Risk Management and Standard Compliance for Cyber-Physical Systems of Systems

George Matta[1], Sebastian Chlup[2], Abdelkader Magdy Shaaban[3], Christoph Schmittner[4], Andreas Pinzenöhler[5], Elke Szalai[6] and Markus Tauber[7]

***Abstract*— The Internet of Things (IoT) and cloud technologies are increasingly implemented in the form of Cyber-Physical Systems of Systems (CPSoS) for the railway sector. In order to satisfy the security requirements of Cyber-Physical Systems (CPS), domain- specific risk identification and assessment procedures have been developed. Threat modelling is one of the most commonly used methods for threat identification for the security analysis of CPSoS and is capable of targeting various domains. This paper reports our experience of using a risk management framework to identify the most critical security vulnerabilities in CPSoS in the domain and shows the broader impact this work can have on the domain of safety and security management. Moreover, we emphasize the application of common analytical methods for cyber-security based on international industry standards to identify the most vulnerable assets. These will be applied to a meta-model for automated railway systems in the concept phase to support the development and deployment of these systems. Furthermore, it is the first step to create a secure and standard complaint system by design.**

I. INTRODUCTION

Cyber-physical systems (CPS) in the railway industry are increasingly being developed using IoT and cloud services, employing generic commercial-off-the-shelf (COTS) components and heterogeneous communication protocols, which raises the potential for cyber-attacks. The challenge is that cyber attacks on critical infrastructure in the rail domain are increasing in intensity. This will raise concerns about employee safety, potential security risks including the loss of sensitive information, reputational damage, financial loss and faulty decisions. Moreover, IBM statistics show that the railway industry is impacted by numerous types of cyber attacks: SQLi (SQL Injection), DDoS (Distributed Denial of Service), malware, brute force, tampering, phishing, etc [1]. For instance, Danish Railways reported that hackers perpetrated a massive DDoS attack on the Danish State Railways (DSB) in May 2018 that crippled part of its operations, including ticketing systems and communications infrastructure [2]. Therefore, we will perform a comprehensive safety and security analysis, taking into account the wireless communication used in networked and autonomous rail vehicles and modern management systems that enable communication between such CPS. In order to provide the required and appropriate mitigation measures, we have considered the risk management process, which is responsible for identifying, analysing and assessing potential threats and their mitigation such as ISO 27001 and NIST SP 800-30 [3], [4] investigated in order to enable appropriate planning [5]. In order to satisfy risk management demands for a CPSoS we adopt a methodology focused on system assets, to identify potential threats affecting the system. This requires system awareness to identify the most critical assets [6]. However, security breaches are tolerated more easily if a company can prove that the system under consideration was vulnerable despite being compliant with an international security standard [7], [8]. Therefore, we will use the existing guidelines and recommendations of IEC 62443-3-3 [9] to investigate the system's compliance to be developed. The system's configuration reflects the level of compliance. This is based on the security controls given by the standard recommendation. In our use case, we show the analysis of communication channels between different system components. For this purpose, we employ an IoT framework as a Separation Kernel (e.g. Arrowhead [10], [11]) to provide an additional abstraction layer to handle the registration, authentication, authorisation and encryption between system components.

We discuss our experience concerning the most vulnerable components of the use case, "a CPSoS in the railway domain," in a cyber-attack event. Moreover, we identify and assess potential threats and present samples related to STRIDE categories. In addition, we investigate the categorisation of potential threats to the system and most vulnerable components. Furthermore, for each threat identified, we discuss how the appropriate security controls extracted from IEC 62443-3-3 can be used as countermeasures to mitigate them. The paper is organized as follows; Section II presents state of the art on model-based approaches for security analysis, security risk assessment methods for connected vehicle systems, and analysis of information flow security CPS. Section III describes the case study and presents the risk management framework. Section IV discusses major challenges and concludes the risk

[1] Forschung Burgenland Eisenstadt, Austria
[2,3,4] Austrian Institute of Technology Vienna, Austria
[5] IQSOFT Vienna, Austria
[6] FH Burgenland Eisenstadt, Austria
[7] Research Studios Austria Vienna, Austria
[1] E-mail: george.matta@forschung-burgenland.at
[2] E-mail: sebastian.chlup@ait.ac.at
[3] E-mail: abdelkader.shaaban@ait.ac.at
[4] E-mail: christoph.schmittner@ait.ac.at
[5] E-mail: andreas.pinzenoehler@iqsoft.com
[6] E-mail: elke.szalai@fh-burgenland.at
[7] E-mail: markus.tauber@researchstudio.at

DOI: 10.36244/ICJ.2021.2.5

management process results. The road-map of our approach is discussed in Section V.

II. RELATED WORK

State of the art research has revealed several model-based approaches to manage risks posed to a system. Multiple security analysis methods based on threat modelling utilising data-flow diagrams were analysed for the CPS domain. Although they have in common that they are model-based, they employ different review methods to assess security risks for networked, autonomous vehicles. Strobl et al. analysed threats and vulnerabilities of connected vehicles, for which system assets and data flows were specified to perform safety analysis. A risk assessment of the threats and vulnerabilities potentially targeting this system was carried out. This resulted in a threat and vulnerability catalogue [12].

Ma and Schmittner [6] introduce guidelines for the implementation of threat models. They propose using a threat modelling approach specified in the "SAE J3061" guidebook [13] to identify threats and vulnerabilities. Hamad and Pervelakis have revised several existing threat modelling approaches and their potential adaption in the automotive sector. This has resulted in a hybrid threat model called SAVTA, which combines several techniques developed for the automotive industry. By identifying potential attackers and targets, an abstract model is created to achieve a holistic model. Hamad and Pervelakis concluded that effective protection measures for threat prevention, countering threats have to be permanently complemented [14].

Sheehan et al. [15] investigated the Bayesian Network (BN) cyber-risk classification model for its ability to classify the risk of vulnerabilities of a Connected and Autonomous Vehicle (CAV) GPS. The purpose was to provide vehicle manufacturers with a method to analyse CAV risk based on known systems vulnerabilities. Moreover, they used the Common Vulnerabilities Scoring System (CVSS) as a standardised framework to assess cyber threats in a CAV.

In addition, Schmittner et al. [16] show how threat modelling for railway safety analysis might be conducted during a development life-cycle based on IEC 62443. In their approach, they have proposed the identification of threats in addition to the IEC 62443-4-2 [17] security standard for Industrial Automation and Control Systems (IACS). Another approach is proposed by Shaaban et al. [18] for utilizing the concept of the IEC 62443 on the component level instead of the system level. By splitting, e.g. storage, processing units and interfaces into independent zones, different criticality levels can be assigned to these zones. This enables the mitigation of possible security risks with the help of a gap analysis for the different zones. Consequently, an application can be split into smaller portions where one part may handle communication between zones, or with other components while another zone may represent the safety-critical part of the CPS of Systems.

Additionally, in the autonomous railway vehicle requires safety measures to be applied. Therefore, besides cybersecurity, the system that will be developed depends on functional safety [19] as well as safety of the intended functionality (SotIF) [20]. Functional Safety focuses on reducing risks within a technological system to avoid malfunctions and to ensure proper operation [21]. However, functional safety does not include topics such as risks that emerge due to insufficient performance of the respective component and, consequently, safety of the intended functionality should be considered, which deals with risks caused by performance issues [21]. A sensor system not detecting obstacles due to insufficient performance may lead to a disaster. Therefore, one of our goals is to apply SotIF to the autonomous railway vehicle and in a broader sense to the railway sector which currently mainly deals with functional safety.

A management process is specified in NIST SP 800-12 rev.1 [22] for developing a set of security policies, which derives security rules from security objectives is recommended. This process analyses the need for **C**onfidentiality, **I**ntegrity, and **A**vailability (CIA) to represent a security goal. In the system concept description, components, assets and cybersecurity properties are specified as part of the system development phase. Attackers could apply different malicious activities against the system to exploit existing security vulnerabilities within components and their corresponding assets. Therefore, a potential threat targeting a vulnerability in the system also affects the CIA's security measures.

III. CONCEPT AND FRAMEWORK

In our project's context, we aim to create a system architecture model and a component catalogue for an existing interlocking system. It aims at developing "Railway Operations as a Service" (ROaaS) as the basis of a fully autonomous CPSoS. As the existing interlocking system is already Safety Integrity Level (SIL) certified, the original underlying system architecture shall remain untouched to avoid the necessity of re-certification.

Therefore, we propose integrating a risk management process within this research to identify, assess, and treat existing cyber risks. We will focus on communication topics, such as the integration of external systems and devices in particular.

In fact, we chose this risk management process approach because of the costs involved in designing and implementing secure CPS, and there are no reliable statistics on the cost differences between average day-to-day system development on the one hand and security-conscious development on the other. Anecdotal evidence suggests that security-conscious systems are more expensive [23].

In this work, we develop a secure railway system architecture. In order to represent the system model, we chose the Systems Modeling Language (SysML). SysML is a common modelling language often used by systems engineers, as discussed in [24]. SysML facilitates implementing all changes in our proposed system model in the design phase of CPSoS.

We defined use cases targeting the intended operation of the autonomous railway system. Moreover, we selected one of these use cases presented in subsection III-A. Subsequently, the required components, communication channels, and security assumptions are defined based on threat modelling.

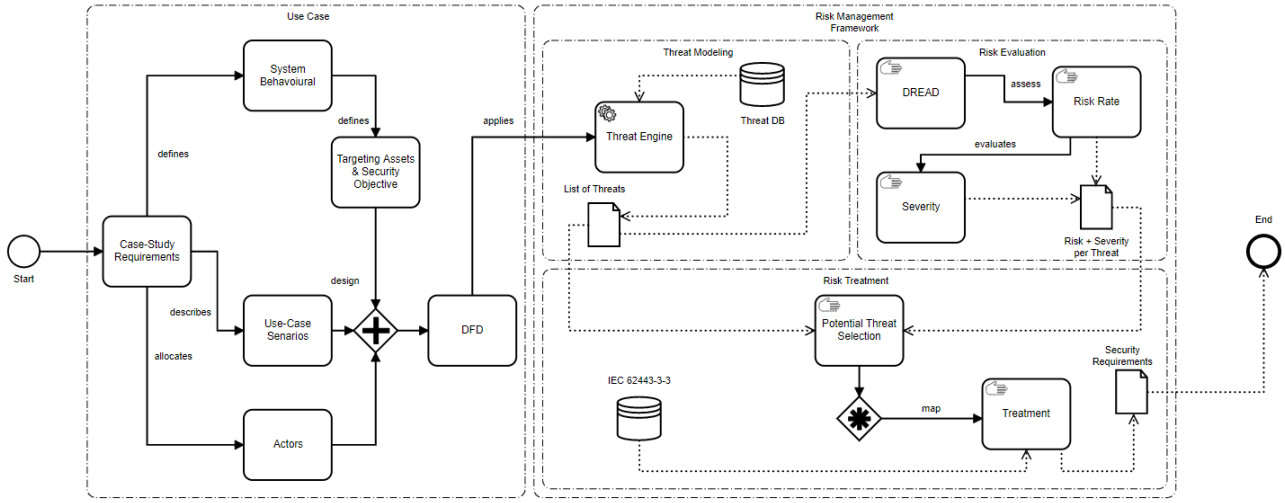

Fig. 1. Risk Management Process Model

Section III-B discusses the analysis process of identifying potential threats in the given system model. According to the identified threats, the risk evaluation process is conducted to rate each threat and define the appropriate risk level, as considered in Section III-C. Once risks have been assessed, security requirements targeting potential threats were selected based on IEC 62443-3-3, as explained in Section III-D. An illustration of this process is given in Fig. 1.

A. Specification of the Use Case

We focused on communication topics to further develop an existing industrial interlocking into a digital interlocking system and manage autonomously operating railway vehicles on secondary, less frequently used railway lines, such as the secure integration of external systems and devices in particular, e.g. COTS. Additional focus is given to their implementation impact on risks and threats.

Therefore, this work utilises an IoT framework as Separation Kernel (e.g., Arrowhead [10], [11]), which adds a layer of abstraction to build a chain of trust in such an SoS for secure communication. Moreover, the IoT framework architecture aims to enable the creation of local automation clouds that provide local real-time performance, security, inseparability, and scalability through multi-cloud interaction. Through this, it is feasible to manage various systems and, consequently, this approach is not limited to one specific interlocking system. On the contrary, by registering with the IoT framework, multiple systems can be controlled without manual configuration. Furthermore, autonomous vehicles can be mounted or unregistered on the fly. We have defined the system behavioural and actuators through the case study requirement and the already existing interlocking system. So we could identify the targeting assets and the security objectives and created the use case diagrams. All these steps enabled the creation of the Dataflow diagram (DFD). A use case diagram of the backbone of this system - the Separation Kernel as shown in fig. 2.

We identified four scenarios relevant for the coordination of such a system:

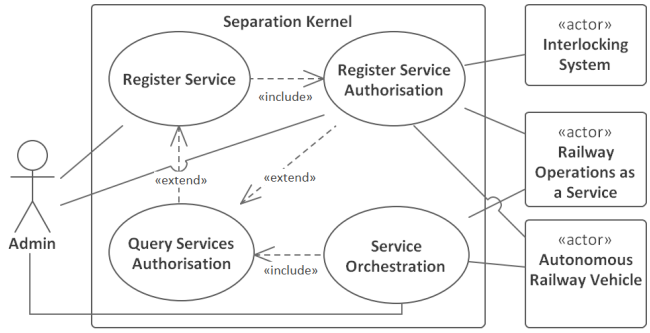

Fig. 2. Use Case: System Enquiry Coordination by Separation Kernel

1) **Register Service**: Registers the service systems in the IoT framework (ROaaS, Interlocking system, Autonomous Railway Vehicles)
2) **Register Service Authorisation**: Authorisation privileges are granted and allocated by the administrator of the registered systems
3) **Query Services Authorisation**: Validates the orchestration service requests: actor identification and authorisation, origin and destination of the request
4) **Service Orchestration**: Manages requests from the registered service systems

B. Threat Modelling

The DFD in fig. 3 illustrates a portion of the communication channels between the Separation Kernel and the several system components. The Separation Kernel serves as the communication gateway for registration, authentication, authorisation within the IoT framework and handles data encryption between system components. According to the use case described in section A, the interactions between the several system assets are as follows:

1) Request: Registration, Authentication, Authorisation; from Interlocking System, ROaaS, Autonomous Railway Vehicles to Separation Kernel

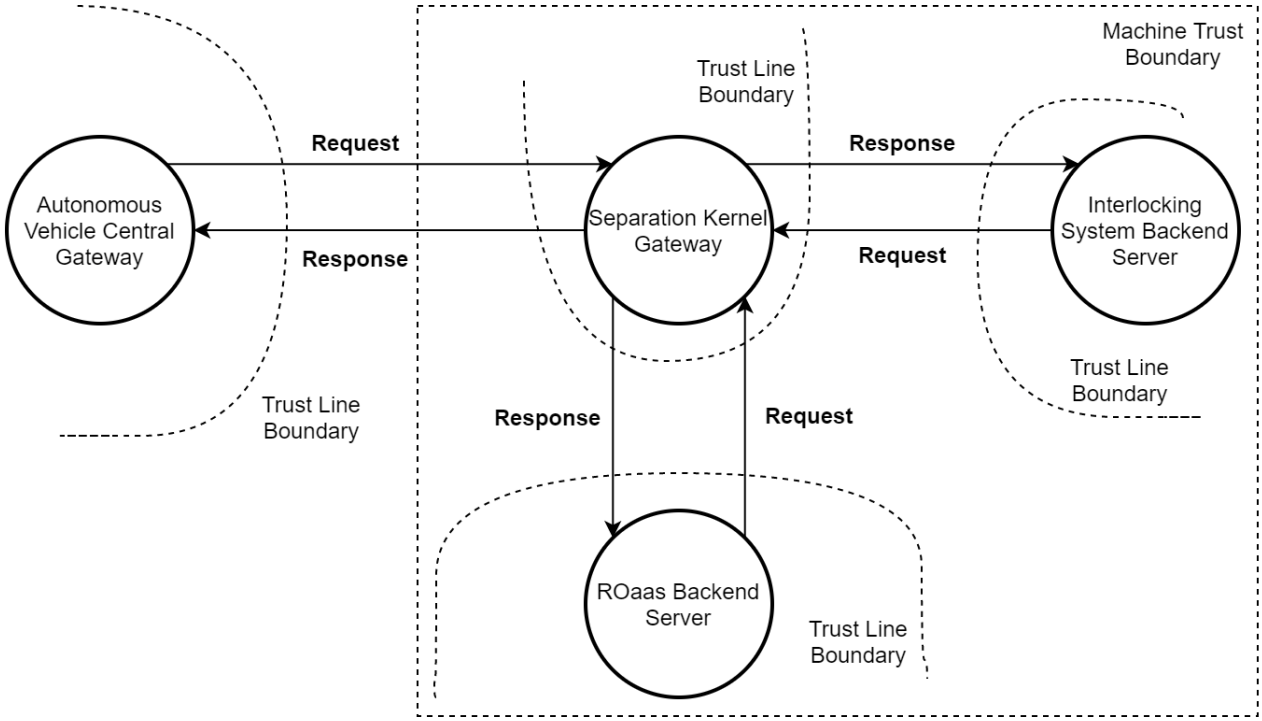

Fig. 3. DFD: Asset System Component Identifiable Data

2) Request: Stored system component identifiable data; from Interlocking System back-end server to database, ROaaS back-end server to database
3) Responses: Confirm Registration, Authentication, Authorisation; from Separation Kernel to each Autonomous Vehicle, ROaaS, and Interlocking System

Based on our DFD, we performed threat analysis using the Microsoft Threat Modelling Tool [1]. According to the threat analysis, there are 31 threats identified in the given diagram, as shown in Table I. These threats are classified based on the STRIDE model [25] categories.

TABLE I
THE IDENTIFIED THREATS COLLECTION CLASSIFIED ACCORDING TO THE STRIDE MODEL AND CIA^3 OBJECTIVES

Threat Category	No. of Threats	Security Objectives (CIA^3)
Tampering	11	Integrity
Elevation of Privilege	8	Authorization
Spoofing	5	Authentication
Information Disclosure	3	Confidentiality
Denial of Service	2	Availability
Repudiation	2	Auditing

The table summarizes the rate of all identified threats and their classifications using the STRIDE model. Each category of threat violates a specific security property (e.g., spoofing violates authentication, tampering violates integrity, repudiation violates non-repudiation, information disclosure violates confidentiality, denial of service violates availability, and elevation of privilege violates authorization). Accordingly, we use CIA^3 [14] as an extended version of the CIA according to the violations of security properties. CIA^3 establishes six categories, as follows:

- Confidentiality - protect confidential data from unauthorized access
- Integrity - ensuring that data remains unchanged
- Availability - ensuring the access to an asset
- Authentication - ensuring that an entity is who it claims to be
- Authorization - ensuring that only entities with permissions can conduct certain actions
- Auditing - Ensuring the traceability of actions

As shown in table I, the most common identified threats are considered in the integrity area for the asset system component identifiable data. In addition, we have investigated which threats may be allocated to the system components by analysing the in- and out-data flows for each component. As a result, the most affected component by 21 identified threats is the autonomous rail vehicle.

C. Risk Evaluation

The risk evaluation process comes into account of this work to assess each identified threat's risk rate. We propose using the DREAD model to analyse the risk for conducting a qualitative risk analysis to assess, compare, and prioritise the severity of risk posed by each potential threat. DREAD represents a method to determine the impact of potential threats based on five foundational aspects: **D**amage Potential, **R**eproducibility, **E**xploitability, **A**ffected Users, and **D**etectability.

[1]https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

According to the DREAD scoring system [26] and classification, the assessment is carried out in terms of a particular threat's criticality. The result reflects the criticality of a particular threat to the system.
For scoring, threats are classified as **high** (3), **medium** (2) and **low** (1). The points per category are awarded on the assumption that the attack has been started successfully. The formula for calculating the overall risk rate is as follows [26]:

$$Risk\ Rate = D + R + E + A + D$$

- **Damage Potential**: What damage will be caused if the threat occurs?
- **Reproducibility**: How easily can the attack be repeated?
- **Exploitability**: How much effort is required to trigger an attack?
- **Affected Users**: How many users are approximately affected?
- **Detectability**: How easily can the exploit be found?

Table II illustrates threats that impact the most critical system component, which we identified as the autonomous railway vehicle. These findings are based on communication between the autonomous railway vehicle and the Separation Kernel and are categorized based on CIA3 objectives and DREAD scores. Although the Separation Kernel, as shown in fig. 3 may appear to be the most critical system component, as it is the central element and has the most inbound and outbound data flows. However, in terms of component interfaces and increased security target allocation, the autonomous railway vehicle is exposed to far more threats; in fact, the autonomous railway vehicle communication is transmitted wirelessly. Furthermore, there are physical interfaces that are cumbersome to secure sufficiently. Consequently, we conclude that security threats targeting critical cyber-physical systems also affect safety. Therefore, a safety and security analysis should be performed in a well-coordinated manner.

Afterwards, a set of security requirements needs to be selected to mitigate risk emanated from the above potential threats. The next section discusses the mapping approach for addressing these threats by selecting a set of security requirements for each threat.

D. Risk Treatment Based on IEC 62443-3-3

This section presents the mapping process between the previously discussed potential threats and a set of security requirements for addressing these system security issues. The IEC 62443-3-3 is applied to create a set of security requirements against existing security threats. IEC 62443-3-3 defines four security levels for each security requirement to define the minimum and maximum security capability of each security requirement against potential threats. The standard classifies security requirements into seven groups called foundational requirements (FR), as discussed in [9]. These FRs are defined as:

- Identification and Authentication Control (IAC)
- Use Control (UC)

TABLE II
LIST OF THREATS WITH THE HIGHEST RISK RATE PER CIA^3 CATEGORY

CIA^3 Objective		Threats
Authentication	**Title**	Spoofing on vehicle gateway
	Description	Spoof autonomous vehicle central gateway with a fake one
	Category	Spoofing
	Risk Rate	11
	Severity	Medium
Confidentiality	**Title**	Access to confidential data
	Description	Gain access to confidential data through SQL Injection
	Category	Information Disclosure
	Risk Rate	15
	Severity	High
Integrity	**Title**	SQL Injection
	Description	Compromise confidential data by performing SQL injection
	Category	Tampering
	Risk Rate	15
	Severity	High
Availability	**Title**	Network Flooding
	Description	Deny actions on gateway due to flooding of network
	Category	Denial of Service
	Risk Rate	11
	Severity	Medium
Authorization	**Title**	Unauthorized access to device
	Description	Gain unauthorized access to privileged features on autonomous vehicle central gateway
	Category	Elevation of Privilege
	Risk Rate	11
	Severity	Medium
Auditing	**Title**	Removing attack footprints
	Description	Deny a malicious act and remove the attack footprints leading to repudiation issues
	Category	Repudiation
	Risk Rate	13
	Severity	High

- System Integrity (SI)
- Data Confidentiality (DC)
- Restricted Data Flow (RDF)
- Timely Response to Events (TRE)
- Resource Availability (RA)

In order to reach a security goal, we need to map between a Security Level (SL) and relevant FRs for selecting appropriate security requirements to address system design security issues, as discussed in [27], [28].
However, we have investigated how FRs could be mapped to the CIA^3 objectives and threat categories in the Risk management processes. In Table III shows the rough mapping of the FRs. In this example, we map the previously identified threats with appropriate security requirements for addressing security issues in the system design. Fig. 4 depicts a mapping of security requirements with potential threats.

The figure illustrates some of the selected security requirements according to the IEC 62443-3-3, for addressing potential threats. Each threat needs at least one appropriate security requirement for addressing its malicious behaviours. In this example, we select one security requirement for each threat according to its FR and SL. According to the DREAD risk rate, as described in Table II, we define the SL of security requirements for addressing a particular security issue. Furthermore, according to these ratings, we propose using SL = 3 and SL = 4 for each selected security requirement concerning the FR to achieve the primary goal.

CPSoS include many cyber components communicating with physical ones through different communication protocols over a network. An attacker could exploit security vulner-

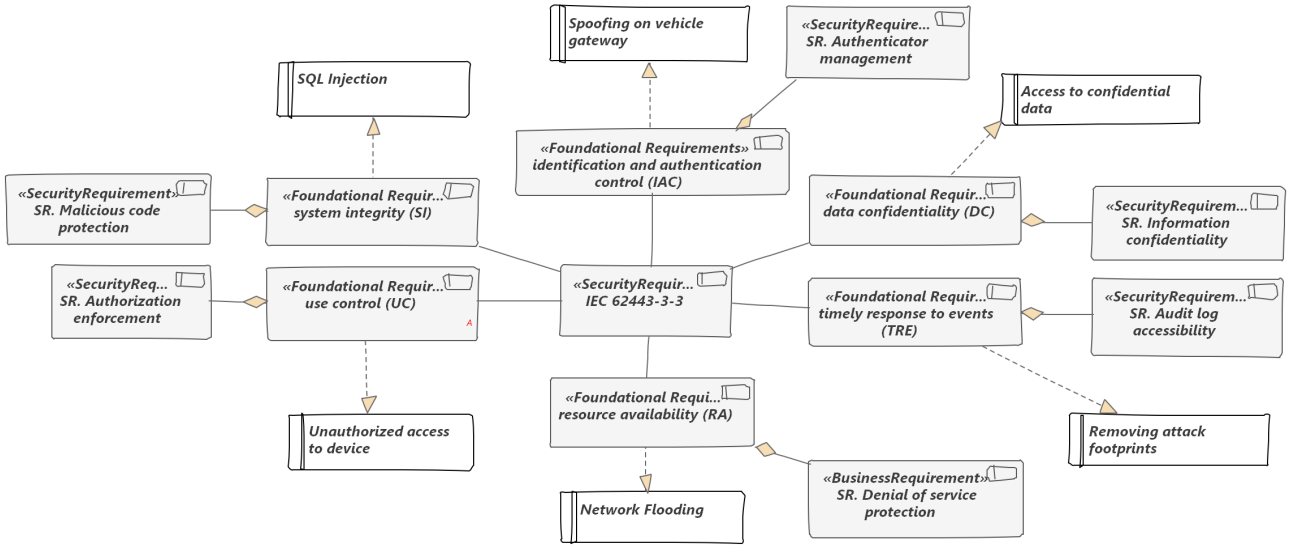

Fig. 4. IEC 62443 System Requirements Mapping with the Highest Risk Rated Threats from Table II

TABLE III
MAPPING IEC 62443-3-3 FOUNDATIONAL SECURITY REQUIREMENT ACCORDING TO CIA^3 AND THREAT CATEGORY

IEC 62443-3-3 FR	CIA³ Objectives	Threat Category
IAC	Authentication	Spoofing
SI	Integrity	Tampering
TRE	Auditing	Repudiation
DC	Confidentiality	Information Disclosure
RA	Availability	Denial of Service
UC	Authorization	Elevation of Privilege
RDF	System Segmentation	

abilities in the system's design, which leads to a different level of negative consequences in terms of safety, reliability, availability and maintainability. Furthermore, cybersecurity in railways protects data and critical units managing functional safety. Therefore, security requirements play an essential role in creating a new feature or updating existing ones for solving security issues [29]. It is essential to understand security issues to address them by an appropriate set of security requirements sufficiently.

E. Safety-Security Interaction

Current standards focus on procedural aspects of safe and secure system development and leave much room for interpretation in terms of the technical characteristics of the solution being assessed. Individual, bespoke solutions increase both the documentation effort and associated assessment costs. Generic, secure system architecture will reduce costs due to its proven and standardized security features. This will be a welcome contribution to the competitiveness of the railway sector in the future.

However, safety and security can usually not be treated independently. Thus insufficient security measures may affect the safety of such a system. This becomes evident when considering the "adversarial attack" on tesla cars [30] in the automotive domain regarding autonomous vehicles and the disruption of railway signals in 2011 [31]. The active threat landscape in the railway domain [16], [32], [33] and the high impact of safety and security issues are defined as a trade-off between security and functional safety. Safety of the intended functionality will be made, and cyber-security measures potentially affecting safety shall be analyzed in detail.

IV. DISCUSSION AND CONCLUSION

Risk management for Cyber-Physical Systems of Systems is and will remain a major challenge. As multiple components have to be examined at the same time, risks can be of various origins and, therefore, differ in their impact. However, threat modelling is a practical approach in order to identify threats in the security analysis of CPSoS in the railway sector. While the adoption of IEC 62443-3-3 was an important step, there are still many open issues that need to be addressed (e.g. the way risks are measured is a highly contested factor). In terms of assessing the likelihood and impact of a threat, most common approaches (e.g. NIST SP800-30, ISO/IEC 27001) use qualitative measures. The advantage is simplicity, risk appetite and measurement of risk. Whereas, the disadvantage of the qualitative approach is its subjectivity and imprecision. As a result, various techniques involving probabilistic models have been proposed to solve these issues (e.g. OCTAVE, CVSS). However, the complexity of the analysis and the costly estimation of the probability of the threat event occurring, as well as, the impact value provide insufficient measures during the concept phase, as there is not enough data available. These aspects have made the application of a qualitative analysis in the form of DREAD beneficial to this work.

We have shown that threat modelling is a useful and efficient threat identification method for IoT framework communication. Moreover, based on our security analysis

in Table 1, we have classified the identified threats into STRIDE categories and CIA^3 security objectives to show the highest impact. We identified the most frequently identified threats are identified in the area of integrity for the system Component identifiable data. In parallel, we have investigated which threats can be attributed to the system components by Analysing the data flow for each component. As result is that the component most affected by 21 identified threats is the autonomous rail vehicle. Table I displays that the tampering category suffers from 11 potential threats, indicating that the integrity attribute is violated the most. Similarly, we see that the attack vectors with the highest risk rate in Table II also fall in this area. We can conclude that the most vulnerable component is the autonomous vehicle and that special attention should be given to integrity and authorisation as a security objective.

V. Future Work

From a socio-technical perspective, research on trust and user vulnerability of the automated system is essential. For this, interviews with system users on security issues will be conducted to develop a concept of a hypothetical archetype of real users (persona) that can be imagined as a real person (name, age, personal habits, hobbies, emotions) which serves to express a certain user behaviour. In the next steps, the persona model and Roberta will allow us to make general deductions that will help us to describe attackers, threats to humans and machines, and also on humans and machines, at a general level. In the future, with this basis, it will be possible to have a model that makes it possible to discuss safety and security aspects comprehensively, independent of the current concrete project and occasion. Use cases depending on the product or application can be extended by these aspects in the modeling with the help of the Persona-Roberta model.

As a result, the interaction between the persona and the CPSoS might be depicted in the safety and security analysis. To evaluate its protection needs and risks and threats to the persona as a system component. Through this, multiple requirements and layers in the risk management processes can be analysed in-depth with socio-technical questions and targeted answers to design more efficient processes. Based on this, we will work on a novel approach that could allow us to integrate social aspects into the safety and security analysis to optimise resources in terms of effort and expenses.

In addition, we aim to integrate the ThreatGet tool [21] for the threat modeling process to define all existing security issues on the component and the asset level of the railway system design. Therefore, we will investigate an ontology-based reasoning approach for linking detected threats to an appropriate set of security requirements.

Acknowledgment

This work is supported by the Austrian Research Promotion Agency (FFG) and the fundings for BESTE-AB (contract no. 871551) from the "Mobility of the Future" Programme, as well as BMK and BMDW.

References

[1] R. Kour, M. Aljumaili, R. Karim, and P. Tretten, "emaintenance in railways: Issues and challenges in cybersecurity," *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, vol. 233, no. 10, pp. 1012–1022, 2019.

[2] P. Paganini, "Massive DDoS attack hit the Danish state rail operator DSB," May 2018. [Online]. Available: https://securityaffairs.co/wordpress/72530/hacking/rail-operator-dsb-ddos.html

[3] G. Disterer, "Iso/iec 27000, 27001 and 27002 for information security management," 2013.

[4] E. Aroms et al., "Nist special publication 800-30 risk management guide for information technology systems," 2012.

[5] S. Radack, "Managing information security risk: organization, mission and information system view," National Institute of Standards and Technology, Tech. Rep., 2011.

[6] Z. Ma and C. Schmittner, "Threat modeling for automotive security analysis," *Advanced Science and Technology Letters*, vol. 139, pp. 333– 339, 2016.

[7] A. Bicaku, C. Schmittner, M. Tauber, and J. Delsing, "Monitoring industry 4.0 applications for security and safety standard compliance," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2018, pp. 749–754.

[8] A. Bicaku, C. Schmittner, P. Rottmann, M. Tauber, and J. Delsing, "Security Safety and Organizational Standard Compliance in Cyber Physical Systems," *Infocommunications Journal*, vol. XI, p. 2, Mar. 2019.

[9] International Electrotechnical Commission, "IEC 62443-3-3: Industrial communication networks – network and system security – part 3-3: System security requirements and security levels," 2013.

[10] A. Bicaku, S. Maksuti, C. Hegedűs, M. Tauber, J. Delsing, and J. Eliasson, "Interacting with the arrowhead local cloud: On-boarding procedure," in *2018 IEEE industrial cyber-physical systems (ICPS)*. IEEE, 2018, pp. 743–748.

[11] D. Kozma and P. Varga, "Supporting Digital Supply Chains by IoT Frameworks: Collaboration, Control, Combination," *Infocommunications Journal*, pp. 22–32, Dec. 2020.

[12] S. Strobl, D. Hofbauer, C. Schmittner, S. Maksuti, M. Tauber, and J. Delsing, "Connected cars—threats, vulnerabilities and their impact," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2018, pp. 375–380.

[13] SAE, "Cybersecurity guidebook for cyber-physical vehicle systems j3061_201601," https://www.sae.org/standards/content/j3061_201601/, (accessed on: March 12, 2021).

[14] M. Hamad and V. Prevelakis, "Savta: A hybrid vehicular threat model: Overview and case study," *Information*, vol. 11, no. 5, p. 273, 2020.

[15] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," *Transportation research part A: policy and practice*, vol. 124, pp. 523–536, 2019.

[16] C. Schmittner, P. Tummeltshammer, D. Hofbauer, A. M. Shaaban, M. Meidlinger, M. Tauber, A. Bonitz, R. Hametner, and M. Brandstetter, "Threat modeling in the railway domain," in *International Conference on Reliability, Safety, and Security of Railway Systems*. Springer, 2019, pp. 261–271.

[17] International Electrotechnical Commission et al., "Iec 62443-4-2: 2019, security for industrial automation and control systems-part 4-2: Technical security requirements for iacs components," 2019.

[18] A. M. Shaaban, E. Kristen, and C. Schmittner, "Application of IEC 62443 for IoT Components," in *Computer Safety, Reliability, and Security*, ser. Lecture Notes in Computer Science, B. Gallina, A. Skavhaug, E. Schoitsch, and F. Bitsch, Eds. Cham: Springer International Publishing, 2018, pp. 214–223.

[19] ISO/TC 22/SC 32, ISO 26262 *Road vehicles - Functional safety*. ISO - International Standardization Organization, 2018.

[20] ——, ISO/PAS 21448 *Road vehicles — Safety of the intended functionality*. ISO - International Standardization Organization, 2019.

[21] C. Schmittner, S. Chlup, A. Fellner, G. Macher, and E. Brenner, "Threat-Get: Threat modeling based approach for automated and connected vehicle systems," in *AmE 2020 - Automotive meets Electronics; 11th GMM-Symposium*, Mar. 2020, pp. 1–3.

[22] S. NIST, "800-12 rev. 1(2017),"*An Introduction to Information Security*, 2019.

[23] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Computers & Security*, vol. 53, pp. 65–78, 2015.

[24] G. Bakirtzis, B. T. Carter, C. R. Elks, and C. H. Fleming, "A model-based approach to security analysis for cyber-physical systems," in *2018 Annual IEEE International Systems conference (SysCon)*. IEEE, 2018, pp. 1–8.

[25] A. Shostack, *Threat modeling: designing for security*. Indianapolis, IN: Wiley, 2014, oCLC: 855043351.

[26] J. Meier, *Improving web application security: threats and countermeasures*. Microsoft press, 2003.

[27] A. M. Shaaban, T. Gruber, and C. Schmittner, "Ontology-based security tool for critical cyber-physical systems," in *Proceedings of the 23rd International Systems and Software Product Line Conference-Volume B*, 2019, pp. 207–210.

[28] B. Glas, J. Gramm, and P. Vembar, "Towards an information security framework for the automotive domain." *Automotive-Safety & Security 2014*, 2015.

[29] OWASP, "C1: Define security requirements," https://owasp.org/www-project-proactive-controls/v3/en/c1-security-requirements, 2018, (Accessed January 19, 2021).

[30] K. Hao, "Hackers trick a Tesla into veering into the wrong lane," Apr. 2020. [Online]. Available: https://www.technologyreview.com/2019/04/01/65915/hackers-trick-teslas-autopilot-into-veering-towards-oncoming-traffic/

[31] K. Zetter, "Hackers Breached Railway Network, Disrupted Service," Wired, Jan. 2012. [Online]. Available: https://www.wired.com/2012/01/railyway-hack/

[32] N. Ralston, "Preventing railway cyber attack," https://www.cyberbit.com/blog/ot-security/railway-cyber-attack/ 2019, (Accessed January 19, 2021).

[33] C. H. News, "Cyber incidents affecting railways - a threat to customer data," https://cyware.com/news/cyber-incidents-affecting-railways-a-threat-to-customer-data-a8d25ccc, 2020, (Accessed January 19, 2021).

George Matta BSc. received his Bachelor degree in IT Infrastructure Management in 2021 at the University of Applied Sciences Burgenland. In parallel to his studies he worked from 2019 until 2021 as a researcher at the research center Forschung Burgenland in the research field " Cloud and Cyber-Physical Systems Security ". His research activity include cybersecurity engineering, mainly in CPSoS secure communication and security requirements management processes driven by security standardizations (e.g., ISA/IEC 62443-series, ISO/IEC27000-series).

Sebastian Chlup MSc received his master's degree in computer science in 2020 at the University of Vienna. He has been working for the AIT Austrian Institute of Technology GmbH for more than 5 years in the department of Safety and Security. His main activities include cybersecurity engineering, developing a threat modeling tool and leading a national project in the railway domain.

BSc. MSc. Abdelkader Magdy Shaaban received his master's degree in computer engineering from the Arab Academy for Science, Technology and Maritime Transport in Alexandria, Egypt. Currently, he is a PhD candidate at the faculty of computer science at the University of Vienna and working at the AIT Austrian Institute of Technology. His research interests are in cybersecurity engineering, mainly in IoT and the automotive domain. He focuses on threat analysis and security requirements management processes driven by security standardizations (e.g., ISA/IEC 62443-series, ISO 21434, IEEE 1686, and ISO/IEC 27000-series).

Christoph Schmittner Received his M.Sc. in System and Software Engineering at the University of Applied Sciences Regensburg in 2013. His main research area is safety and security co-engineering. He works on safety, security analysis and co-analysis methods, connected and safety-critical / fault & intrusion tolerant system architectures, functional safety and cybersecurity standards and interdependence of safety and security in critical systems. He is a member of the Austrian mirror committees for ISO/TC 22 Road vehicles and IEC TC 56 Dependability and designated Austrian expert in corresponding international standardization groups (IEC 61508, IEC 62443 ISO 26262 and ISO/SAE 21434), member of TC65/WG20 "Industrial-process measurement, control and automation– Framework to bridge the requirements for safety and security", TC65/AHG2 "Reliability of Automation Devices and Systems" and TC65/AHG3 "Smart Manufacturing Framework and System Architecture" and coordinating the Austrian contribution to the development of ISO/SAE 21434 "road vehicles – cybersecurity engineering".

Dr Andreas Pinzenöhler is head of innovation management and new technologies at Austrian software company IQSOFT. He graduated in "Social and Economic Sciences" at Vienna University of Economics and Business. Already his Ph.D. thesis focused on implementation of open standards in combination with model driven development methodologies. After serving as university assistant at the beginning of his career he still fulfills teaching duties giving lectures on business process modeling at his alma mater. As a senior consultant at IQSOFT, more recently he focuses on process and technology consulting for infrastructure projects. He is actively participating in international standardization activities. He contributed to the UIC RailTopo model which provides a robust fundament for the development of joint vocabularies both for rail infrastructure and rail operations. Since 2017 as member of the IFC Rail Technical Services team he made substantial contributions to the infrastructure extension of the upcoming IFC 4.3 specification. IFC is the most successful open BIM standard.

DI Elke Szalai MA works as university lecturer and research associate at the University of Applied Sciences Burgenland. Current research and teaching focus: Technology&Society, SDGs, gender and diversity aspects as well as creative techniques in technology design.

Markus Tauber He works as Chief Scientific Officer at Research Studios Austria Forschungsgesellschaft mbH. Between 2015 until 2021, he worked as FH-Professor for the University of Applied Sciences Burgenland, where he held the position: director of the MSc program "Cloud Computing Engineering" and led the research center "Cloud and Cyber-Physical Systems Security". From 2012 until 2015, he coordinated the "High Assurance Cloud" research topic at the Austrian Institute of Technology (AIT) part of AIT's ICT-Security Program. Amongst the coordinator of the FP7 Project "Secure Cloud other activities, he was computing for CRitical infrastructure IT" - (www.seccrit.eu) and involved in the ARTEMIS Project Arrowhead. From 2004 to 2012, he was working at the University of St Andrews (UK), where he worked as a researcher on various topics in the area of network and distributed systems and was awarded a PhD in Computer Science for which he was working on "Autonomic Management in Distributed Storage Systems".