Applying Penetration Testing Techniques to Strengthen ERTMS Communication Security

Presented by:
Yasmine Benghename,
PhD student,
yasmine.benghename@hds.utc.fr

Région Hauts-de-France
RAiLENiUM RAIL RESEARCH & INNOVATION
heudiasyc
ALLIANCE SORBONNE UNIVERSITÉ
utc

Table of **contents**

- Introduction
- Cyberattacks Over the Last Two Decades
- Cyberattacks on Poland's Rail Network
- Research Objectives
- Defining the Security Analysis Process
- Applying the Security Analysis Process to the BTS
- Findings and Realizations
- Conclusion & Future Work

ERTMS : European Rail Traffic Management System

ETCS : European Train Control System

BTS: EuroBalise Transmission System

Introduction

Modernization of Railway Systems

- The railway industry has undergone significant transformations with the introduction of digital technologies, which have revolutionized operations.
- While these advancements have improved operational efficiency, they have also introduced **new vulnerabilities.**

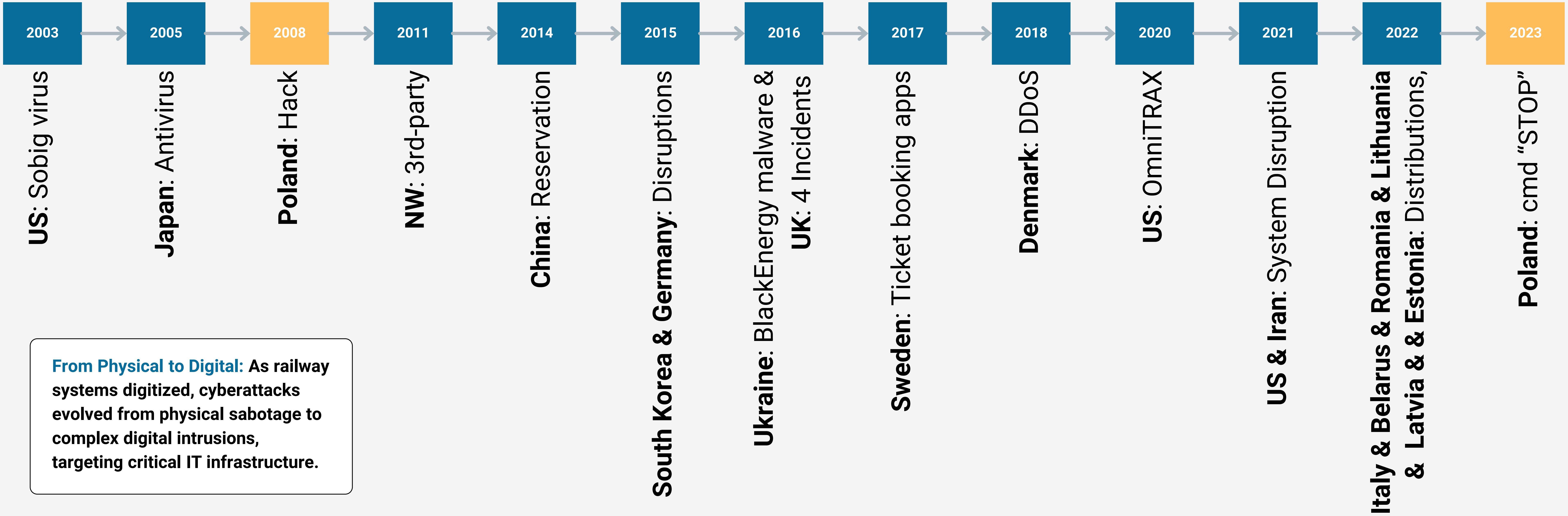
Importance of Cybersecurity

- In the context of railway systems, cybersecurity threats involve unauthorized access, data breaches, and attacks on critical infrastructure components such as signaling and control systems. These threats can **disrupt operations**, **compromise safety,** and result in significant **financial losses.**

Research Focus

This research aims to **identify and analyze vulnerabilities** within the ERTMS/ETCS transmission system, particularly **focusing on the Eurobalise** component, and to assess the effectiveness of existing safety and security measures in mitigating these risks.

Cyberattacks Over the Last **Two Decades**



2003 — **US**: Sobig virus

2005 — **Japan**: Antivirus

2008 — **Poland**: Hack

2011 — **NW**: 3rd-party

2014 — **China**: Reservation

2015 — **South Korea & Germany**: Disruptions

2016 — **Ukraine**: BlackEnergy malware & **UK**: 4 Incidents

2017 — **Sweden**: Ticket booking apps

2018 — **Denmark**: DDoS

2020 — **US**: OmniTRAX

2021 — **US & Iran**: System Disruption

2022 — **Italy & Belarus & Romania & Lithuania & Latvia & & Estonia**: Distributions,

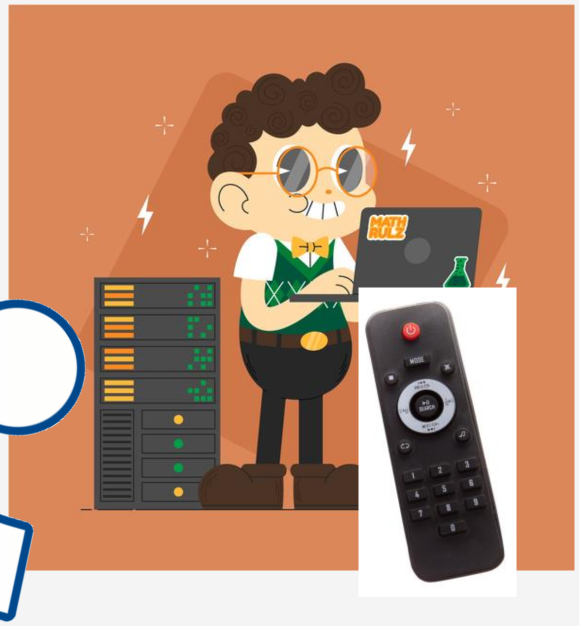
2023 — **Poland**: cmd "STOP"

From Physical to Digital: As railway systems digitized, cyberattacks evolved from physical sabotage to complex digital intrusions, targeting critical IT infrastructure.

Cyberattacks on Poland's Rail Network

2008 Attack: A Notorious Cyberattack on Poland's Railway System

- Four trams derailed
- Emergency stops injured passengers
- A dozen people hurt



2023 Attack: The Cyber Sabotage of Polish Railways

- No injuries
- No damage
- Sabotage operation affected radio systems

Quiz: Let’s Hear Your Insights!

Question: What was the key factor that allowed the 2023 Poland railway cyberattack to succeed?

a) Use of outdated radio technology
b) Insider involvement
c) Inadequate firewalls
d) Lack of employee cybersecurity training

a) Use of outdated radio technology

The attack was possible due to **a combination of factors**

Vulnerability of the railway network

The Polish railway network used older radio technology that was susceptible to interference and manipulation.

Availability of the equipment

he equipment used for the attack, such as radio transmitters and receivers, is widely available.

Lack of sufficient security measures

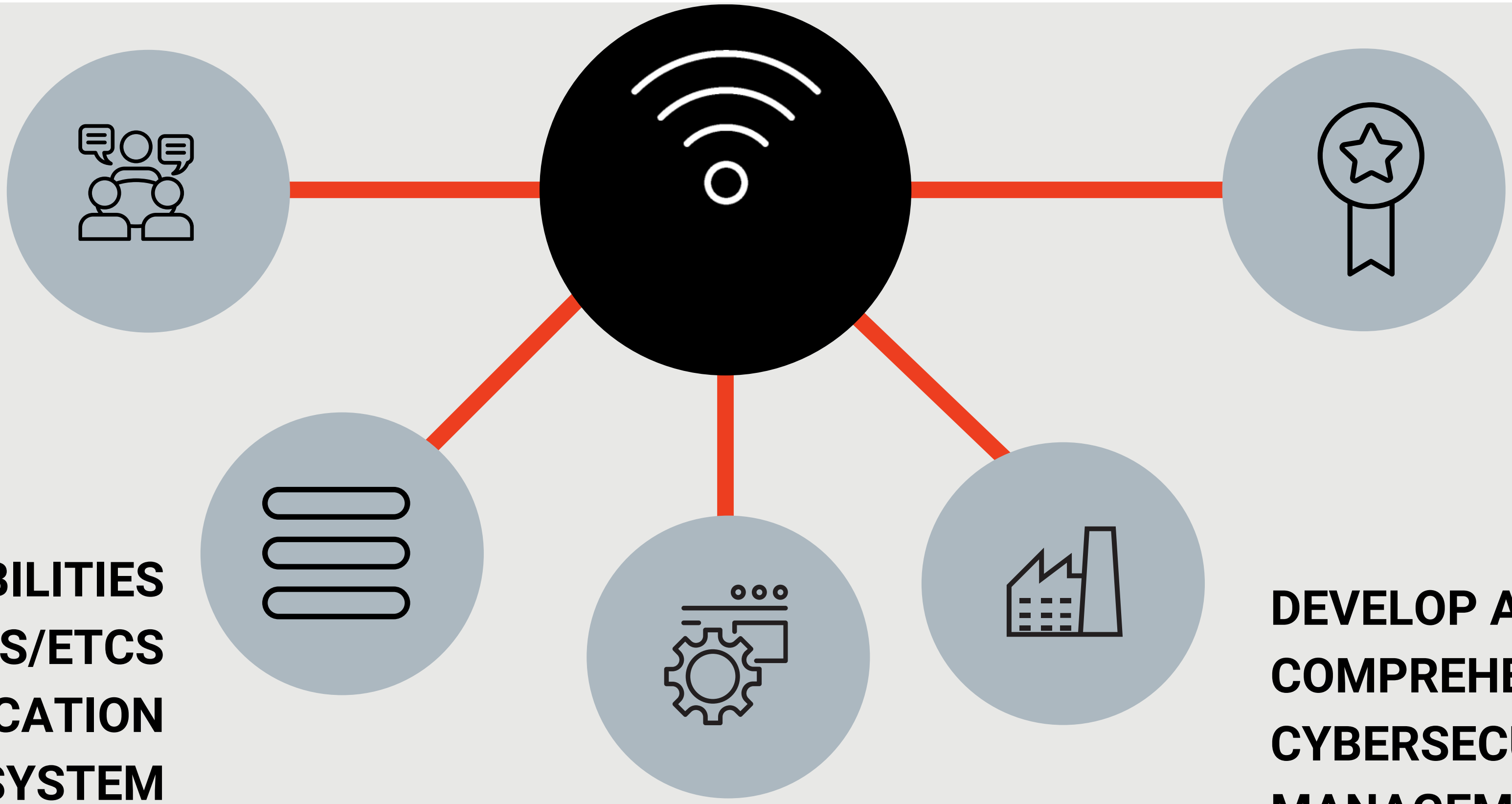
The Polish railway network may not have had adequate security measures in place to prevent such attacks.

Potential insider knowledge

t is possible that the attackers had insider knowledge of the railway network, which may have helped them plan and execute the attack more effectively.

Research **Objectives**

Current Objective: Enhance the cybersecurity of modern railway systems, specifically focusing on identifying and mitigating vulnerabilities within the ERTMS/ETCS transmission system;



ANALYZE EXISTING SECURITY GAPS IN RAILWAY SYSTEMS

ASSESS VULNERABILITIES IN THE ERTMS/ETCS COMMUNICATION SYSTEM

EVALUATE THE RISK OF CYBERATTACKS ON RAILWAY OPERATIONS

DEVELOP A COMPREHENSIVE CYBERSECURITY RISK MANAGEMENT FRAMEWORK

VALIDATE THE EFFECTIVENESS OF CYBERSECURITY SOLUTIONS

Final Objective: Develop a comprehensive risk management framework that integrates both safety and security to protect against evolving cyber threats.

Région Hauts-de-France
RAILENIUM RAIL RESEARCH & INNOVATION
heudiasyc
ALLIANCE SORBONNE UNIVERSITÉ
utc

Breaking Down Key Security Terms

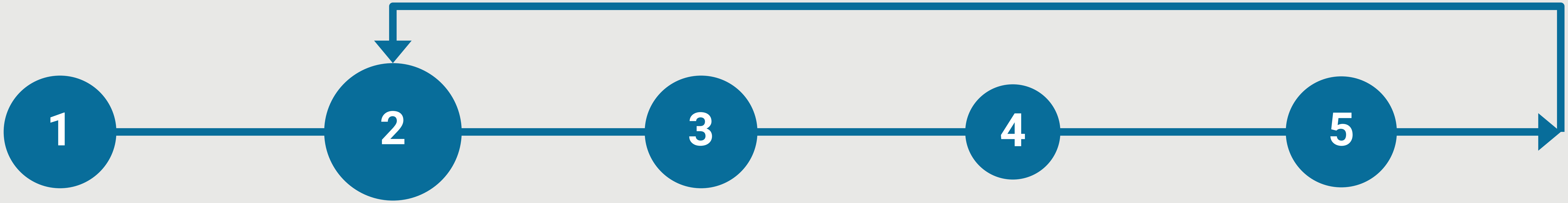
A vulnerability in cybersecurity is a weakness in a host or system, such as a missed software update or system misconfiguration, that can be exploited by cybercriminals to compromise an IT resource and advance the attack path. (CrowdStrike)

A threat is a malicious act that can exploit a security vulnerability. (CrowdStrike)

Weaknesses are errors that can lead to vulnerabilities. (CWE)

A risk is what happens when a cyber threat exploits a vulnerability. It represents the damage that could be caused to the organization in the event of a cyberattack. (CrowdStrike)

Five-Stage **Penetration Testing** Methodology



PLAN

- Define Goals;
- **Gather Information;**
- Passive Reconnaissance.

SCAN

- Identify potential vulnerabilities in the target system;
- **Dig deeper** into the system, identifying misconfigurations and potential weaknesses.

GAIN & MAINTAIN ACCESS

- **Exploitation**;
- Privilege escalation.

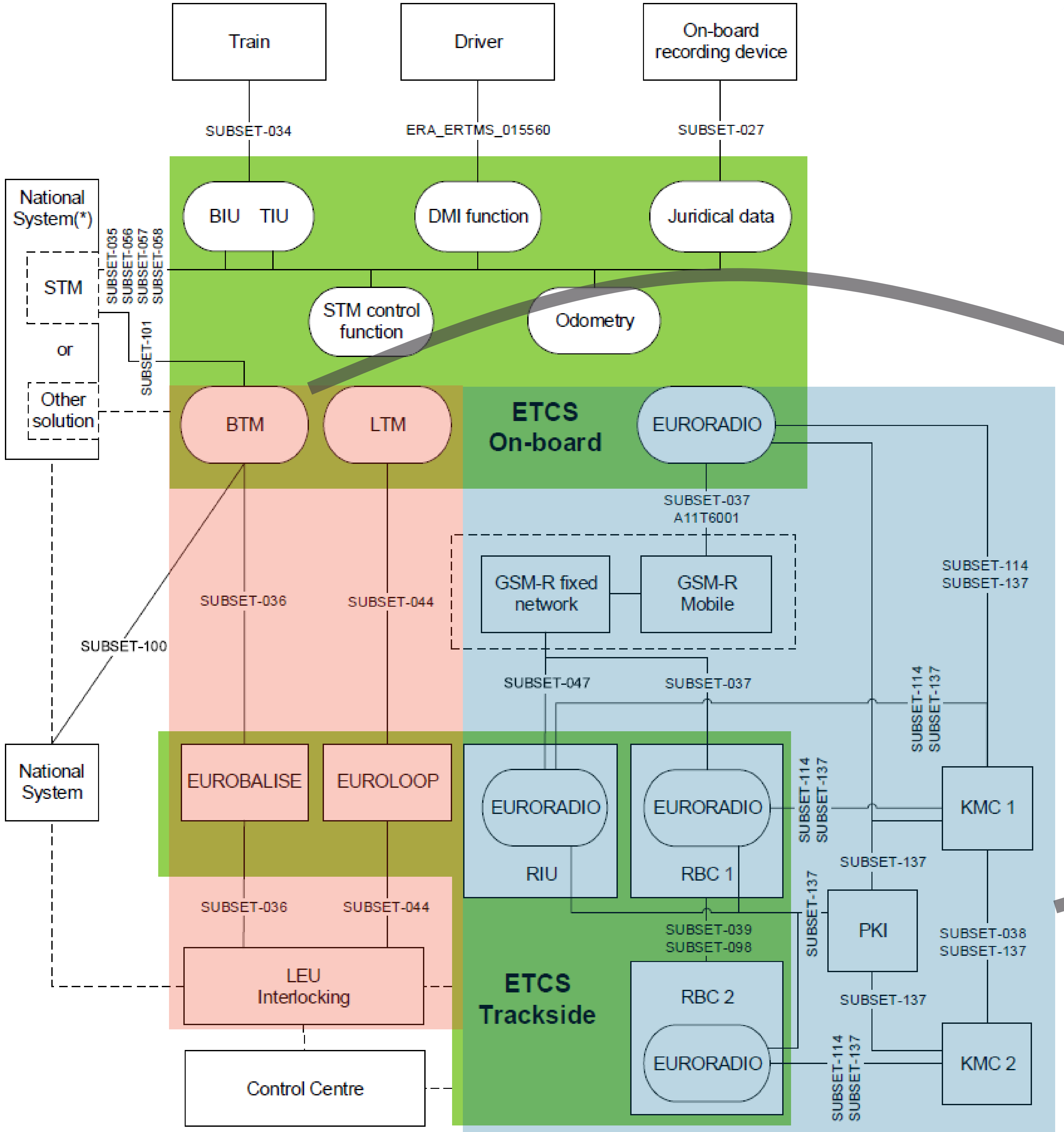
ANALYZE & REPORT

- Analyze the results of the penetration test.;
- Report writing.

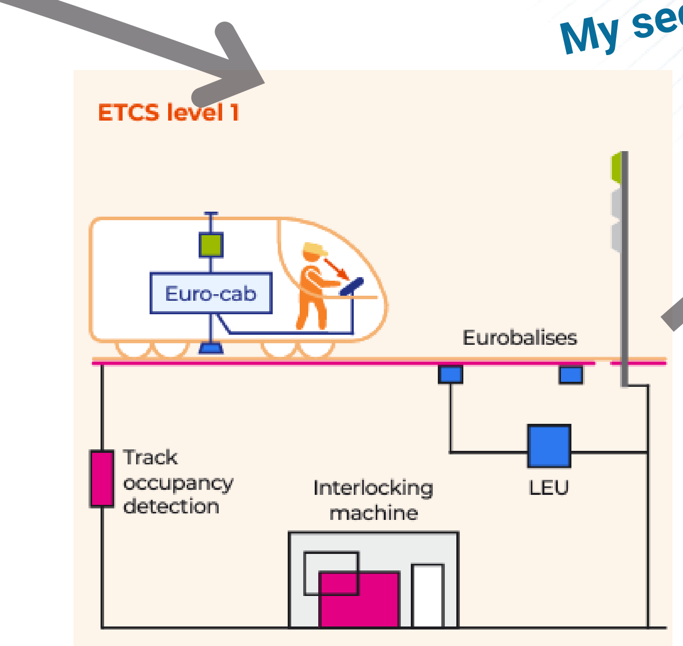
REMEDIATION

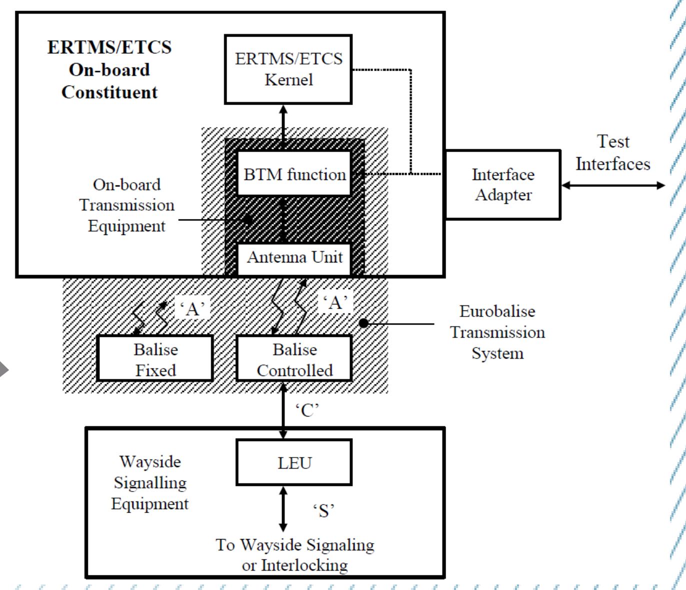
- Fix the identified vulnerabilities;
- Ensure that the vulnerabilities have been properly addressed.

PLAN: Overview of ERTMS/ETCS System



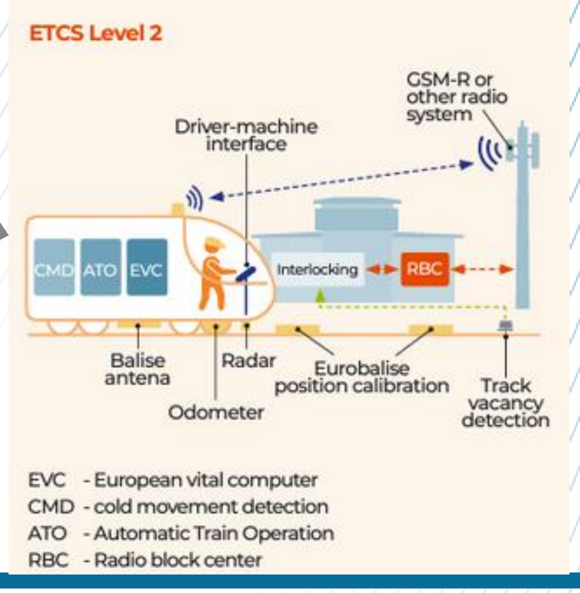
My security analysis will focus on the BTS as the target system.





ERTMS/ETCS On-board Constituent
ERTMS/ETCS Kernel
On-board Transmission Equipment
BTM function
Antenna Unit
Interface Adapter
Test Interfaces
'A'
'A'
Balise Fixed
Balise Controlled
Eurobalise Transmission System
'C'
Wayside Signalling Equipment
LEU
'S'
To Wayside Signaling or Interlocking

ERTMS/ETCS Level 1 is an add-on system designed to work on existing conventional railway lines **already** equipped with lineside signals and train detectors.

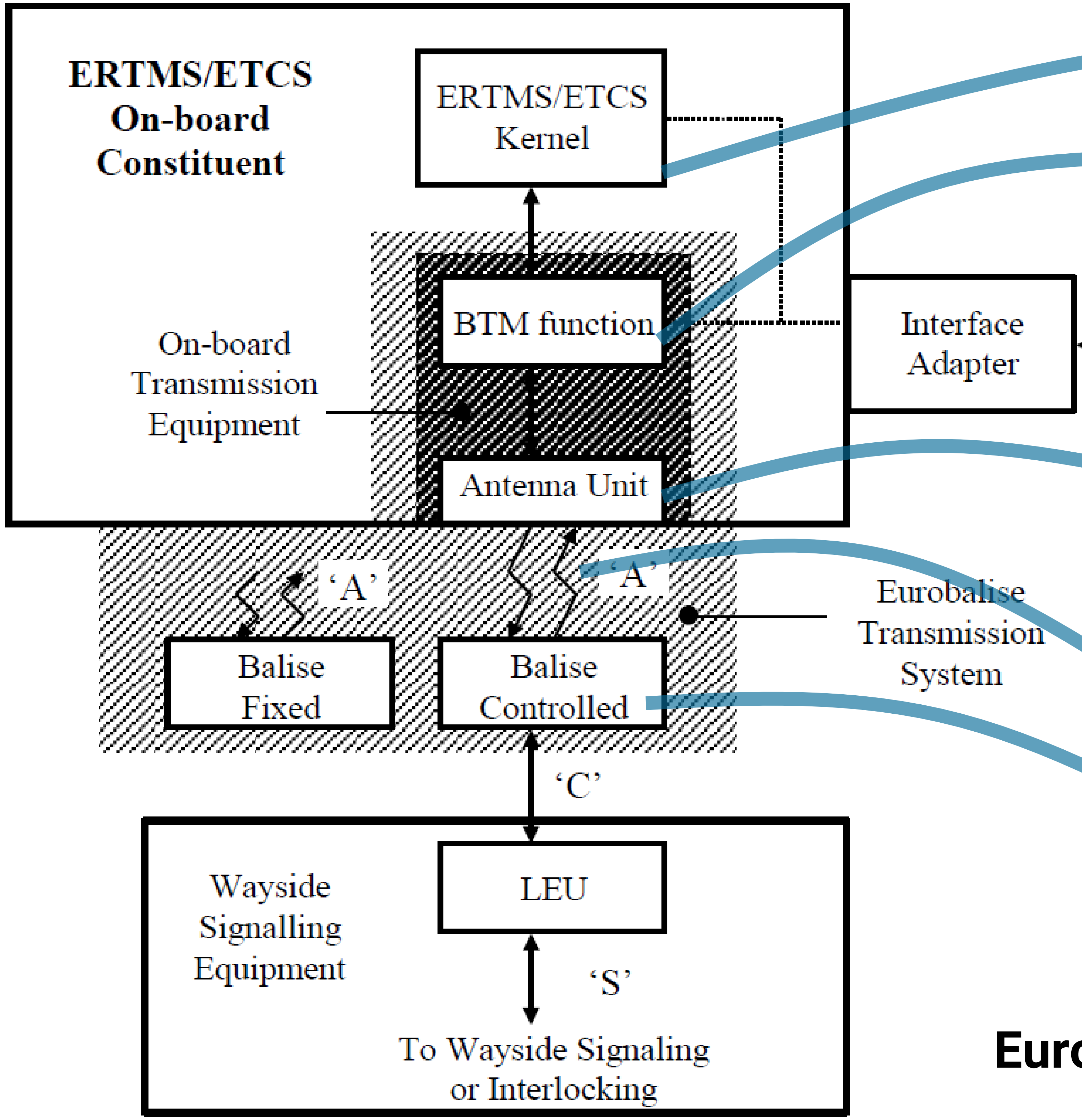


ETCS Level 2
GSM-R or other radio system
Driver-machine interface
CMD
ATO
EVC
Interlocking
RBC
Balise antena
Radar
Odometer
Eurobalise position calibration
Track vacancy detection
EVC - European vital computer
CMD - cold movement detection
ATO - Automatic Train Operation
RBC - Radio block center

ERTMS/ETCS Level 2 is a radio based signalling system which displays signalling and movement authorities **in the cab**, **eliminating** the need for lineside signals.

Région Hauts-de-France RAILENIUM RAIL RESEARCH & INNOVATION heudiasyc ALLIANCE SORBONNE UNIVERSITÉ utc

SCAN: The Eurobalise Transmission System (BTS)


ERTMS/ETCS On-board Constituent
ERTMS/ETCS Kernel
BTM function
Interface Adapter
On-board Transmission Equipment
Antenna Unit
'A'
'A'
Eurobalise Transmission System
Balise Fixed
Balise Controlled
'C'
Wayside Signalling Equipment
LEU
'S'
To Wayside Signaling or Interlocking

BTM Functions

EVC

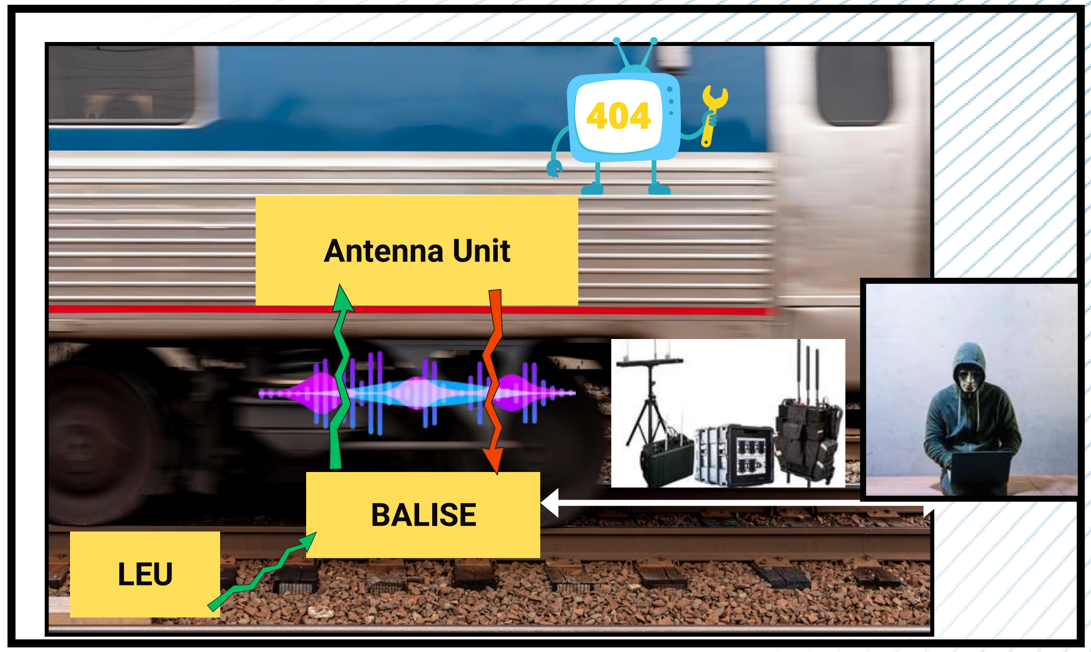
Antenna Unit

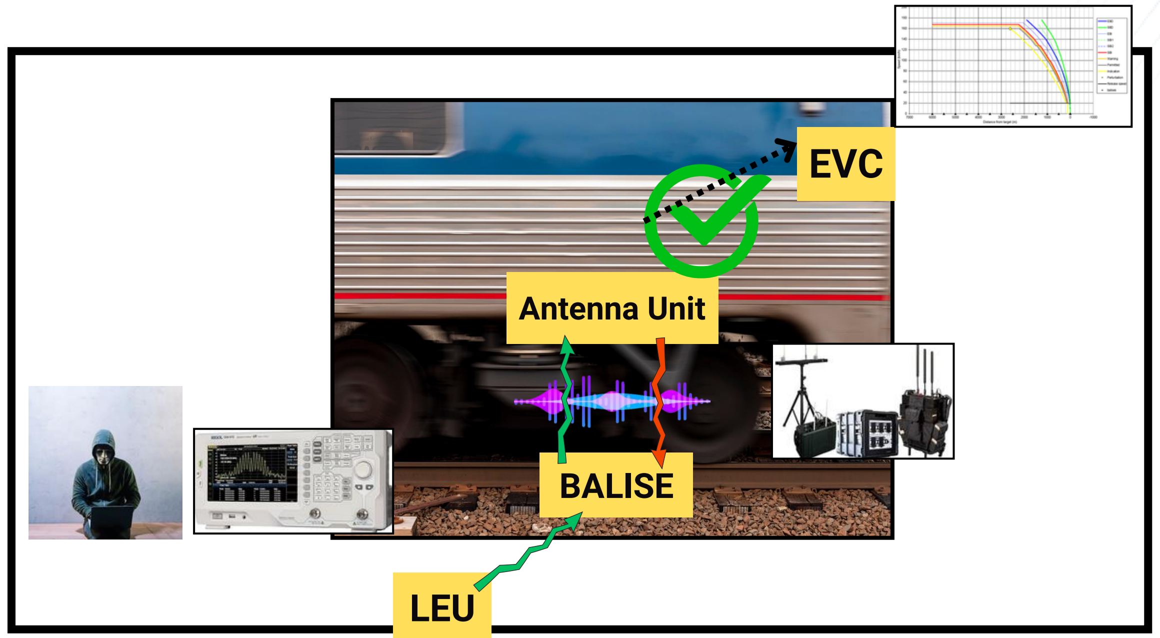
Shaped Data	cb	sb	esb	Check bits
83·11=913 or 21·11=231 bits	3 bits	12 bits	10 bits	85 bits

EuroBalise

1.Use of Coding Algorithm Instead of Encryption;
2.Absence of Authentication and identification;
3.No Formal User Access Rights Assignment;
4.Absence of Access Activity Tracking;
5.Lack of Timestamping for Data;
6.Vulnerability to Physical Access;
7.Unsecured area installation.

GAIN & MAINTAIN ACCESS





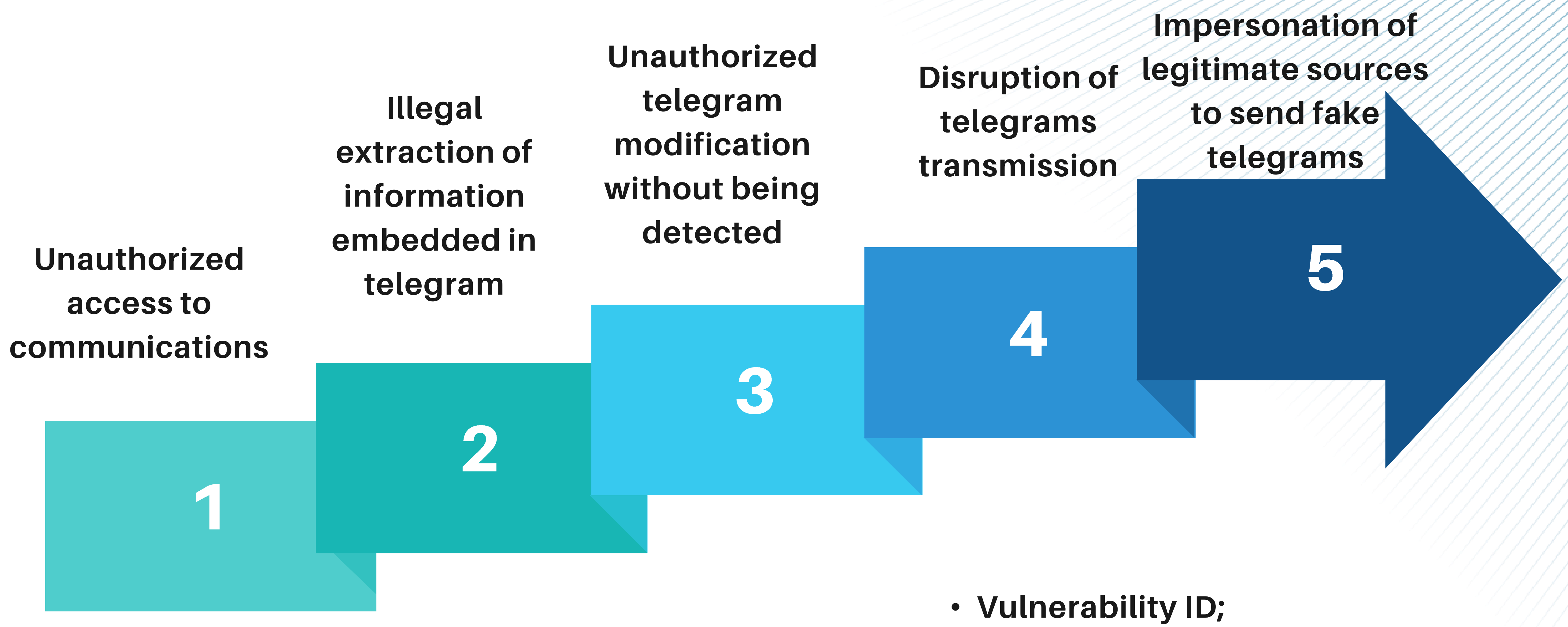
Quiz: Let’s Hear Your Insights!

Question: Which vulnerability in the BTS poses the highest risk for a potential cyberattack?

a) Absence of encryption
b) Lack of timestamping for data
c) Physical access to Eurobalise units
d) No formal user access rights assignment

a) Absence of encryption

ANALYZE & REPORT



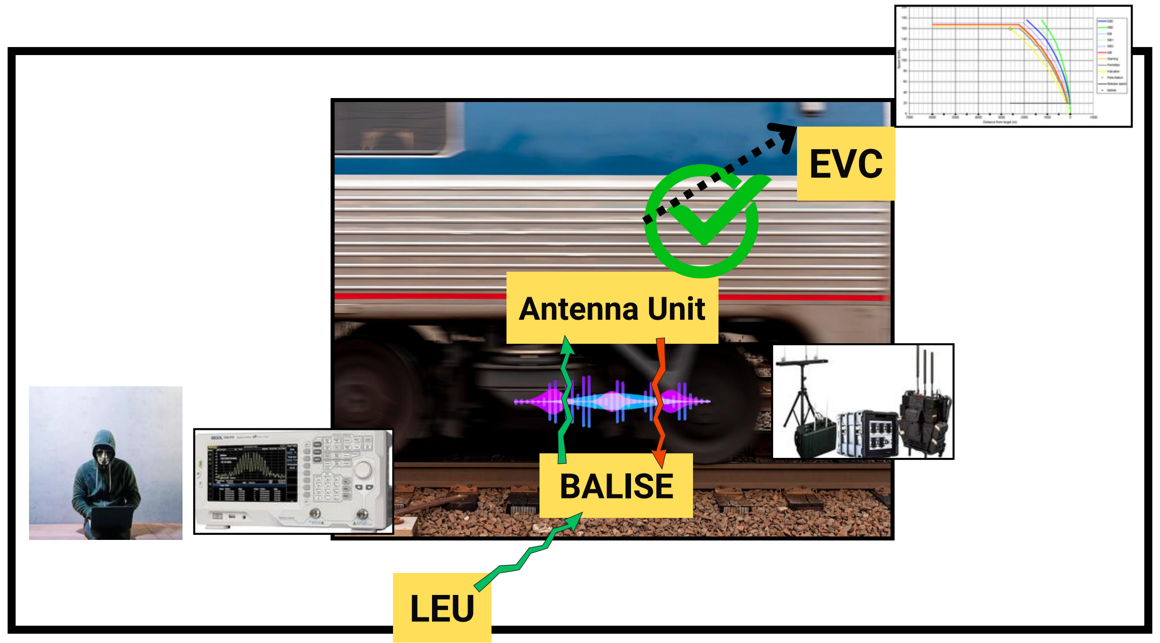
1 Unauthorized access to communications

2 Illegal extraction of information embedded in telegram

3 Unauthorized telegram modification without being detected

4 Disruption of telegrams transmission

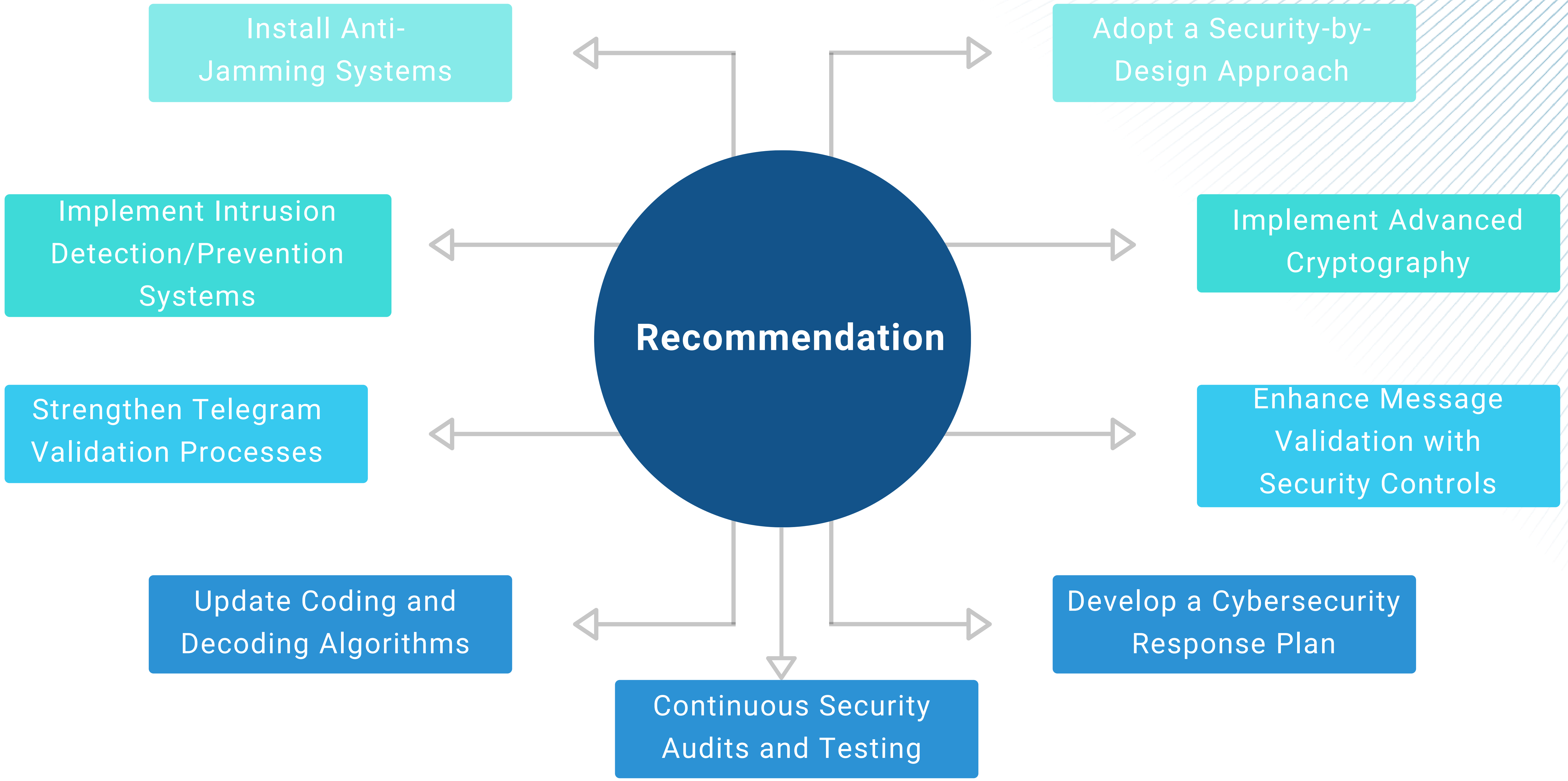
5 Impersonation of legitimate sources to send fake telegrams



What a Penetration Testing Report Looks Like?

- Vulnerability ID;
- Vulnerability Name/Description;
- Severity (CVSS);
- Impact;
- Likelihood;
- Risk Level;
- Root Cause;
- Exploitation Method;
- Affected Systems/Assets;
- Proof of Concept.

REMEDIATION



SHORT-TERM MITIGATIONS

Install Anti-Jamming Systems

Implement Intrusion Detection/Prevention Systems

Strengthen Telegram Validation Processes

Update Coding and Decoding Algorithms

Recommendation

Continuous Security Audits and Testing

STRATEGIC ENHANCEMENTS

Adopt a Security-by-Design Approach

Implement Advanced Cryptography

Enhance Message Validation with Security Controls

Develop a Cybersecurity Response Plan

Quiz: Let’s Hear Your Insights!

Scenario: Imagine a cybersecurity breach that halts train operations in a major city. What would be your first action to mitigate the impact?

a) Shut down the entire rail network to prevent further damage
b) Isolate the affected section and continue operations elsewhere
c) Alert the public to avoid travel until the issue is resolved
d) Attempt to quickly patch the system while monitoring other sections

For this scenario, the answer could be either a) or b)

Conclusion & **Future Work**

Ensuring Rail Safety and Security

In conclusion, as railway systems continue to evolve, so do the cyber threats they face. Ensuring robust cybersecurity is now essential for maintaining the safety and reliability of modern rail networks. By addressing vulnerabilities in critical systems like ERTMS/ETCS, we can protect the future of rail transportation against these emerging risks.

Ongoing Lab Project: Launching New Lab Platform

***Objective:* Upgrade the current railway platform in our lab by integrating cutting-edge communication technologies.**
***Goal:* Validate the effectiveness of our cybersecurity solutions and recommendations in a controlled, emulated environment**

Quiz: Let’s Hear Your Insights!

Question: What is the most significant cybersecurity challenge expected with the introduction of autonomous trains?

a) Increased attack surface due to digital communication
b) Difficulty in monitoring real-time threats
c) Securing communication between trains and control centers
d) Ensuring safety and security integration

a) Increased attack surface due to digital communication

Région Hauts-de-France

RAiLENiUM RAIL RESEARCH & INNOVATION

heudiasyc

ALLIANCE SORBONNE UNIVERSITÉ | utc

Thank you for **your attention.**

Connect **with me.**

E-mail

yasmine.benghename@hds.utc.fr

LinkedIn

www.linkedin.com/in/yasmine-benghename