

# TC9X : Electrical and electronic application for railways

## WG 26 Status : Railway Applications – Cybersecurity

# IT Security in Railway ?

- Directive 2016/797 concerning Railway Interoperability
- Directive 2016/1148 concerning measures for a high common level of security of Network and Information Systems across the Union (NIS-Directive)
- NIS is increasingly important to European economy and society.
- NIS is an important precondition to create a reliable environment for Europe wide trade in services.
- Security incidents are becoming bigger, more frequent, and more complex.

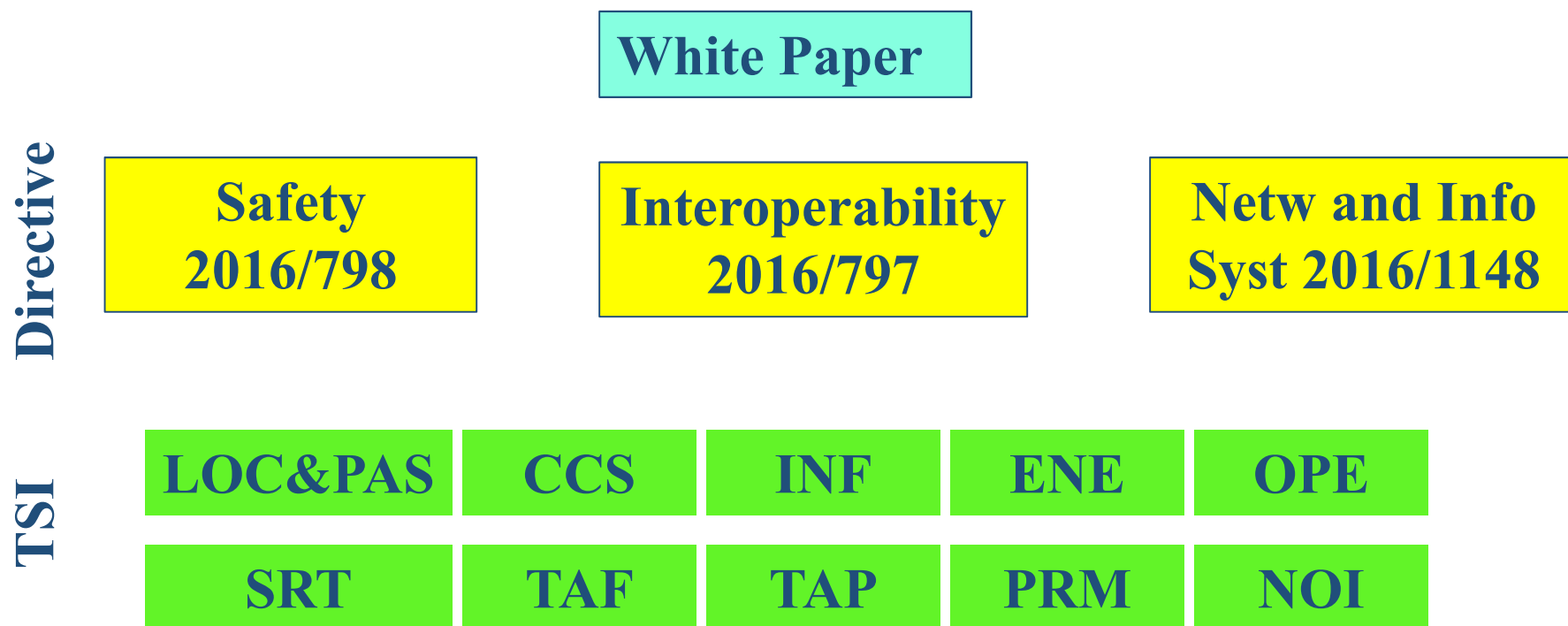


# Challenges

- Train-specific challenges need to be addressed
  - Attackers have fairly easy physical access
  - The train is only one part of an diverse eco-system
  - There are safety-critical and non safety-critical systems on board
- Commercially viable methods for operators, manufacturers and vendors are needed



# Regulation context



# Top 5 Critical Societal/Business functions

- According to ENISA
  - Passengers safety and security
  - Transportation safety and security
  - Data protection and privacy
  - Traffic and vehicle management
  - Sustainable urban mobility

# Coordination at European level with

## Sector Forum Rail (JPC Rail)



Cybersecurity is one of the 4 priority topics of the sector

# Cooperation with standardisation bodies

**Not re-invent the wheel  
but adapt to Rail context**



ETSI TC Cyber



IEC TC 65 : IEC 62443-X-Y  
ACSEC Guide



ISO/IEC JTC1 : ISO/IEC 27000,  
ISO/IEC 15408



**NLST**



Denis Miglianico – TC9X Secretary

## Coordination

- Exchange of information with TD2.11
- Use of IEC Framework
- EUAR : observer
- ENISA : observer





# Cybersecurity in TC9X

- May 2014 : SC9XA Survey group (SGA16)
- Sep 2016 : SC9XA/SGA16 report
- June 2016 : Creation of a TC9 X – SG24.  
investigate and identify the various, varying and intended approaches
- July 2017 : Creation of TC 9X – WG 26 to produce a Technical specification
  - 60 people registered,
  - 30 people participating
  - Regular meetings and conference calls

## On-going work in WG 26

- Creation of 13 sub-groups including terms and definition, lifecycle, cybersecurity risk assessment, security requirements, acceptance process, operational and maintenance requirements
- Analysis of gaps and parts of IEC 62443 which are not applicable. Keep compliant to the parts 4-1 and 4-2 in order to enable the usage of COTS without having to do new certifications
- Analysis of IEC Guide 120 Security aspects – Guidelines for their inclusion in standards
- Security lifecycle under preparation
-

## Next steps

- Security requirements
  - Acceptance process
  - Operational and maintenance requirements
  - ...
- 
- Next Meeting 26-27 of September 2018

Thank you for your attention

[denis.miglianico@alstomgroup.com](mailto:denis.miglianico@alstomgroup.com)