www.cyrail.eu

CYRAIL

CYbersecurity in the RAILway sector

Railway infrastructures are moving towards more intelligent, connected, user-centric and collaborative systems. While they bring many advantages for the industry and users, they also pose new opportunities for cyber-criminals and terrorists.

In this context, CYRAIL is a collaborative project funded by the European Commission as part of the call for proposals under the Shift2Rail programme for Rail Research and Innovation (R&I), addressing the topic “Threat detection and profile protection definition for cybersecurity assessment”.

An analysis of threats targeting railway infrastructures will be developed as well as innovative, attack detection and alert techniques. Adapted mitigation plans and countermeasures will be defined, taking into account their potential impact on operations. Protection profiles for railway control and signalling applications will be delivered to ensure security by design of new rail infrastructures.

Starting date: 01.10.2016
Duration: 24 months
EU Project 730843

Horizon 2020
European Union Funding
for Research & Innovation

Shift2Rail

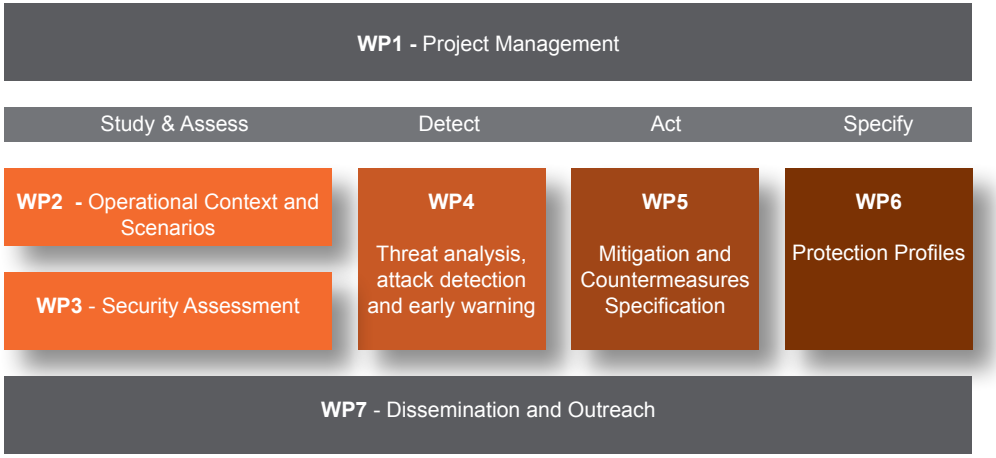
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 730843.

Objectives

The main technical objectives are:

- To perform an exhaustive cyber security assessment of the Railway systems focusing on the most critical railway services, zones and communications
- To deliver a taxonomy of threats targeting rail management and control systems capable of classifying, describing and analysing cyber-attack threats;
- To assess and select innovative rail management systems attack detection techniques;
- To specify countermeasures and mitigation strategies for improved quality levels;
- To describe resilience mechanisms for operational safety;
- To specify protection profiles with evaluation of assurance levels.

Project structure



Description of work

The CYRAIL project is structured around 7 work packages (WPs) with a total duration of 24 months according to the description below:

The project starts with the definition of **Operational Context and Scenario (WP2)** that will deliver the safety and security requirements of an intelligent public transport systems in a multi-stakeholder environment, considering the railway domain. An operational transport scenario involving different types of environment will be proposed for further security assessment in WP3.

Then, **WP3 (Security Assessment)** will carry out an overview of current national and international security risk analysis frameworks, as well as their evaluation in order to identify the most suitable for the railway context. Special mapping and attention will also be paid to the automotive, aeronautic and energy industry to identify synergies.

WP4 (Threat analysis, attack detection and early warning) will deliver a taxonomy of threats targeting rail management and control systems; provide threat classification, description and analysis. A set of innovative techniques to detect attacks targeting rail management systems will be assessed, taking into account the potential combination of cyber and physical threats. Last but not least, a number of innovations supporting early warning, context-enriched alerting and collaborative incident management will be proposed.

WP5 (Mitigation and Countermeasures Specification) will provide the specifications for countermeasures, identify the different mitigation strategies and resilience mechanisms that allow the operation to continue with guaranteed quality levels, without having an impact on operational safety.

Lastly, **WP6 (Protection Profiles Specification**) will integrate the essential concepts considered in WPs 4 and 5 into profiles which capture the scenario and security requirements of WPs 2 and 3, respectively. The protection profiles specification shall include: security by design; specification of protection profiles; selection of standard framework; and evaluation assurance level.

The project includes a set of cross-cutting activities that will run throughout the project: project management and dissemination and outreach activities (**WP1 - Project Management** and **WP7 - Dissemination and Outreach)**

Added Value

CYRAIL aims to have a significant impact on enhancing the operational security level of the different rail segments and the robustness of the railway information, control and signalling sub-systems.

With the challenge of boosting innovative and cost-efficient technologies and system for railway signalling, traffic control and automation with an ever increasing reliance on communications technologies, CYRAIL will contribute to the prevention of cyber-attacks, improving the operational security level of the different rail segments.

www.cyrail.eu

Consortium

EVOLEO Technologies LDA , Portugal

Jakintza Lanezko Ikerkuntza Investigación Universidad Empresa, EUSKOIKER, Spain

Fortiss GmbH, Germany

International Union of Railways, UIC, France

AIRBUS Defence & Space, France

ATSEC Information Security AB, Sweden

Contact us

info@cyrail.eu
www.cyrail.eu