Shift2Rail TD 2.11 Overview

Serge Benoliel, *S2R X2Rail-3 WP 8/9 Leader*, **Alstom Transport**

ENISA-ERA – Online Conference on Cybersecurity for Railways
March, 17th 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No: 826141

Agenda

- **Introduction to Shift2Rail**
  - Programme objectives
  - Project overview
- **Results of X2Rail-1 (2016 – 2018)**
  - Analysis and selection of international standards for cybersecurity in Europe
  - Risk assessments for rail automation systems
- **Results of X2Rail-3 (2019 – 2020)**
  - Generic cybersecurity architecture and definition of shared security services
  - Definition of protection profiles
- **Outlook - S2R Cybersecurity**
- **Q&A**

Shift2Rail: Overview

CAPACITY INCREASE	OPERATION RELIABILITY	REDUCE EMISSIONS	ENERGY EFFICIENCY	LCC REDUCTION	INCREASE PUNCTUALITY

Contributing to the achievement of the Single European Railway Area (SERA)

Founding Members

ALSTOM · BOMBARDIER · CAF · Hitachi Rail STS · NetworkRail · SIEMENS · THALES · TRAFIKVERKET

Associated Members

amadeus · DB · DIGINEXT · Fairwaley · HaCon · indra · KNORR-BREMSE · kontron · mermec · SNCF · Talgo

Virtual Vehicle Austria Consortium (VVAC+)

AVL · FCP · getzner · PJM · virtual vehicle · voestalpine

European Rail Operating community Consortium (EUROC)

bls · ÖBB · ProRail · TCDD · SBB CFF FFS · VÁVLA

Swi'Tracken Consortium

egis · izt · TATA STEEL · TRONICO · RALENIUM · vossloh

Smart DeMain(SDM) Consortium

acciona · cemosa · DLR · Fraunhofer · Strukton

AERFITEC

AERinnova · FIDAMC · tecnalia

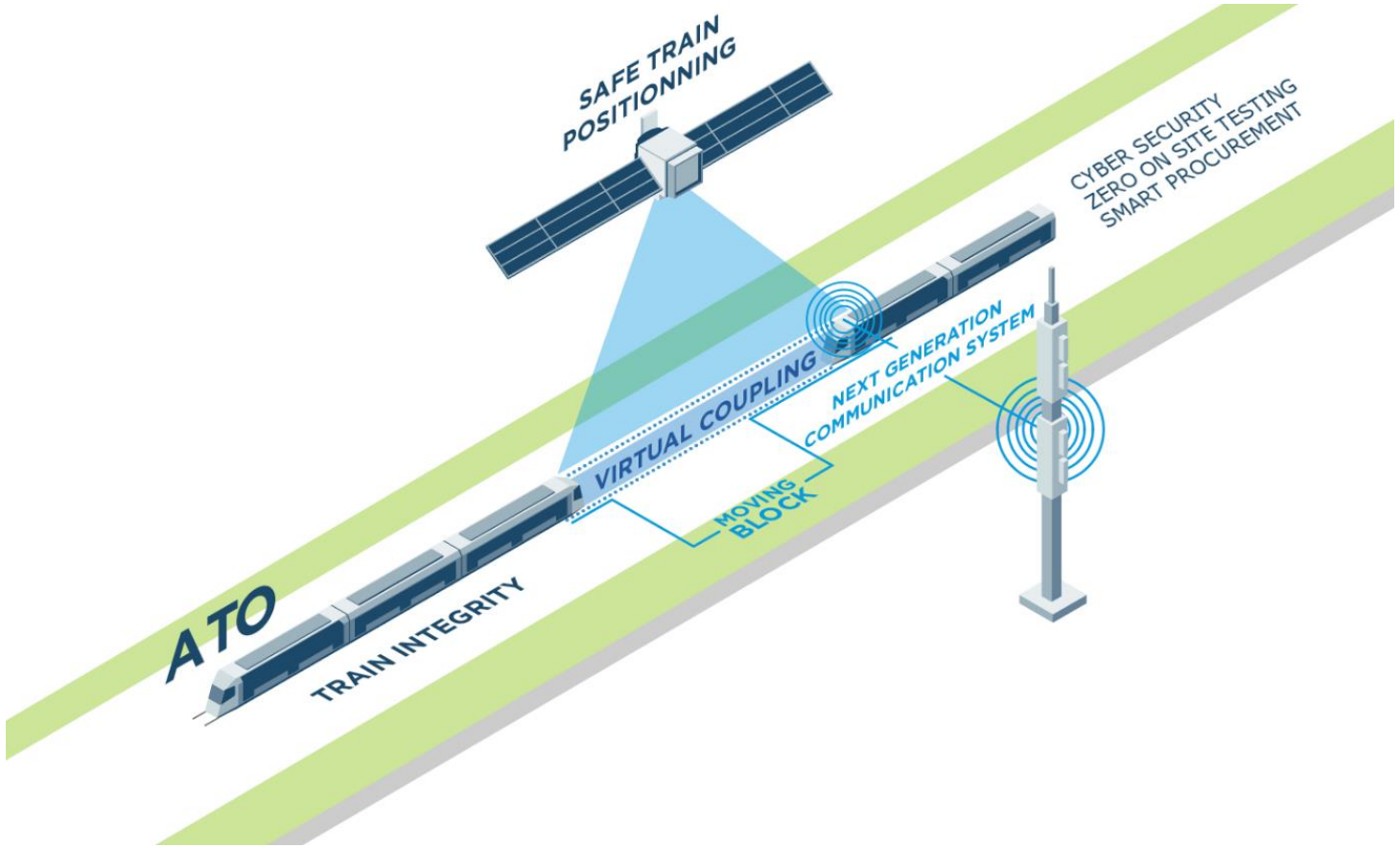
Competitive Freight Wagon Consortium(CFW)

ceit · ConTraffic · DIE BAHNINDUSTRIE. · DLR · WBN

Smart Rail Control (SmartRaCon) consortium

ceit · DLR · NSL · RALENIUM

Shift2Rail: Advanced Traffic Management and Control System Innovation Programme (IP2)



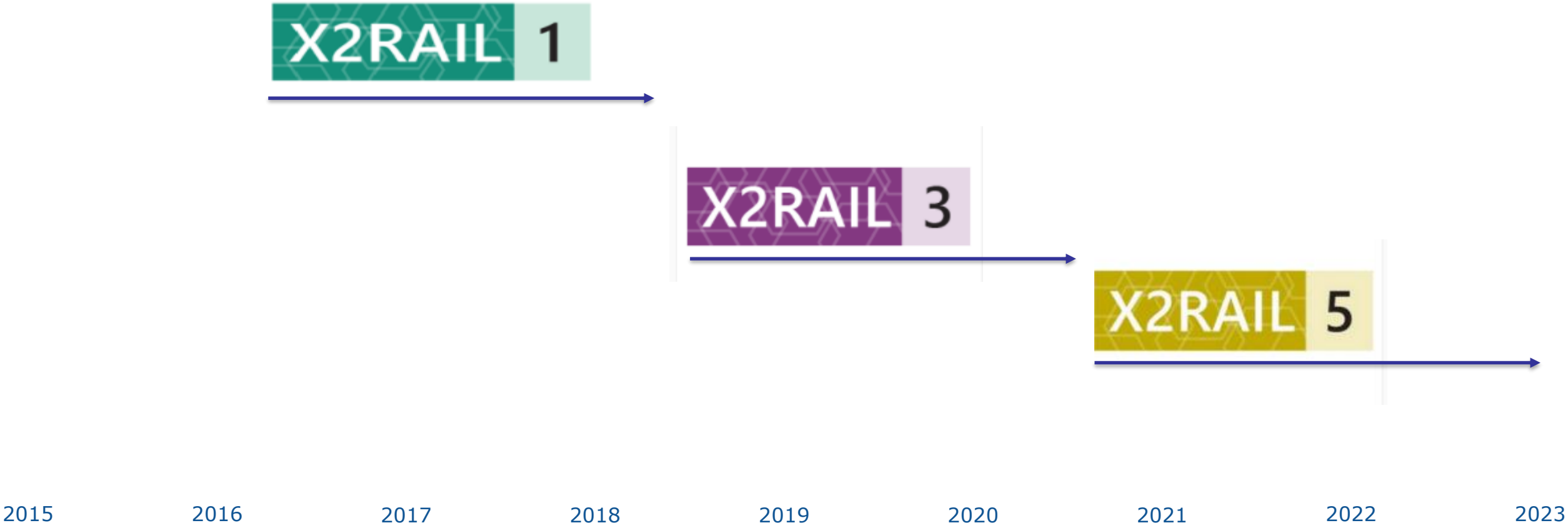
Cybersecurity in S2R

Achieve the optimal level of protection against any significant threat to the signalling and telecom systems in the most economical way

Impact of Cybersecurity to Users of Rail Systems

Passengers	Product / System Suppliers	Integrators / Service Providers	Operators
Availability / Punctuality not impacted	Additional requirements for products and for development processes (IEC 62443-4-1/4-2)	Additional requirements for system integration, commissioning and maintenance (IEC 62443-2-3, 2-4, 3-2, 3-3)	Additional requirements for operation (IEC 62443-2-1 / ISO 27001)

Cybersecurity in S2R - timeline



WP8 & WP 9 Participants

Key stakeholders of EU rail automation:
railway operators, solution providers & research organizations

Result of X2Rail-1 (2015-2018)

Conclusion of D8.1 – Selection of the Security-by-Design standard

„ The **IEC 62443-4-1** – Secure product development requirements and **IEC 62443-4-2** – Technical security requirements for IACS components of the multi-part standard ISA/IEC 62443 is proposed as the **standard framework** for the "Secure-by-design" standard **in the railway domain**"

Conclusion of D8.7 – Application of the risk assessment to the railway signalling system

The Target Security Level (SL-T) evaluation resulted on SL-T vectors with **SL3** on **all** (13) but two **zones**

X2Rail-1 Deliverables D8.1 and D8.7 are available at:
https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1

Results of X2Rail-3 WP 8 Cybersecurity (2019-2020)

1. Definition of a generic cybersecurity architecture and the security environment for next generation rail automation products (shared security services)

2. Investigation and selection of protocols to shared security services for interoperability

3. Define protection profiles for trackside, on-board and ACS components based on selected protocols for shared security services

4. Update of risk assesment method (simplification over X2Rail-1), reports on IoT security, security for legacy systems and securing resilient architectures

Outlook on X2Rail-3 WP 9

X2Rail-3 WP 9 publications (Fall 2021)

- D9.1: Product security verification best practices
- D9.2: Supply-chain security approach for railways
- D9.3: Security evaluation of X2Rail demonstrators (internal)
- D9.4: Railway CSIRT feasibility study in cooperation with 4SecuRail (internal)

Dissemination during 2021 and onwards

- Input of D9.1 towards a rail automation certification scheme (ENISA / CENELEC, EU Cybersecurity Act)

Outlook on X2Rail-5

Project duration X2Rail-5 WP 11 Cybersecurity

- Oct 2021 – May 2023

Planned X2Rail-5 WP 11 Cybersecurity publications

- D11.1: Cybersecurity assessments of other X2Rail demonstrators
- D11.2: Technical demonstrators and report
- D11.3: CSIRT prototype and test use-case
- D11.4: Recommendation on railway systems cyber resilience and response capabilites