role does the Engineering Workstation play within the signalling environment?
4. Why can timing failures become safety-critical?

Security-Informed Safety Discussion

1. Why are railway software updates treated differently from traditional IT updates?
2. How did the cyber security patch contribute to the hazard?
3. What is the purpose of a railway safety case?
4. What safety mechanisms prevented a collision?

Reflection Questions

1. How could the patching process have been improved?
2. Which barriers failed and which barriers succeeded?
3. How does this scenario illustrate Security-Informed Safety?
4. Could the cyber security team's decision be considered reasonable?
5. How should cyber security and safety teams coordinate during urgent operational changes?

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

- Railway signalling systems
- ETCS Level 2

- Radio Block Centres (RBC)
- Electronic Interlocking
- GSM-R communication
- Movement Authorities
- Braking supervision
- Railway safety cases
- Safety assurance
- Software change management
- Cyber-to-physical escalation
- Independent protection layers
- 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	Risk Management & Governance; Secure Software Lifecycle; Cyber-Physical Systems Security
Patch Governance and Safety Assurance Discussion	Secure Software Lifecycle; Cyber-Physical Systems Security; Risk Management & Governance
Security-Informed Safety Discussion	Cyber-Physical Systems Security; Risk Management & Governance

9. Alignment with Security-Informed Safety

Key Message

This scenario is neither purely a cyber security problem nor purely a safety problem.

The cyber security team acted to reduce exposure to a known vulnerability.

The safety issue emerged because assurance activities were not completed before operational deployment.

Cyber security and safety objectives were both reasonable.

The difficulty arose because they were considered independently.

Security-Informed Safety recognises that:

- cyber security actions can affect safety
- safety decisions can affect cyber security
- effective risk reduction requires coordinated decision-making

An understanding of how cyber security and safety interact is central to Security-Informed Safety and one of the key lessons of this episode.

10. Additional Resources

Relevant Standards and Frameworks:

- EN 50126
- EN 50128
- EN 50129
- CSM-REA
- IEC 62443
- NIST SP 800-82
- Security-Informed Safety

Instructor Notes

The primary objective is not to teach railway cyberattacks.

The primary objective is to help students understand how cyber security decisions can influence safety-critical railway behaviour and why cyber security, safety assurance, engineering, and operational decision-making must be considered together.

Students should leave the session understanding the distinction between:

- Security vulnerability
- Cyber security action
- Hazard
- Potential harm

and the importance of safety assurance, independent protection layers, and coordinated cyber-safety governance in safety-critical railway environments.