Threat Modeling in the Railway Domain

Christoph Schmittner[1], Peter Tummeltshammer[2], David Hofbauer[3], Abdelkader Magdy Shaaban[1], Michael Meidlinger[2], Markus Tauber[3], Arndt Bonitz[1], Reinhard Hametner[2], and Manuela Brandstetter[3]

[1] AIT Austrian Institute of Technology GmbH, Giefinggasse 4, A-1210 Vienna, Austria
[2] Thales Austria GmbH, Handelskai 92, A-1200 Vienna, Austria
[3] Fachhochschule Burgenland GmbH, Campus 1, A-7000 Eisenstadt, Austria

Abstract. Connected and intelligent railway technologies like the European Rail Traffic Management System (ERTMS) introduce new risks in cybersecurity. Threat modeling is a building block in security engineering that identifies potential threats in order to define corresponding mitigation. In this paper, we show how to conduct threat modeling for railway security analysis during a development life cycle based on IEC 62443. We propose a practical and efficient approach to threat modeling, extending existing tool support and demonstrating its applicability and feasibility.

Keywords: Railway · Cybersecurity · Threat Modeling · IEC 62443 · Cybersecurity Analysis.

1 Introduction

The railway system is changing towards an Internet of Things (IoT)-based system with an increased usage of Components of the Shelf (COTS) [19] and wireless communication technologies [10]. With the transition to information and communication systems, the cyber-attack surface has increased tremendously. Evaluations showed vulnerabilities and weaknesses in European Rail Traffic Management System (ERTMS) [3, 15] and a rail-based honeypot setup showed an active threat landscape [14].

In order to address cybersecurity concerns, different existing standards have been examined [4] and the IEC 62443 series [12] was selected. A pre-norm from the German standardization committee DKE [7] provides guidance on how to apply IEC 62443 in the railway domain. IEC 62443-3-2 [2] does not prescribe or propose a methodology for the identification of cybersecurity risk.

In this paper, we present a novel Thread Modeling approach for identifying threats in the safety critical railway domain. To the best of the authors' knowledge, no previous works exist that treats thread modeling in the railway domain in a systematic and concise manner. The remainder of this paper is structured as follows. Section 2 gives an overview about the Railway Domain, existing approaches towards security and Threat Modeling. Section 3 describes our approach of Threat Modeling and a proof-of-concept. Finally, Section 4 concludes the paper.

2 State of the Art

This section presents the State of the Art of the railway systems based on ERTMS and summarizes the current framework regarding safety. The focus was on the already existing coverage of security. Section 2.3 presents the IEC 62443 series as a security framework for the railway domain. The section is concluded by presenting existing approaches towards railway security assessment and the existing work for threat modeling.

2.1 Overview over the railway system

ERTMS is a European Union initiative to create a common standard for train signaling, control, communication and management. The goal is to increase efficiency, especially for cross-border traffic [21].

The two main components of ERTMS are ETCS (European Train Control System) and GSM-R (Global System for Mobile Communications Railway) or LTE-R (Long Term Evolution Railway). ETCS is intended for safety-critical signaling and control systems. In ETCS Level 3, trains find their positions themselves with the help of onboard sensors (tachometer, radar) and absolute position reference (APR) beacons located on the track. The trains continuously transmit their signals (position and speed) to theRadio Block Center (RBC) which is further connected to a Control Centre. Based on the high-resolution information which is received from all trains in the zone, the limit of movement authority[4] and speed is determined and fed back to the vehicle via the GSM-R or LTE-R radio link, alongside some additional route information.

Automatic Train Supervision (ATS) is responsible for monitoring and controlling the rail systems to ensure real-time optimization of railway operations and to ensure the schedules are met. The onboard systems of the train Automatic Train Protection (ATP) and Automatic Train Operation (ATO) uses control logic software with the received information to issue appropriate commands to trains — typically through some Driver Machine Interface (DMI).

2.2 Safety Framework

In the railway domain, safety engineering is guided mainly by the following standards.

EN 50126: *The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).* This document defines security as the resilience of a system to "vandalism and unreasonable human action", but the aspect of protection against cyber threats is outside the scope of this standard. However, "security hazards" are listed in system hazard analysis [8].

EN 50128: *Software for railway control and protection systems.* This standard does not consider security because it is out of the scope of this standard [6].

[4] i.e. the section on the tracks which is pre-approved for the train

EN 50129: *Safety related electronic systems for signalling.* This standard addresses "protection against unauthorized access" [9].

EN 50159: *Safety-related communication in transmission systems* This standard is aimed at the safety-related usage of transmission systems which might be endangered by security threats. The focus is on ensuring the integrity of the communication, availability and confidentiality is excluded [5].

2.3 Security Framework

Based on an evaluation of different security standards [4], the IEC 62443 series was identified as a suitable security framework for the railway domain. The IEC 62443 series "Security for industrial automation and control systems" is divided into four groups. Note that not all parts of the standard have been released yet, and the development is still ongoing. Table 1 gives an overview of the parts and structure of IEC 62443 [12]

Table 1: Overview of the IEC 62443 series structure and parts

General	IEC 62443-1-1 Terminology, concepts and models	IEC TR 62443-1-2 Master glossary of terms and abbreviations	IEC 62443-1-3 System security conformance metrics	IEC TR 62443-1-4 IACS security lifecycle and use-cases
Policies & Procedures	IEC 62443-2-1 Establishing an IACS[5] security program	IEC TR 62443-2-2 Implementation guidance for an IACS security management system	IEC TR 62443-2-3 Patch management in the IACS environment	IEC 62443-2-4 Security program requirements for IACS service providers
System	IEC TR 62443-3-1 Security technologies for IACS	IEC 62443-3-2 Security risk assessment and system design	IEC 62443-3-3 System security requirements and security levels	
Component	IEC 62443-4-1 Product development requirements	IEC 62443-4-2 Technical security requirements for IACS components		

The standard defines the following roles "Asset Operator", "System Integrator" and "Product Supplier". Depending on the role, different parts of the standard apply.:

IEC 62443-1-x: *General* describes overarching concepts, terms and metrics for secure IACS systems.

IEC 62443-2-x: *Policies & Procedures* present the management framework for implementation, patching and operation.

IEC 62443-3-x: *System* is aimed at "Asset Operator" and "System Integrator" and describes necessary activities and processes during the system engineering.

IEC 62443-4-*x*: *Component* is for "Product supplier" and describes how to develop secure components for the integration in IACS.

The Asset Owner uses Part 3-2 to determine the security needs of the system while considering safety and business criticality. Based on the security needs and logical and functional distribution a security architecture is developed which divides the system into zones and conduits. A zone collects systems with a similar criticality level or security needs and has a Security Level Target (SL-T) assigned.

The System Integrator can use Part 3-3 to design a system which achieves Security Level Achieved (SL-A). For this, components and systems with a suitable Security Level Capability (SL-C) have to be chosen.

The Product Supplier can use Part 4-1 and 4-2 to develop secure components with SL-C. Part 4-1 describes security development life cycle and the required capabilities for the process. Part 4-2 describe technical security requirements fore components.

To summarize, IEC 62443 uses the following Security Level (SL).

SL-T: Desired level of security, usually based on a risk assessment.
SL-C: Level of security achievable if a system or component is properly configured and installed.
SL-A: Achieved level of security, based on an assessment of system design or deployment.

2.4 Existing Railway Risk Analysis Approaches

For both, the detailed and the high-level risk assessment, it is suggested to use the same risk assessment methodology [2]. In [23], fault trees are used to analyze safety and security in a Communication Based Train Control (CBTC) system of urban railways. Security events are added as additional nodes in the fault tree. There are however some drawbacks to that approach. First of all, this approach requires all relevant security events to be identified beforehand. The thread modeling approach presented in this paper provides a systematic methodology to do so and can be used to resolve this issue. Additionally, once the events have been identified, they need to be weighted by the probability of their occurrence, which is difficult to assess.

More specifically, [22] extends hazard and operability studies (HAZOP) to also take into account security threats in a Train Leader Telephone System. The HAZOP guide-word driven system is used to formulate a set of generic expressions which are then used to examine the system for potential threats. This is similar –but less formal– than the approach of using an explicit "threat model" with corresponding knowledge base of threats and vulnerabilities.

Another line of work [3] puts more focus on developing approaches towards risk assessment, e.g. how to rate and classify identified threats.

2.5 Threat Modeling

Our approach proposed in Section 3 is based on threat modeling. Threat modeling is a technique for the identification of security risks and has been promoted

as part of the Microsoft Secured Development Lifecycle (MS-SDL) [11]. It defines an abstract model of potential threats, which is applied to the system model in order to identify representations of the threats.

In general, threat modeling can be divided into the following steps:

1. Model the system with all security related assumptions and necessary information.
2. Model potential adversaries with capabilities, actions, tactics, techniques, and procedures.
3. Apply the threat model to the system model to identify potential threats
4. Evaluate all identified threats and decide on the risk treatment
5. Update the system model with the security countermeasures
6. Repeat step 3 in order to identify missed or new threats

Generally, systems are modeled in a Data-flow Diagram (DFD). There are five basic diagram elements in a DFD:

Processes are elements that, based on their input, perform actions and/or generate outputs.

Data stores are sinks or sources of data. Examples are databases or internal storage.

Data flows represent the flow of information between elements. A data flow can be a protocol specific communication link such as HTTPS or UDP.

External interactors are elements whose influence should be taken into account, but which are outside the scope of the analysis.

Trust boundaries divide the elements in the diagram into different trust zones, e.g. elements in open networks vs elements in internal networks

A model can have different levels of granularity. Depending on the available system details and threat identification needs, a high-level process can be further decomposed into multiple lower-level components in a hierarchical way. One can use Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege (STRIDE) to define a generic threat model (see Table 2). As an example, a Data Flow can be tampered with, the transmitted information can be disclosed or a denial of service can impact the Data Flow. Since a data flow is not an entity, it cannot be spoofed.

Depending on the level of granularity and available information, threat models can contain more specific descriptions of threats. For example, if the Data Flow is wireless one can define subcategories for Denial of Service like Jamming.

Research regarding threat modeling in the mobility domain has been carried out in [20]. There, components are modeled for a scenario of connected cars, which are then used to derive a threat and vulnerability catalogue.

With regards to the automotive domain, thread models have been employed successfully in [16, 13]. Consequently, we propose to use this approach also for modeling components, threats and vulnerabilities in the railway domain, e.g. for autonomous trains. One benefit of using threat modeling is the availability of tools which support the method [18]. Microsoft developed a Threat Modeling

Table 2: STRIDE Threat Model

	Spoofing	Tampering	Repudiation	Inf. Disclosure	DoS	Elev. of priv.
Data Flows		×		×	×	
Data Store		×		×	×	
Processes	×	×	×	×	×	×
Interactors	×		×			

Tool (TMT) which is available as a free plugin for Microsoft Visio [17]. With the 2016 release of the tool, it is possible to create new templates derived from system modeling elements and the threat knowledge database. This allows for the TMT to be applied to new domains such as rail, as we will present in the upcoming Section 3.

3 Railway Threat Modeling

In order to conduct a cybersecurity risk assessment according to IEC 62243, we need a systematic approach to identify threats to a system. As Section 2.4 has shown, the current approaches are either based on already identified threats or rely on expert judgment and brainstorming for the identification of threats. We developed a railway specific template, which allows the modeling of railway systems and a railway threat model and integrate the Railway threat modeling process with the IEC 62443 workflow.

3.1 Railway Template

The template is the central storage of modeling elements, threats, and corresponding mitigation. It should be periodically updated with external information regarding vulnerabilities and mitigation and experiences from applying threat modeling.

When creating a new template, the most important parts are stencils for drawing DFDs and threat types that define threat and mitigation catalogues. We created stencils for railway components such as RBC or GSM-R. For each stencil, different properties and values are be defined. Once defined, they can be used during the threat modeling to define already known security relevant information.

The threat model in the template consists of threats, classified in different threat types. Each threat is described by title, threat description, potential mitigation and include and exclude statement. The statements describe with logical expressions when a threat is generated for an element in a system model.

Threat modeling can be performed in further phases of the lifecycle as monitoring activity to identify if new threats are relevant for a certain system. This requires updating the model to mirror the real system and re-analyzing it with an updated threat database.

As an example, based on [15], we add the property Cipher Algorithm to the GSM-R stencil (see Figure 1) and extend the rule set accordingly. Based on this

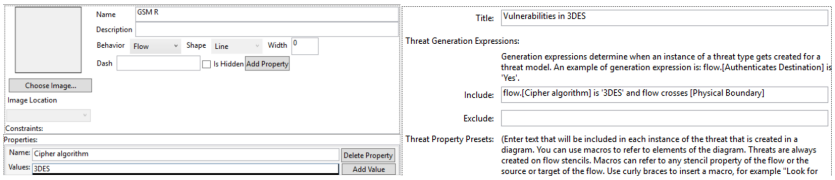

Figure 1: Extensions of stencil properties and rules

in further evaluation of existing models we will receive a warning that there are potential problems with 3DES. If there are more concerns or real world attacks we can increase the suggested impact and justification. Doing this allows us to document new concerns in existing systems and monitor for new risks.

3.2 Proposed Process

Figure 2 shows our proposal how threat modeling can be used in the the IEC 62443 workflow.

The specification of the system under consideration and the security related properties is done by defining a data flow diagram of the system. The elements in the data flow diagram need to be able to represent already implemented security measures. Based on this data flow diagram, threats for the high level cybersecurity risk assessment are identified. This is done by applying the railway threat data base on the model and checking which elements of the model are susceptible to a certain threat.

Figure 3 shows the model we created for a rail use case using the Microsoft TMT. Only a subset of railway-specific modeling elements are selected from he more general railway template repository we developed. Applying the railway threat data base to this initial system model results in 103 identified threats. If we configure this initial system for SL-A 1 and assume that all elements undertake basic measures to protect confidentiality, integrity and availability this number is reduced to 82.

There are different likelihood scales proposed in [2], but all of them rely on expert judgment to rate risks. We propose to use the attack potential rating from [1], which considers the factors "Time taken to identify and exploit (Elapsed Time)", "Specialist technical expertise required (Specialist Expertise)", "Knowledge of the TOE design and operation (Knowledge of the TOE)", "Window of opportunity", "IT hardware/software or other equipment required for

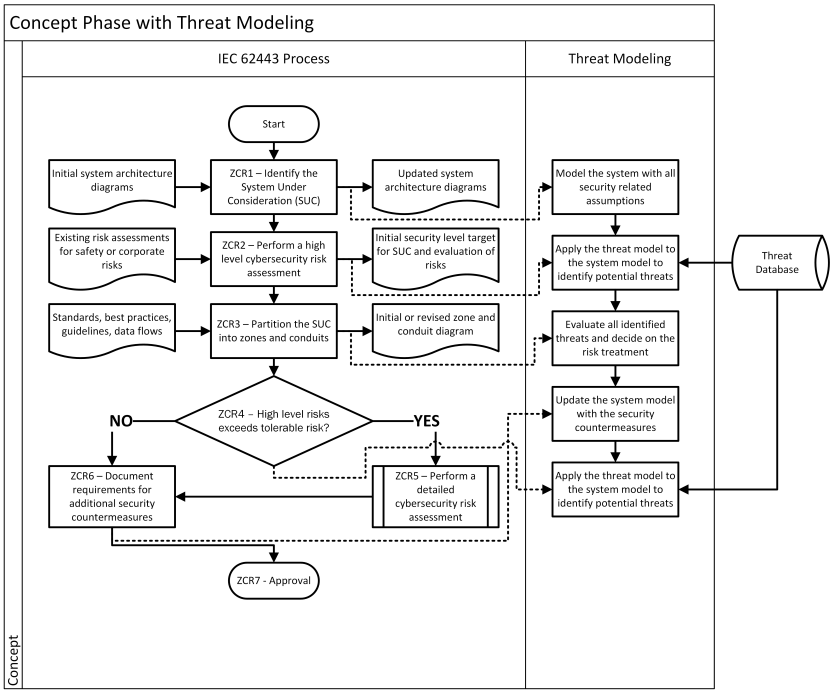

Figure 2: Integration of Threat Modeling into IEC 62443 security analysis

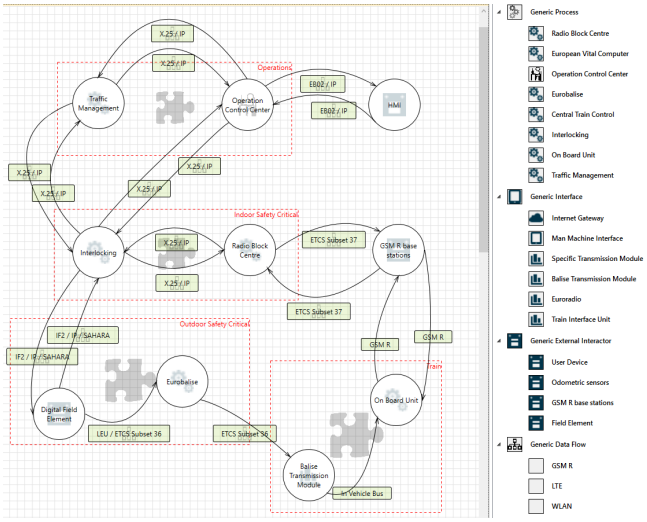

Figure 3: Application of Threat Modeling

exploitation". Based on this factors a attack potential is calculated, which is

used to determine the likelihood of a successful attack. [2] proposes a severity scale, considering Operational, Financial and HSE. Both qualitative values are be combined in a risk matrix to conduct the risk assessment.

Based on its outcome, the system is partitioned into zones and conduits and initial security measures are assigned. The zones are modeled by adding corresponding trust boundaries and security measures into the diagram. Repeating the threat modeling shows if the applied measures resolved the threats, or if new threats are introduced. If, after this initial step, the risks are not tolerable, additional threat modeling for subsets of the first data flow diagram are carried out. When all threats are either accepted or resolved, the identified cybersecurity requirements are documented and approved.

4 Conclusion

Security is one of the biggest new challenges in the railway domain. While the adoption of IEC 62443 was an important first step, there are still many open points especially regarding detailed approaches to threat identification and risk assessment. One step to improve the situation is shown in this paper: We demonstrate that Threat Modeling is a viable solution with a sufficient tool support to develop railway specific templates and apply it to real world use cases. This enables a systematic identification of threats and can be integrated into a IEC 62443 based workflow. There are some restrictions on the expandability of the Microsoft Threat Modeling tool. Due to the implementation as a Visio plugin there is no possibility to integrate it into a model-based engineering tool. Further the interface was not developed for ongoing maintainability to manage, update and extend the stencil and threat database. Further features like the integration of an automated interface between the threat database and vulnerability databases are also not possible. Due to these points we work on a new implementation of Threat Modeling in the tool Enterprise Architect which allows us to integrate the method into a model-based engineering workflow.

Acknowledgments This work is partially supported by the ECSEL projects Productive4.0 and SECREDAS (contract no. 737459, 783119) and Austrian Research Promotion Agency (FFG).

References

1. Common Methodology for Information Technology Security Evaluation. Tech. Rep. CCMB-2017-04-004 (Apr 2017)
2. IEC 62443 Security for industrial automation and control systems - Part 3-2: Security risk assessment and system design. Committee Draft for Vote (CDV) IEC 62443-3-2 ED1, France (2018)
3. Bloomfield, R., Bendele, M., Bishop, P., Stroud, R., Tonks, S.: The risk assessment of ertms-based railway systems from a cyber security perspective: Methodology and lessons learned. In: International Conference on Reliability, Safety and Security of Railway Systems. pp. 3–19. Springer (2016)

4. Braband, J.: Towards an IT Security Framework for Railway Automation. Toulouse (Feb 2014)
5. CENELEC: EN 50159:2010: Railway applications - communication, signalling and processing systems – safety-related communication in transmission systems
6. CENELEC, European Committee for Electrotechnical Standardization: EN 50128 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems (2011)
7. DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik: Electric signalling systems for railways Part 104: IT Security Guideline based on IEC 62443 (2014)
8. European Committee for Standardization: EN 50126-1 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Basic requirements and generic process (2010)
9. European Committee for Standardization: EN 50129, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling (2010)
10. He, R., Ai, B., Wang, G., Guan, K., Zhong, Z., Molisch, A.F., Briso-Rodriguez, C., Oestges, C.P.: High-Speed Railway Communications: From GSM-R to LTE-R. IEEE Vehicular Technology Magazine **11**(3) (Sep 2016). https://doi.org/10.1109/MVT.2016.2564446, http://ieeexplore.ieee.org/document/7553613/
11. Howard, M., Lipner, S.: The security development lifecycle, vol. 8. Microsoft Press Redmond (2006)
12. International Electrotechnical Commission: IEC 62443: Industrial communication networks Network and system security
13. Karahasanovic, A., Kleberger, P., Almgren, M.: Adapting Threat Modeling Methods for the Automotive Industry p. 11 (2017)
14. Koramis, Sophos: Whitepaper Project HoneyTrain. Tech. rep. (Sep 2015)
15. Lopez, I., Aguado, M.: Cyber security analysis of the European train control system. IEEE Communications Magazine **53**(10) (Oct 2015)
16. Ma, Z., Schmittner, C.: Threat Modeling for Automotive Security Analysis. pp. 333–339 (Nov 2016)
17. Microsoft: Microsoft Threat Modeling Tool (2016), https://www.microsoft.com/en-us/download/details.aspx?id=49168
18. Per Hakon Meland, Daniele Giuseppe Spampinato, Eilev Hagen, Egil Trygve Baadshaug,: SeaMonster: Providing tool support for security modeling. p. 10 (2008)
19. Rong, H., Liu, W.: Development and Research of Train Operation Control System and Safety Computer Platform Based on COTS (18), 7 (2017)
20. Strobl, S., Hofbauer, D., Schmittner, C., Maksuti, S., Tauber, M., Delsing, J.: Connected carsthreats, vulnerabilities and their impact. In: 2018 IEEE Industrial Cyber-Physical Systems (ICPS). pp. 375–380. IEEE (2018)
21. unife: From Trucks to Trains - How ERTMS Helps Making Rail Freight More Competitive (2018)
22. Winther, R., Johnsen, O.A., Gran, B.A.: Security assessments of safety critical systems using hazops. In: International Conference on Computer Safety, Reliability, and Security. pp. 14–24. Springer (2001)
23. Yi, S., Wang, H., Ma, Y., Xie, F., Zhang, P., Di, L.: A safety-security assessment approach for communication-based train control (cbtc) systems based on the extended fault tree. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN). pp. 1–5. IEEE (2018)