IT security risk analysis and threat mitigation for railway applications

Patric Birr, Martin Hetzer, Simon Petretti

IT security risk analysis and threat mitigation for railway applications

Patric Birr, Martin Hetzer, Dr. Simon Petretti
ICS AG
Berlin, Germany
{Patric.Birr, Martin.Hetzer, Simon.Petretti}@ics-ag.de

***Abstract*— In this article, we present a best practise approach for the evaluation and assessment of IT security demands for railway applications. State-of-the-art standards and guidelines are used to identify and evaluate threats concerning the IT security of a given railway system and corresponding requirements are derived. Taking threat mitigation measures into account, the system under consideration is revised based on its technology and system architecture. Using combined "Top-Down" and "Bottom-Up" analysis techniques, the most relevant attack patterns and penetration paths are identified for each system component or function. The result of such an analysis may require iterative revisions and eventually extends IT security requirements as compared to the derivation from standards.**

Keywords— IT security, vulnerability, risk analysis, threat mitigation

I. Introduction

Technological advances and ongoing digitalization in the last decades have led to new challenges for IT security of industrial automation systems. Due to the increased use of commercially available systems and the need to interconnect applications, the railway industry is also part of this development. New threat scenarios can have significant effects on system availability and data integrity, which are essential to operators in the railway sector due to high demands on reliability and safety. Changes in the European and National legal framework reflect the new challenges by means of new responsibilities, e.g.:

- obligations to a comprehensive proof of state-of-the-art requirements on process and technology,
- obligations to report significant IT security incidents for operators of critical infrastructure.

In the past, the main focus was on the proof of safe operation in the sense of technical safety, which is based on rigid functional requirements. Nowadays, the focus is clearly extended. A new challenge arises due to the necessary incorporation of IT security requirements into partly safety-critical railway systems integrated in a dynamic and changeable IT infrastructure.

II. State of Standardization

The German draft standard DIN VDE V 0831-104 [4] serves as a guideline for the application of IT security measures to railway systems in accordance with IEC 62443 [1]. DIN VDE V 0831-104 provides proof of considerable overlap of rules and regulations between railway and industrial automation systems described in IEC 62443. The integration of IEC 62443 into the established approaches for safety-related railway systems (according to EN 50129 [5] or EU Regulation 402/2013 [6]) serves as a basis for the approach described in this article. DIN VDE V 0831-104 references the well-established Risk Management Guide NIST SP 800-30 [7] for a simplified railway specific IT security risk analysis process. We apply and expand this railway specific analysis. The subsequent detailed risk analysis is based on specific threats, vulnerabilities and the corresponding impacts on system security goals as required by IEC 62443.

III. Railway Specific Approach

DIN VDE 0831-104 provides guidance towards conducting a railway specific IT security risk analysis in four steps:

1) Separation of the system into zones and conduits
2) Threat analysis
3) Explicit risk analysis
4) Assignment of IT security requirements

Separation of the system into zones is to be done based on functionality, safety relevance and modes of communication of the devices as well as corresponding users and their roles. Conduits represent connections between zones. Threat analysis is done based on the seven foundational IT security requirements (FRs) defined in IEC 62443-3-3 [3]. Threats and their consequences are evaluated for every zone and conduit individually.

The simplified approach to conducting an explicit risk analysis derives Security Level Targets (SL-Ts) from skills, motivation and resources of the realistic type of attacker for every zone and conduit. Taking pre-defined railway specific risk factors into account, the explicit risk analysis yields SL-T vectors as a result. Each element of such a vector represents the SL-T for one of the seven FRs. The SL-T vectors are then used to assign a set of IT security requirements to every zone and every conduit based on the catalogue provided in IEC 62443-3-3.

IV. Detailed Risk Analysis

According to IEC 62443-2-1 [2], IT security risk assessments shall include identification and prioritization of risks based

upon vulnerabilities as well as threats and consequences to system assets. The railway specific approach described in DIN VDE 0831-104 [4] derives SL-Ts from threat source characteristics, thereby neglecting vulnerabilities of the system architecture as well as the actual threat events. The simplified approach is therefore extended by a detailed analysis based on the architecture and technology used.

The risk assessment process as described in NIST SP 800-30 [7] is used to create a model of real attack patterns based on reliable data which is prioritized by the risk posed to system availability as well as data integrity and confidentiality. The data required to create such a model are provided by two governmentally founded and sponsored databases: CAPEC [8] and CWE [9]. As proposed in IEC TR 20004 [11], these two databases are used to identify relevant attack patterns (CAPEC) and software weaknesses (CWE) in the scope of vulnerability analyses under the Common Criteria IEC 15408 [10]. This prioritized model of real attack patterns, including their exploitable weaknesses as well as technical context and consequences, serves as a basis for the final detailed technical evaluation by means of Top-Down and Bottom-Up analyses.

V. Top-Down & Bottom-Up Combination

The combination of Bottom-Up and Top-Down analyses allows for the identification of critical attack patterns and penetration paths for every system component and function in the system. The Bottom-Up Security FMEA uses the prioritized model of attack patterns to evaluate the criticality of each attack for all devices based on technology, attack execution flow and attack prerequisites, e.g. software weaknesses. Taking planned or existing threat mitigation measures into account, a risk priority number (RPN) can be assigned to every attack pattern to identify threats which cannot yet be considered to be properly mitigated. These critical attack patterns are then used as input for the Top-Down approach called Attack Tree Analysis (ATA). During an ATA, all possible penetration paths leading to a loss of assets need to be considered. Assumptions about safe operation can be used to eliminate certain paths, e.g. the ones that would require assistance from trustworthy employees. Other paths can be evaluated quantitatively to identify the need of additional security measures to mitigate specific threats.

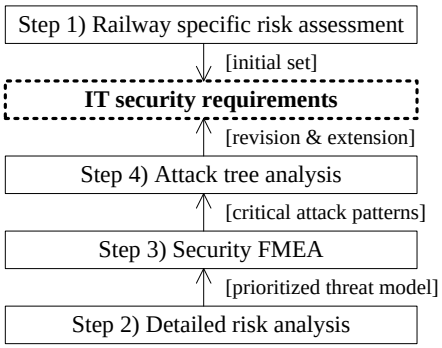

Figure 1: Proposed steps and linked artefacts

VI. Requirements Revision & Extension

Identified unmitigated threats above a determined criticality require additional security measures in the existing system architecture. The implementation of such additions needs to be triggered by documentation of additional requirements, extending the catalogue taken from IEC 62443-3-3 [3]. Each CAPEC [8] entry contains a detailed list of recommended measures to mitigate the specific attack pattern. Additionally, national institutions may provide catalogues of requirements and corresponding security measures, which should be taken into consideration as well. The recommended security measures provided by CAPEC can be used to extend the set of requirements from IEC 62443-3-3, thereby providing the system with additional protection against specific threats.

The proposed approach and linked artefacts between the different steps are visualized in Figure 1. The presented process is highly generic and adaptable to other industrial sectors, provided that domain specific assumptions and regulatory frameworks are adjusted

References

[1] IEC 62443, “Industrial communication networks – Network and system security”, Series of 13 Standards on Industrial Automation and Control System Security

[2] IEC 62443-2-1, “Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program”, November 2010

[3] IEC 62443-3-3, “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels”, August 2013

[4] DIN VDE 0831-104, “Electric signalling systems for railways – Part 104: IT Security Guideline based on IEC 62443”, May 2015

[5] EN 50129, “Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling”, February 2003

[6] EU 402/2013, “EU Regulation 402/2013 on the Common Safety Methods (CSM) for risk assessment and repealing Regulation 352/2009”, in effect since May 2015

[7] NIST SP 800-30 Revision 1, “Information Security – Guide for Conducting Risk Assessments”, September 2012

[8] Common Attack Pattern Enumeration and Classification, http://capec.mitre.org

[9] Common Weakness Enumeration, http://cwe.mitre.org

[10] IEC 15408, “Common Criteria for Information Technology Security Evaluation”, Version 3.1, Revision 4, September 2012

[11] IEC TR 20004, “Technical Report: Information technology – Security techniques – Refining software vulnerability analysis under IEC 15408 and IEC 18045”, August 2012