Cyber Security for Railway Signalling

Dr. Cédric LÉVY-BENCHETON

Network and Information Security Expert

European Union Agency for Network and Information Security

How to protect signalling system against cybercrime – UIC, Paris, 28 January 2015

Summary

- Presentation of ENISA
- Cyber Security for Railway Signalling
- Conclusion

EU Cyber Security Strategy

- The Five strategic objectives of the strategy:
  - Achieving cyber resilience
  - Drastically reducing cybercrime
  - Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
  - Developing the industrial and technological resources for cybersecurity
  - Establishing a coherent international cyberspace policy for the European Union and promote core EU values

ENISA explicitly called upon

Presentation of ENISA

- The European Union Agency for Network and Information Security was formed in 2004. The original mandate was renewed and extended in 2013

- The Agency is a Centre of Expertise that supports the Commission and the EU Member States in the area of information security

- We facilitate the exchange of information between communities, with particular emphasis on the EU institutions, the public sector and the private sector

ENISA Activities

Recommendations

Policy Implementation

Mobilising Communities

Hands on

ENISA and Transport: preparatory study

- Challenges found
  - Cyber security is a difficult area for transport operators
  - Security of a “system of systems”
  - Cohabitation between old and new technologies

- Issues raised by public transport operators
  - No clear definition of cyber security for transport in the EU
  - Lack of information sharing and coordination
  - Lack of framework for securing exchanges in the Smart City

- Two ENISA studies in 2015
  - Architecture model to map interactions with other operators
  - Good practices and recommendations adapted to the sector

Summary

- Presentation of ENISA
- Cyber Security for Railway Signalling
- Conclusion

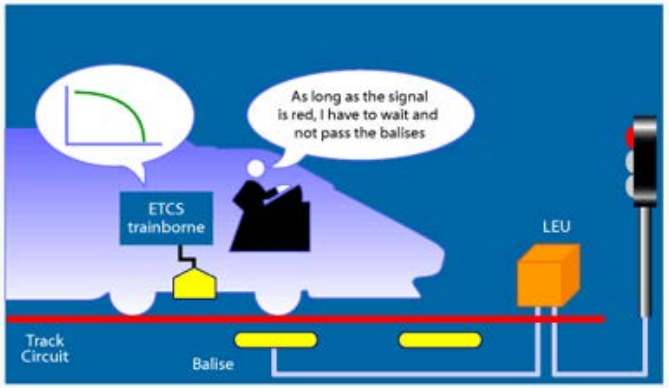
Railway is a critical infrastructure

- Cyber security
  - Ensure confidentiality, integrity, availability
  - Protect critical assets from cyber threats

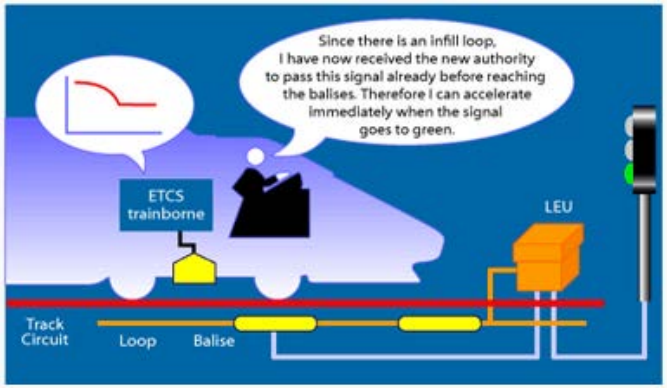
- What happens if something goes wrong?
  - Trains stop (Emergency Brake)
  - Economical impact
  - Loss of trust
  - Human casualties

Evolution toward IP-connected railway signalling

ERTMS Level 1

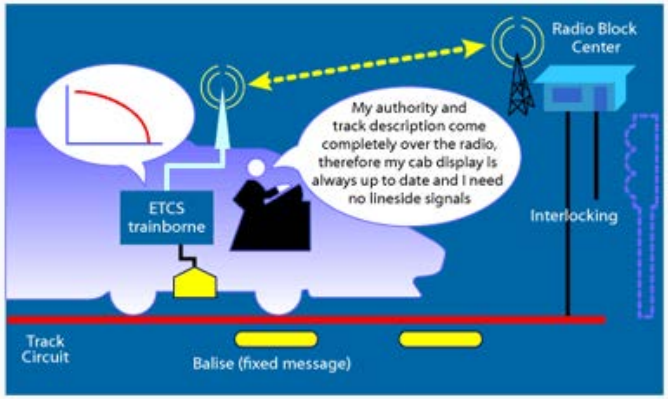


Eurobalise without infill



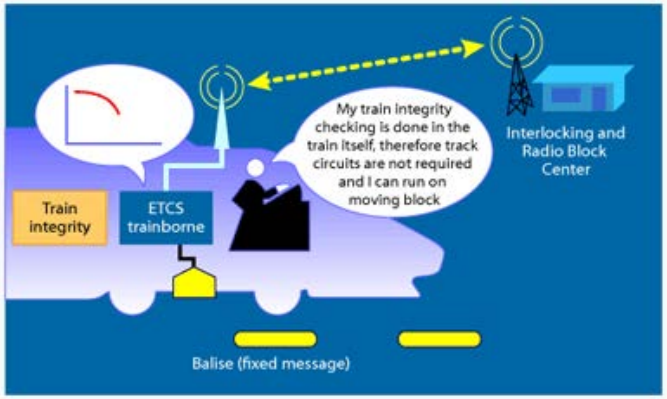
Eurobalise + infill (euroloop, radio, or extra balises)

ERTMS Level 2



Eurobalise + Euroradio (GSM-R) + Radio Block Center

ERTMS Level 3



Eurobalise + Euroradio (GSM-R) + Radio Block Center

Source: ERTMS.net

Threat Landscape for Internet Infrastructure

Threat groups	Threat types	Trends
Routing Threats	Nefarious Activity/Abuse	Increasing
	Eavesdropping/Interception/Hijacking	Increasing
DNS Threats	Nefarious Activity/Abuse	Decreasing
Denial of Service	Nefarious Activity/Abuse	Increasing
Generic Threats	Physical attack	N/A
	Damage/Loss	Increasing
	Failures/Malfunctions	Increasing
	Nefarious activity/Abuse	Increasing
	Eavesdropping/Interception/Hijacking	Increasing

- Current threats and assets exposed
- Good practices to overcome these threats
- Recommendations to enhance the security level

Particularities of ERTMS

- A system of systems
  - Central systems
  - Network connections
  - Trackside equipment
  - Radio links
  - On-board equipment

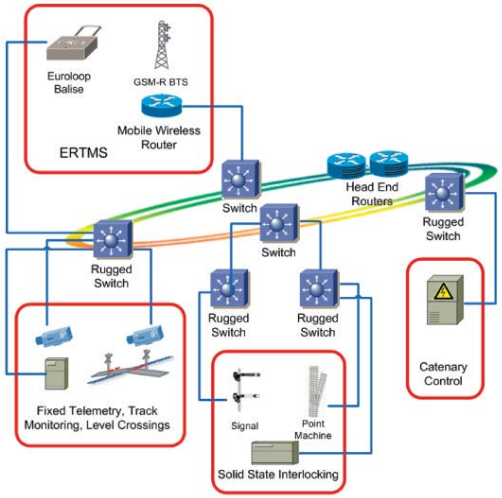
- Every sub-system has specific cyber security concerns
  - Railway uses ICT equipment
  - **Railway ≠ ICT**

Cyber security concerns – Central systems

Source: RFF

- **Integrity**
- **Availability**
- **Physical security**, for example against unauthorized access
- **Processes**, such as monitoring and reporting

Cyber security concerns – Network connections



Source: Cisco

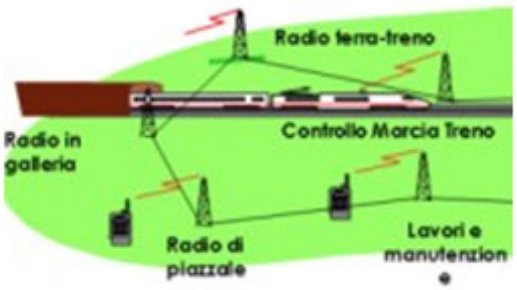
- **Availability** is critical
- **Resilience**, for example against cable theft
- **"COTS" network components**
- **Multi-services network**: sharing of equipment and cables
- **Internet threats** (DDoS, Routing…)

Cyber security concerns – Trackside equipment

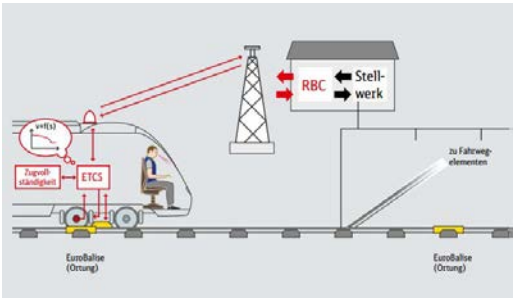
Source: Wikipedia

- **Availability**
- **Integrity**
- **Physical security** (vandalism, weather conditions…)
- **External dependencies** (power supply…)

Cyber security concerns – Radio links



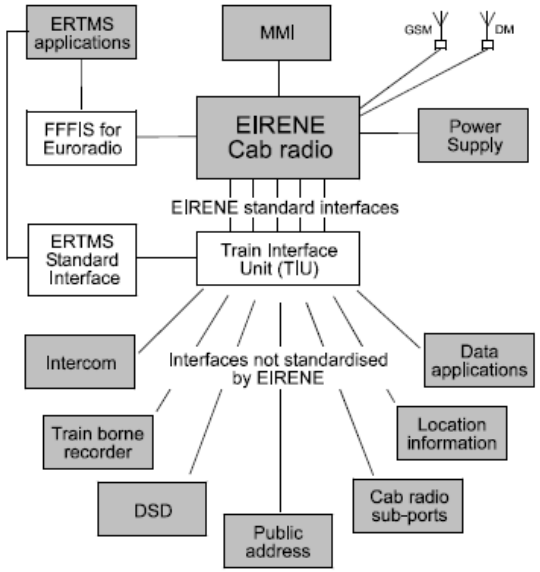
Source: RFI



Source: DB Netz

- **Jamming**
- Failed **handover**
- **Integrity** of messages
- **Capacity** of the radio link

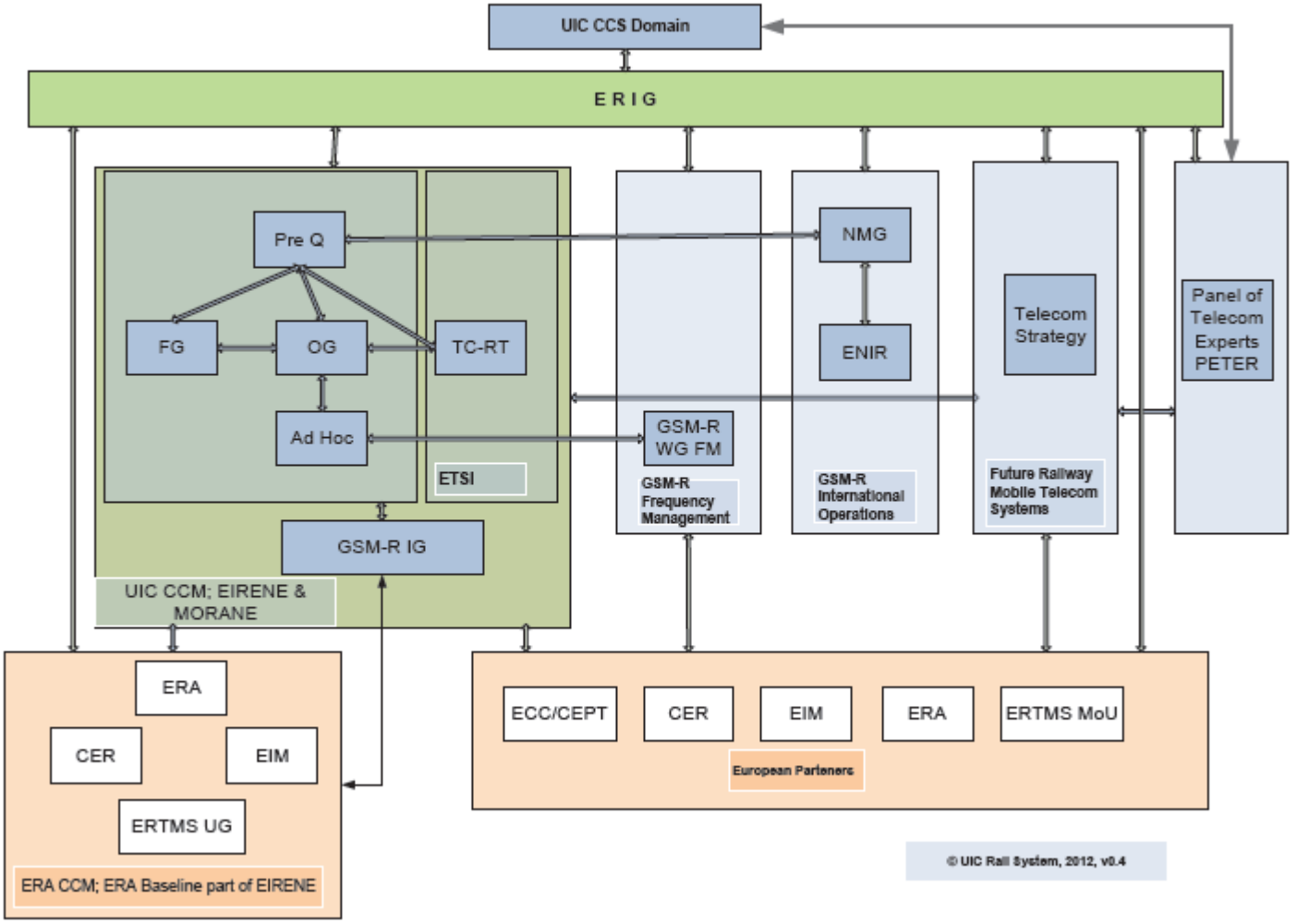
Cyber security concerns – On-board equipment



Source: EIRENE Specifications

- **Supply chain integrity**
- System **upgrade**
- Component **failure**
- **Interactions** with other on-board components

A need for collaboration



Entities and Working Groups involved in the development of ERTMS

A need for cross-border collaboration

- ERTMS is already cross-border
  - Inter-connections of systems
  - Harmonization of procedures

- Harmonization in cyber security
  - Define baseline security requirements
  - Exchange good practices
  - Share incident reports
  - Prepare for the future NIS Directive

Cyber security is not only technical

but also operational and organisational

Summary

- Presentation of ENISA
- Cyber Security for Railway Signalling
- Conclusion

Conclusion

- Railway signalling relies more and more on ICT systems
- Cyber security is a new domain in railway
  - For every sub-system
  - Can rely on concepts from other critical domains
- Collaboration needed for a better harmonization
  - Multi-stakeholders
  - Cross-border

$\Rightarrow$ ENISA aims at facilitating the deployment of cyber security measures through good practices and recommendation

Thank you
Questions?

Dr. Cédric LÉVY-BENCHETON

cedric.levy-bencheton@enisa.europa.eu

Phone: +30 2814 409 630

Mobile: +30 6948 460 133

Follow ENISA: