# Cybersecurity vs Safety in railways: What border ?

**Laurent CEBULSKI**

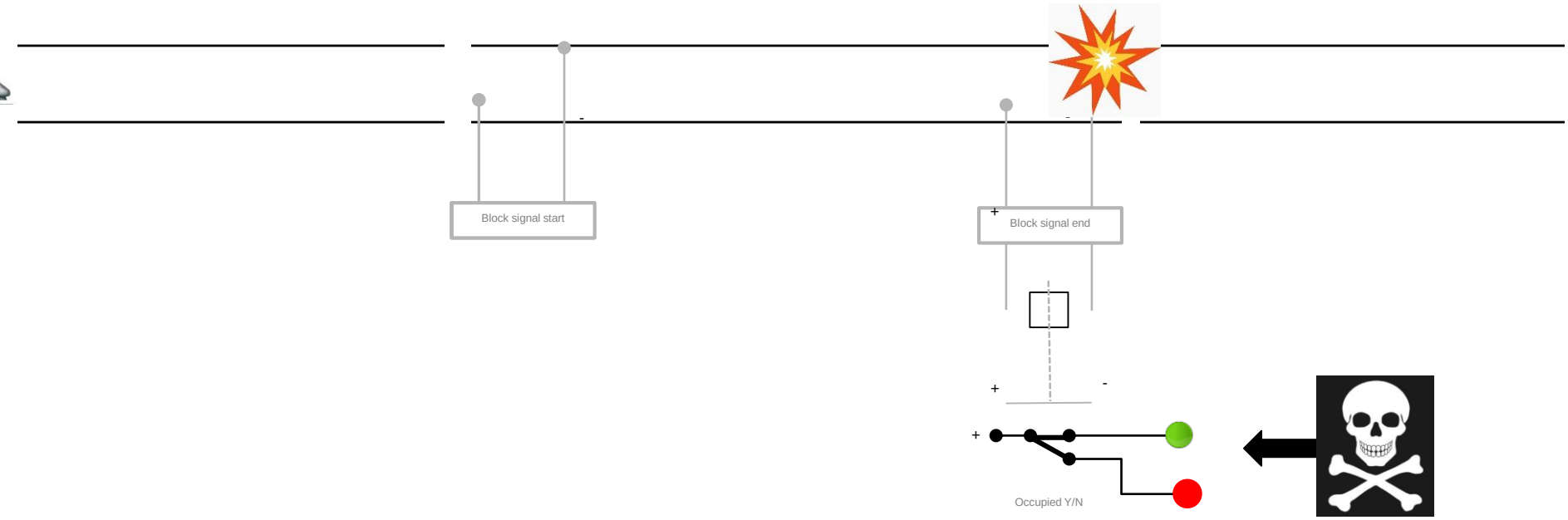
**16 March 2021**

# Speaker introduction

**Laurent CEBULSKI, Managing Director, EPSF, France**

**Doctor in mechanical engineering, Laurent CEBULSKI has been working in the railway sector for nearly 25 years. He was notably an expert, head of research and development, then director of authorizations within the French railway safety authority. He was appointed CEO in September 2020.**

# What are we talking about ?




*Railway safety* or
*railway cybersecurity ?*

# How to define the border ?

We started a think tank in 2018

Objective:

To write a « state of the art » position paper that share the point of vue of authorities and stakeholders.

# Observations

The digitization of the rail sector is increasingly important

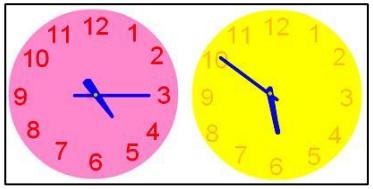
We see cyberattacked sectors every day (hospitals, security agencies,…)

The railway sector is part of an operation dependent on other potentially attackable sectors (energy, telecommunications)

New technologies increase the attack surface (ATO, AI, IoT and other embedded sensors, …)

This is both a technological issue and an organizational issue

Time frame is also an issue : railway safety and cybersecurity don’t have the same time frame



# How to mix both worlds ?

## Railway safety

*Technical objects*: rolling stock, infrastructures, signalling

→ Operational safety

→ TSI Rules

→ Technical standards

*Organisation*: SMS, operation rules, CSM

?

INTEROPERABILITY

## Cybersecurity

NIS *(network and information systems)* directive for *"operators of essential services"*

Military programming law in France

*No specific design rules for cybersecurity*

*Applicable only for certain operators*

# Main common risks

- Maintenance physical accesses, remote operations, subcontracting.


- Wireless public communications vs trains network and information systems

- Impact of OTA updates on railway operation → time for cyberprotection vs time for safety demonstration are NOT the same

- Regulatory disparities between Member States could become a barrier to interoperability → different access conditions depending on the railway infrastructure rules

- Attacking an adjacent sector (communications, energy) could block the rail system by rebound

# Existing actions

- 20 March 2018: cooperation agreement between ANSSI & EPSF

- 2019: ER-ISAC *(European Railway – Information Sharing and Analysis Center)* with FR-BE-NL-DE infrastructure managers

- CEN/CENELEC WG26 to work on a future standard (TS 50701 on Railway applications – Cybersecurity)

- CCTA (*Air transport cybersecurity council*) set-up in France:
  - TC1: “cyber risks”, responsible for updating a hierarchy of risks that may affect the air transport sector;
  - TC2: "impact", responsible for proposing measures to mitigate these risks, taking into account the impact of these measures (safety, economy, etc.);
  - TC3: "regulations", responsible for writing draft national texts and deploying a strategy of influence with international bodies.

# Proposals

- R1: Stepping up cooperation between authorities to move towards a shared and applicable position on the link between rail safety and cybersecurity

- R2: Perform a European benchmark on the link between cybersecurity and rail safety

- R3: Promote information sharing and coordinate actions by the rail industry on cybersecurity

- R4: Integrate the cybersecurity dimension from the start of project

- R5: Implement a reasoned holding in safety condition while minimizing the impact on safety demonstrations

# Other ideas

- To set up a consultancy mechanism between authorities (example of civil security in France)

- To introduce EC certificates with cybersecurity garantees for technical systems

- To bring together railway CSM and cyber risks analysis (EBIOS)

# THANK YOU FOR YOUR ATTENTION