



GSM-r Conference

Paris, UIC, 18 May 2017

Marie-Hélène Bonneau, UIC security
division



EU Project 730843



CYRail : Cybersecurity in the RAILway sector

- Duration: 1 Oct. 2016 - 30 Sept. 2018
- Estimated Budget : 1,500 000

- Coordinator :



- Consortium :



CYRail Goal

- Perform a cyber security assessment of the Railway systems;
 - What are the most critical railway services, zones and communications?
- Deliver a taxonomy of threats targeting rail management and control systems
 - What are the threats?
- Assess and select innovative rail management systems attack detection techniques;
 - How to detect attacks targeting rail management systems?
- Specify Countermeasures and Mitigation strategies for improved quality levels;
 - How to prevent , how to make the system resilient
- Achieve Security by Design, by selecting a development framework and specifying Protection Profiles with Evaluation of Assurance Levels.

CYRAIL Structure

WP1 - Project Management

Study & Assess

Detect

Act

Specify

WP2 - Operational Context and Scenarios

WP3 - Security Assessment

WP4

Threat analysis,
attack detection
and early warning

WP5

Mitigation and
Countermeasures
Specification

WP6

Protection Profiles

WP7 - Dissemination and Outreach

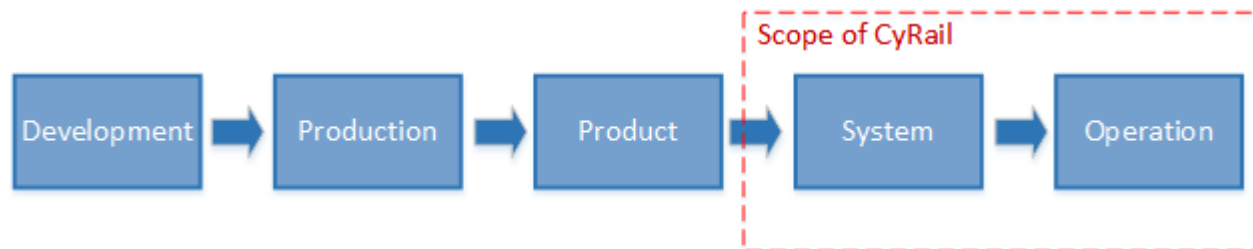
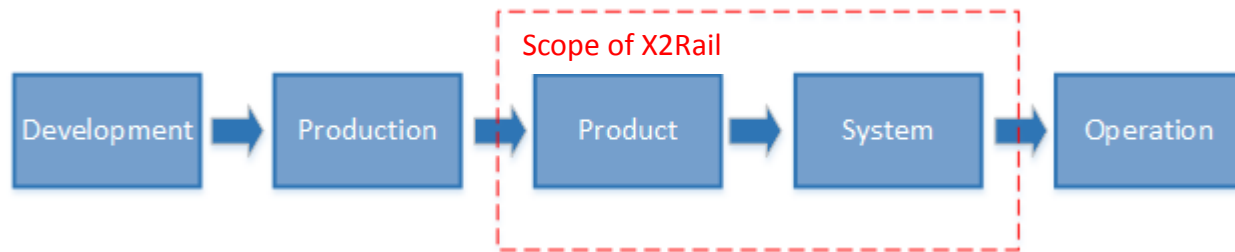
CYRAIL Planning

Workpackage Descriptions	Duration																											
	2016			2017												2018												
	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9				
WP 1 - Project Management	D	D			D						D													D				
T1.1 - Financial management																												
T1.2 - Scientific and Technical Coordination																												
T1.3 - Data protection and gender issues																												
T1.4 - Management of contributions from the Project Advisory Board																												
WP 2 - Operational context and scenario																												
T2.1 – Rail systems within the public transport environment																												
T2.2 – Safety and security of the Railways systems																												
T2.3 – Operational scenario																												
WP 3 - Security assessment																												
T3.1 - Analysis and selection of the security assessment methodology																												
T3.2 - Definition of security zones and vulnerabilities																												
T3.3 - Iterative risk assessment																												
WP 4 - Threat analysis, attack detection and early warning																												
T4.1 – Threat identification and analysis																												
T4.2 – Early attack and anomaly detection																												
T4.3 – Enhanced alerting and collaborative incident management																												
WP 5 - Mitigation and countermeasures specification																												
T5.1 – Identification of Mitigation Strategies																												
T5.2 – Specification of Countermeasures																												
T5.3 – Definition of resilience mechanisms																												
WP 6 - Protection profiles																												
T6.1 – Selection of standards and relevant frameworks																												
T6.2 – Specification of protection profiles and assurance levels																												
T6.3 – Compliance to Protection Profiles																												
WP 7 - Dissemination and Outreach																												
T7.1 – Communication and Dissemination Strategy																												
T7.2 – Involvement of the stakeholders																												
T7.3 – Exploitation and Sustainability Strategy																												

CYRAIL : Cooperation with X2Rail

- X2RAIL-1 : Shif2rail project on "Start-up activities for Advanced Signalling and Automation Systems" from 01/09/2016 to 31/08/2019
- WP8 on Cyber Security led Alstom
 - Definition and demonstration of a Cyber Security System (CSS) dedicated to Railway and Urban systems.
 - The CSS will specify:
 - A standardised way to perform security assessment for railway
 - A solution for a railway secure network
 - monitoring and protection system dedicated to the railway system (threat, prevention and response)

Definition of the scope (Related to CYRAIL WP2)



On-going work : operational scenario

- Definition of the operational scenario based on
 - different communication systems
 - smart rail transport technologies such as automatic train Location, train movement management, train data management, smart ticketing, ..
- Focus on signaling and communication system
- To be defined with the operators

On-going work : Security Assessment Methodology for the railway domain

- Terminology
- Cyber Security Assessment Methodologies
- Selection of the security assessment framework
- Definition of a Security Risk Assessment Methodology For ERTMS

Agreement on the chosen methodology will be found with X2RAIL-1

CYRAIL added value

- Preventing cyber-attacks
- improving the operational security level of the different rail segments
- enhancing the robustness of the railway information, control and signalling sub-systems

Further information

- Website : www.cyrail.eu
- Coordinator of the project : magno.santos@evoleotech.com