CYRail Report Summary

Project ID: 730843
Funded under: H2020-EU.3.4.8.2.

Periodic Reporting for period 1 - CYRail (Cybersecurity in the RAILway sector)

Reporting period: 2016-10-01 to 2017-09-30

Summary of the context and overall objectives of the project

Railway infrastructures are moving towards more intelligent, connected, user-centric and collaborative systems. While it brings many advantages for the industry and users, it also poses new opportunities for cyber-criminals and terrorists. CYRail aims to deliver tailored specifications and recommendations for secure modern rail systems design and operation.

The challenges are multiple: wide and distributed geographical display of rail systems limit the traditional cyber-protection and cyber-defence tools & practices; the heterogeneous nature of rail systems make them vulnerable to blended attacks; the collaboration with other transportation infrastructures increase the number of points for attack; new passenger-centric services may expose rail systems to threats known in the IoT; last but not least, ICT supporting these trends are not necessarily trusted for critical applications.

The CYRail consortium takes advantage of developments in other industries (aeronautics, automotive and energy) and bring them into the railway sector, taking similarities and specificities into account. To address these challenges, operational context and scenarios will be defined, followed by a security assessments of railway systems. An analysis of threats targeting those infrastructures will be developed as well as innovative, attack detection and alerting techniques. Adapted mitigation plans and countermeasures will be defined, taking into account their potential impact on operations. Protection Profiles for railway communications will be delivered to ensure security by design of new rail control and signalling applications.

Work performed from the beginning of the project to the end of the period covered by the report and main results achieved so far

CYRail has reached the middle of the project, and although some minor deviations have happened, CYRail Project and Consortiums members had successfully accomplished the main goals for the period reaching the planned milestones and associated deliverables for the working period.

For this first period of 12 months all work packages were started but WP6, and WP1, WP2, WP3 and WP7 produced deliverables foreseen for the period. CYRail project, after a productive end-users workshop were several Advisory Board members were present, was able to define a comprehensive operational scenario with different use cases. With the definition of a formal methodology for security assessment, CYRail performed a first cyber security assessment, within a set of assets identified on the Operational Scenario, producing a list of vulnerabilities. This are now going to be used on the next tasks to be performed. We can safely say, that the project is moving forward as foreseen.

Progress beyond the state of the art and expected potential impact (including the socio-economic impact and the wider societal implications of the project so far)
Security requirements, such as Protection Profile are usually specified based on general, expected security needs by the developers and government agencies that may usually result in generic requirements for a component only with limited security context.

In our case we will also develop a Protection Profile, but this is done on a well-founded understanding of the security needs of the users (operators), derived from a risk assessment, taking into account the specific use cases and scenarios. This means that we will be able to better address the actual needs.

Second we will develop this Protection Profile in a context of system accreditation, ISA-62443. This means that aspects such as integration and maintenance, which are essential for secure operation over time, will be addressed by the project.

Third, we will also take the aspects of secure design into consideration. Although this is the basis for security, it is something that is often neglected when specifying security requirements, independent if these are ISO/IEC 15408 or any other standard. Finally, we believe that the project could provide valuable input into the European security initiative [COM-2017-477] by increasing the overall transparency of cyber security assurance and avoiding fragmentation of in the EU and related security requirements and evaluation criteria by relying on and integrating existing security standards for an important industry.

Related information

[logo-cyrail.png]

**Last updated** on 2018-03-28
**Retrieved on** 2019-05-24

**Permalink:** https://cordis.europa.eu/result/rcn/223899_en.html

© European Union, 2019