Cybersecurity Risk Assessment of Virtually Coupled Train Sets

Aria Mirzai, Ramana Reddy Avula, Marvin Damschen
Dependable Transport Systems, RISE Research Institutes of Sweden

This work presents a cybersecurity risk assessment of the Virtually Coupled Train Set (VCTS) design developed within the Europe's Rail project R2DATO. Methodologies developed under the Shift2Rail initiative, particularly the X2Rail-5 project are leveraged to identify potential vulnerabilities and assess the impact of potential threats.

By applying a risk assessment tool **based on IEC 62443-3-2 and CLC/TS 50701** towards regulatory compliance measures, this work seeks to fortify the cybersecurity of railway systems, ensuring safer and more reliable operations in an increasingly digital and interconnected world.

System Description

The nine VCTS missions defined in X2Rail-3 have been identified as the system's essential functions and therefore used as primary assets in this assessment.

Following the evaluation of risk levels, cybersecurity requirements from IEC 62443-3-3 (system level) and IEC 62443-4-2 (component level) should be allocated to the security zones (onboard & trackside) of the system.

Cybersecurity Risk Assessment

The **publicly available Excel-based risk assessment tool of X2Rail-5** offers practical guidance for enhancing cybersecurity in railway systems.

As first step, an "Initial Risk Assessment" is performed for each primary asset. This entails evaluation of the impact of each feared event on four different business stakes. An excerpt of our results for the primary asset "Virtual Coupling Set Up" is provided in the table above. **The evaluation for each primary asset was performed twice by independent pairs, consisting of experts from RISE, DLR, Renfe, Indra and CEIT**.

Next follows a more detailed, so-called "Unmitigated Risk Analysis". While the Initial Risk Assessment focuses on impact, the Unmitigated Risk Analysis proceeds by evaluating the likelihood of threats materialising. Several factors are considered, including threat type, attacker capability, intent, and targeting. The likelihood assessment is further refined using the Common Vulnerability Scoring System (CVSS) exploitability metrics.

The assessment's results are presented in the table below, where **risk levels have been mapped to the seven foundational requirements of IEC 62443 as well as to their corresponding target security level (SL-T):**

	IAC	UC	SI	DC	RDF	TRE	RA	SL-T Vector
OB-Z	2	2	2	2	2	2	1	{2, 2, 2, 2, 2, 2, 1}
TS-Z	2	2	2	2	2	2	1	{2, 2, 2, 2, 2, 2, 1}

Feared Event	Primary Asset	Safety	Performance	Reputation	Compliance	Total Damage Potential	Overall Impact
Loss of Confidentiality	Virtual Coupling Set Up	1	1	2	3	112	2
Loss of Integrity	Virtual Coupling Set Up	3	4	3	3	1300	4
Loss of Availability	Virtual Coupling Set Up	4	3	2	3	1210	4

Conclusions & Future Directions:

Key findings highlight the importance of continuous improvement of risk assessment methodologies.

Future enhancements could include:

- More **detailed guidelines and examples for generating system-specific vulnerability vectors**, possibly leveraging attack trees and MITRE attack techniques.
- **Broader asset types**, including information assets and processes.
- Aligning with **ENISA's Transport Threat Landscape for the European Union** would increase legitimacy.

More information:

Aria Mirzai, MSc | aria.mirzai@ri.se

https://www.ri.se/en/what-we-do/projects/europes-rail-r2dato

Funding Disclaimer

This work is funded by the European Union (grant agreement n° 101102001) and Trafikverket (TRV 2022/46318). It is supported by the Europe's Rail Joint Undertaking and its members. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Europe's Rail Joint Undertaking. Neither the European Union nor the granting authority can be held responsible for them.