Approach to generic multilevel risk assessment of automotive mobile access systems

Thomas Termin

Institute for Security Systems, University of Wuppertal, Germany. E-mail: termin@uni-wuppertal.de

Daniel Lichte

Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center, Germany. E-mail: daniel.lichte@dlr.de

Kai-Dietrich Wolf

Institute for Security Systems, University of Wuppertal, Germany. E-mail: wolf@iss.uni-wuppertal.de

Nowadays mobility companies have to deal with the digitization of analog products and services. A central scope of interest is the design of mobile access systems, intended to replace the physical key. However, these systems do not only involve new use cases but also risks that place safety and security issues in the foreground of the system design. To ensure protection against safety and security risks, a procedure that allows multilevel system evaluation is necessary. Practical experience in risk assessment (SRA) shows field-specific approaches widely used. In order to facilitate an embedded safe and secure system design, this paper introduces a generic assessment method, which considers different system configurations and multilevel safety and security risks. Within this procedure, previously identified technical requirements are mapped in a Morphological Box (MB) to describe the configuration space (CS) of the system. In order to evaluate the system, use cases and sequences as well as misuse cases are mapped using UML. Identified threats and attack paths are transferred into fault and attack trees. The results of the fault tree analysis (FTA) and attack tree analysis (ATA) allows the definition of security requirements. Additionally, the process reveals non-standard scenarios that demand further detailed analysis. The proposed approach is applied to the example of an automotive mobile access system.

Keywords: Security, Safety, Risk Assessment, Mobile Access System, Morphological Box, UML, Misuse Diagram, Requirement Engineering, Attack Tree, Fault Tree.

1. Introduction

Nowadays, Cyber Physical Systems (CPS) have become increasingly relevant in business and everyday use. By linking informational units to physical elements, these systems enhance the functional space of conventional, analog systems and are able to communicate with other CPS. According to Meyer (2019) and Schelewsky (2013), CPS offer advantages in the form of accelerating and facilitating processes. They are used in different fields of application, i.e. networked automotive systems (Lee 2008) or smart homes (Geisberger & Broy 2012),

This paper focuses on the application of mobile access systems (MAS) for vehicles. Here, the concept of CPS plays a key role in digitizing fleet and driver management (flinkey 2020). In the case of MAS, a user utilizes an application on a mobile device to interact with the locking device using a digital key that is transmitted by a backend (Fazel 2013). Additionally, MAS use cases can be extended by using software interfaces like the Software Development Kit (SDK) and the Application Programming Interface (API). However, these systems also create new risks that place both safety and physical as well as information security issues in the foreground of the system design. A primary challenge is to maintain safe and secure conditions without functional limitations within the scope of application (Wheeler 2011), since safety and security are key factors to support social acceptance by reducing operational risks (Meyer 2019); (Prokein 2011).

If several networked MAS are considered simultaneously, the task to maintain safe and secure operations gets even more complex because this potentially involves a high number of MAS configurations and use cases, respectively.

Recently, MAS research focuses especially on standardization approaches that allow consistent system design. Current research shows that the evaluation of MAS while meeting individual boundary conditions, e.g. bring-your-own-device (BYOD) policies and offline functionalities, is a major challenge (Kim et al. 2014); (Knight 2007); (Sarijari et al. 2014).

In this regard, the paper introduces a generic risk assessment method (GRAM) which considers

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Copyright © ESREL2020-PSAM15 Organizers.*Published by* Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

different MAS configurations and use cases in consideration of boundary conditions. It introduces an UML-based method, which is applied to MAS in order to enable both safe and secure design. Via this method, use cases and sequences are examined regarding potential threats. Threat scenarios are identified to design the system. The proposed method is subsequently developed and demonstrated for the example of MAS. With the suggested method, an evaluation of safety and security for MAS is possible. Finally, results are summarized and discussed.

2. Background

Due to the increasing computerization, a growing number of security requirements have to be fulfilled by system functions and questions about privacy and compatibility have to be considered in the design of the system as well (Kofler et al 2018,).

The business model (BM) of CPS often faces goal conflicts (Hoffmeister 2015). A growing number of use cases has to be fulfilled by the CPS while users demand high-level safety and security (Gerling 2017); (Steidl 2012). At the same time, meeting security and safety requirements is important for business growth, since a BM can thrive or drop in sales due to security or safety-related risks (Becker et al 2018).

In contrast to classic analog business models (ABM) (Hoffmeister 2015), digital business models (DBM) are either offered digitally or in the form of a hybrid approach (Hoffmeister 2015). MAS can be categorized into these hybrid business models (HBM). As there are different configurations and individual use cases of such hybrid systems, a generic assessment method considering physical and information risks can be helpful to ensure safe and secure design.

In order to support decision making by meeting both comfortability as well as safety and security requirements, the CPS analysis should focus on the description of interfaces of the system components (Cockburn 2015). In order to reach an acceptable level of safety and security in MAS, different methods and approaches can be used, e.g. risk analysis, checklists according to BSI basic protection guidelines (BSI 2020) or Common Criteria (CC) (CC Portal 2020). Although there are several approaches, simultaneous consideration of both safety and security requirements in system design remains a difficult task (Lichte et al. 2016).

A use case based approach for the assessment of CPS was introduced by Nicklas et al. (2016) for the example of smart homes. Still, there is no standardized method for assessing MAS in its specific application contexts (Schwerdtfeger 2018). However, security gaps in CPS still emerge years after market entry of the systems. These gaps are often detected only by security incidents (Kofler et al. 2018). As a result, customers trust gets lost despite updates because they are not willing to install them (Möller et al. 2012).

Gaps in the system performance can be analyzed from different perspectives. From the safety point of view, it is analyzed how the MAS affects the environment, people or nature (Beyerer et al 2010). Accidents are caused by events due to hazardous (sub)system conditions. Ostrom and Wilhelmsen (2019) recommend the FT to identify and define areas of hazard that potentially can lead to damages (Ostrom and Wilhemsen 2019, p. 185). Generally, accident vectors can be mutually dependent on each other.

In contrast to safety, security analyzes the impact of the environment (attacker) on the system (Wheeler 2011). According to Kofler et al (2018), threat vectors on the infrastructure of a CPS can occur physically or digitally (compare Fig. 4). Since MAS are categorized as CPS, both threat vectors apply to these systems.

In order to identify critical system units, fault tree analysis (FTA) and attack tree analysis (ATA) can be used for safety and security, respectively (Zio 2012); (Schneider 1999). In a FTA, the event is described by the detected error of a component (i.e. lack of availability according to the task) (Zio 2012). The ATA was introduced by Schneider (1999) and focusses on the intention of the potential attacker achieving a target (i.e. impairment of the availability of a unit according to the task) (Ingolsby 2016). The goal of the FTA is to find out a cause of failure, while the ATA examines the paths that are sufficiently attractive for an attacker. FT and AT show implicitly how to deal with threats as well (Wheeler 2011).

The consequences of risks are similar in safety and security cases. In the safety case, consequences are, for example, technical errors. This failure type is stochastic and the probability of occurrence can be determined for example by fatigue tests (Bertsche et al. 2004). Failure behavior can be represented by reliability respectively failure curves (Zio 2012). Human errors due to incorrect operation (misuse) are another cause for failures. This failure type is not consistently stochastic. In this case, experiments can be used to estimate how likely such errors are. (Ritz 2015).

In security cases, there are premeditated attacks on a technical system or an entity (Wheeler 2011). Here, the estimation of frequencies is not as predictable as in the safety case due to the intention of the attacker, which may be determined by many factors, i.e. threat situation or attacker properties (Wheeler 2011).

Practice has also shown that the calculation of probabilities, i.e. using Bayesian statistics, are challenging in security-related assessments because probabilities cannot be determined from evidence (event has not occurred yet) or not estimated accurately enough (due to multilevel attacks) (Wheeler 2011). As a result, high uncertainties have to be considered. For this reason, common approaches for the calculation of the probability of an attack cannot be applied for security assessments.

In this case, analysts use semi-quantitative techniques to predict the target preference of a particular attacker (Ingolsby 2016). The skill parameters of an attacker (time, skill level, necessary equipment, profit, etc.) are analyzed considering the needed resources for a specific attack. In general, attacks which are near or above the abilities of an attacker are less preferred than attacks which are fast, easy and cost-efficient (Wheeler 2011). With this, attack paths of MAS can be estimated sufficiently. However, this approach has not been applied to MAS yet.

A generic approach for multi-level and dynamic risk assessment of MAS would be helpful to support the targeted implementation of safety and security measures (Wheeler 2011).

3. Approach

In this paper, we propose a generic approach to assess safety and security risks. It allows analyzing MAS considering different configurations and use cases. The basic principles are illustrated in Fig. 1. Within this approach, a safety and security risk assessment (SSRA) of MAS is conducted. Initially, the configuration space of the system is derived from a previous technical requirement analysis and mapped in a Morphological Box (MB). The MB allows developing consistent system configurations.

In a first step, the system under examination (SUE) is categorized in the MB, thus enabling its analysis and evaluation. The categorization shows the scope of units, interfaces and general system requirements. The definition of use cases and sequences is possible by using the unified modeling language (UML) (Kecher et al. 2017). Within the scope of SSRA, the use cases are examined for possible security- and safety-related threats. The identified threat vectors are transferred into misuse cases. They point out the interdependencies between a threat and the functions of the MAS. The identified threats are then analyzed in detail by using attack trees (AT) for security and fault trees (FT) for safety.

Using the results of FTA and ATA, safety and security requirements can be defined. The results extend the requirements which are already defined in standards and guidelines.

Furthermore, these standards and guidelines can be used to check which measures are appropriate to meet safety and security requirements in the context of the misuse case and which are not. With this comparison, non-standard attack scenarios can be revealed that demand further detailed analysis. This second-last and are out of scope of this paper.

In the following, the approach will be explained by considering an example of a MAS.

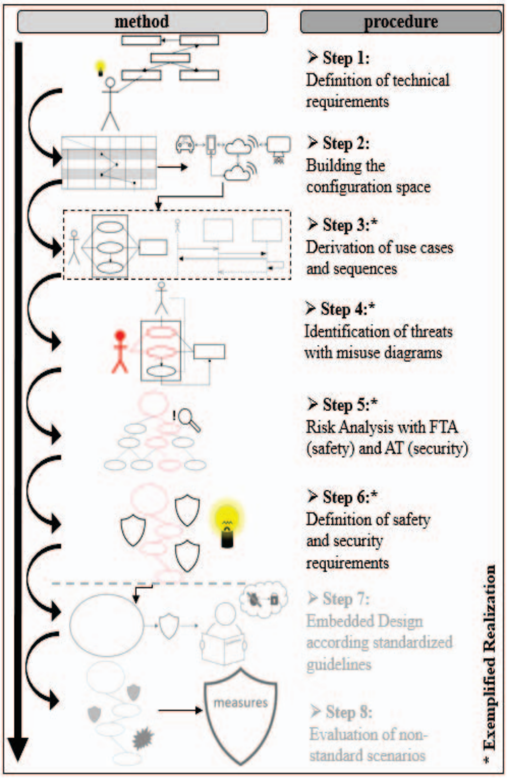
method
procedure
➤ Step 1:
Definition of technical requirements
➤ Step 2:
Building the configuration space
➤ Step 3:*
Derivation of use cases and sequences
➤ Step 4:*
Identification of threats with misuse diagrams
➤ Step 5:*
Risk Analysis with FTA (safety) and AT (security)
➤ Step 6:*
Definition of safety and security requirements
➤ Step 7:
Embedded Design according standardized guidelines
➤ Step 8:
Evaluation of non-standard scenarios
measures
* Exemplified Realization

Fig. 1. Generic Approach

3.1 MAS definition

The first step for a safe and secure MAS design is the system definition. For this, basic functions have to be identified that are characteristic for every possible configuration. This can be done by interviews or the Delphi method (Klipper 2015). In general, each MAS has to fulfill the following requirements:

- User interaction with the locking device.
- Control mechanism for user permissions.
- Interface that is accessible to the user and allows the input of user commands.

Table 1. Configuration Space of MAS

Spec Unit	1	2	3	4	5	6	7
Device	Smartphone	Smartwatch	In-house Development				
Operating System	Android	iOS	Android, iOS combined				
Mobile App	Native	Web	Hybrid				
Authentication	1-Factor	2-Factor	n-Factor				
Control Interface	Direct radio from key	NFC	BLE	Radio, NFC combined	Radio, BLE combined	WLAN	RFID
User	Only executing rights	Executing and administrative rights					
Authorization Concept	No concept	Role concept	Firm role assignment				
Key Assignment	Mobile – real time	Mobile – certain time	Immobile – certain time	Immobile – real time			
Assignment Request	Communication channel not system integrated	Systematic integrated communication channel					
Update	Update and synchronization in the background	Update and synchronization in the foreground by using	Foreground, background combined				
Protocol	User, time stamp	User, position	User, time stamp, position	Time stamp, position			
(Trust) Service	Centralized	Decentralized					

- Authentication in the app
- Hierarchical rights for users (in the form of a simple user permission (open/close) only or with administrative role (assign new users to the locking device) additionally.
- User request for locking device authorization via a channel.
- Delivery of digital keys.
- Revocation feature for ending authorization periods or invalid digital keys.
- If an authorization is time-restricted (this includes time-restrictive keys) and / or should be available offline: Option to update the device or locking device.
- Documentation of access authorizations at a central point for the traceability and transparency of user events.
- Definition of the service for secure key transmission.

3.2 MAS configuration space (CS)

In order to be able to build the general CS of MAS, it is necessary to structure the MAS in such a way that configurations emerge for elementary use cases. Therefore, the previously defined general technical requirements can be mapped in a MB in order to create the CS of MAS (compare Table 1). A MAS use case scenario is generated by combining one configuration of every system unit.

3.3 Definition of use cases and sequences

As shown in Sec. 3.2, every MAS configuration is based on use cases. They are needed to analyze the interfaces between the MAS units. Application-specific use cases demand a further detailed analysis. The CS of MAS can be described as an ecosystem consisting of the three scalable elements vehicle, backend and user with

mobile device. The communication between all three elements is carried out via interfaces.
The connections between backend and device or backend and vehicle are intended to facilitate the mutual authentication and can be realized via different channels and methods (compare Fig. 2).

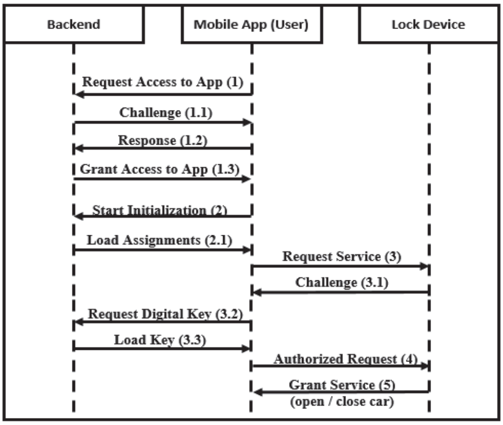

Fig. 2. Exemplary General Sequence of the Mobile Access Ecosystem

Exemplarily for the introduced example, the process of authentication between the vehicle and user can be divided into five subsequent steps (compare Fig. 2): Authentication of the user (registration and/or login): clear assignment of a (true) identity to an (authorized) user; initialization of the system (ready for operation): clear assignment of the vehicle to authorized users; key receipt ("download"); authentication on the vehicle and locking or unlocking the vehicle. As MAS must have revocation mechanisms in order to be able to deactivate or revoke user authorizations (see sec. 3.1), they have to be considered in the risk analysis.

In the scope of this paper, an exemplarily MAS is assumed that consists of the triplet mobile app, access and key management (compare Fig. 3).

3.4 Analysis of misuses cases

Accident and attack vectors are now generated and matched with MAS elements, functions and interfaces in order to show local occurrence of risks in the use cases of MAS. E.g. for the case of security, misuse cases are used to define the goals of a potential attacker. Interdependencies between an attacker the user are revealed. As illustrated in Fig. 4, the exemplary misuse cases in the analysis of the novel system show that every risk vector aims to deny car access.

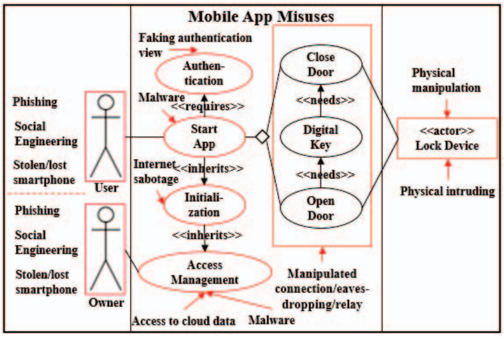

Fig. 4. Exemplary Security Misuse Cases for the Mobile App

3.5 Generation of accident and attack paths

The identified misuse cases of the previous step have to be analyzed with regard to different causes of the accident or attack vectors in order to conduct the risk assessment. For this, the accident

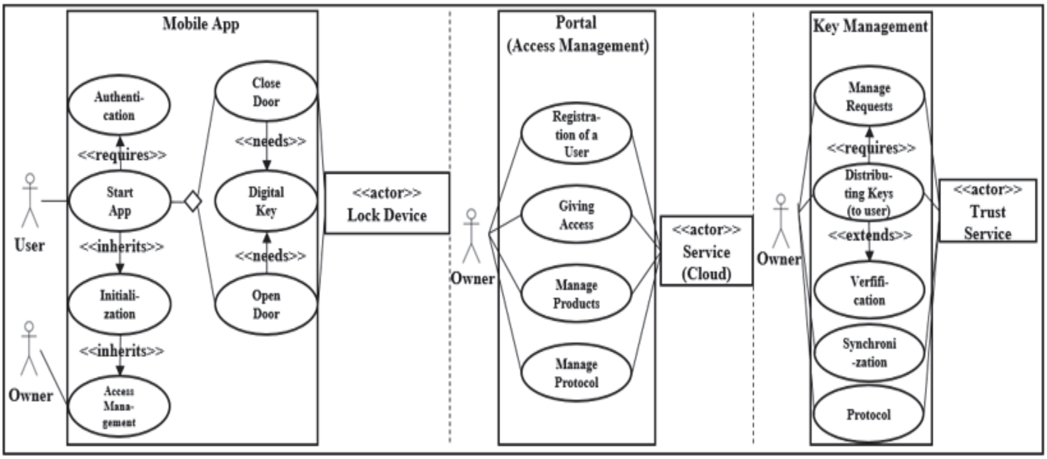

Fig. 3. Exemplary Use Cases for Mobile App, Access and Key Management

and attack vectors are transferred into FT and AT respectively (compare Fig. 5).

The results of the FT can be summarized as a failure function. A single, undesirable event (misuse) is written at the top of the FT (top event). Based on this top event, the FT is created by a top-down analysis down to the individual component failure states (Zio 2012). The failure combinations are logically linked with Boolean algebra respectively its symbols, especially "*and*" and "*or*" (Zio 2012).

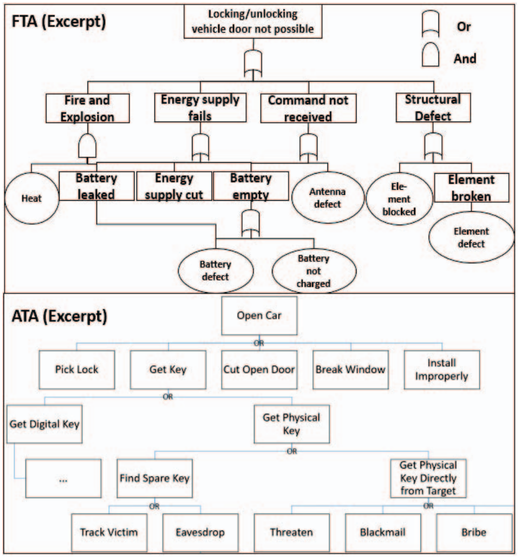

Fig. 5. Building FTA and ATA for MAS (Excerpts for the Example of the Locking Device Respectively Opening the Car)

In contrast to FT, AT help to structure attack paths and realization options. Starting from an abstract threat (= target of the attacker), concrete implementations of attacks can be identified (Ingolsby 2016). The attack combinations can be logically linked with the Boolean algebra and its symbols as well.

3.5.1 Assessment of accident and attack paths

The identification of critical paths (CP) is the basis for distributing the company's resources regarding the implementation of safety and security measures. They include system units that need to be protected in particular (Garcia 2005). CP are very system-specific, i.e. in case of MAS, elements and functions depend e.g. on the material of assemblies and the number of interfaces.

As an example, accident vectors of the locking device are assessed. In order to identify CP, the system is generally subjected to various reliability tests, i.e. cold or heat tests and load cycles for the fatigue behavior of components (Bertsche 2004). As a result, accident paths analysis is possible using the failure rates of a system unit or assembly. Thus, CP can be estimated either semi-quantitatively or quantitatively using e.g. Bayesian rules (Zio 2012); (Ostrom and Wilhemsen 2019). If the execution of such tests is not possible, reference books or expert interviews should be used to estimate the probability of failure semi-quantitatively (Klipper 2015).

From the security point of view, the primary goal of an attacker is to deny access to the vehicle. Possible Attack paths and interfaces are already illustrated in Fig. 5. Based on this diagram, the attack scenarios have to be analyzed regarding criticality. Due to the challenge of quantifying the influencing factors of an intentional attack properly, the probability of occurrence and the probability of goal achievement are ranked semi-quantitatively. This is done by the need for

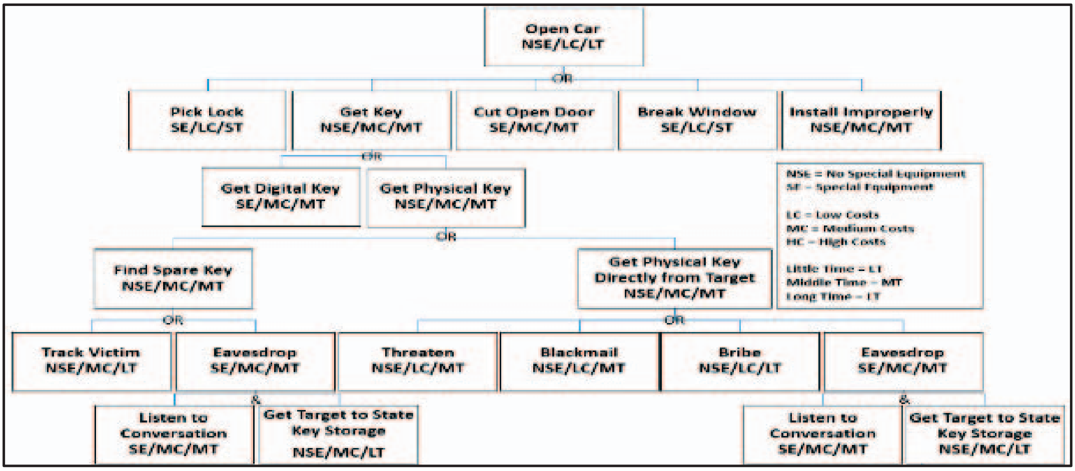

Fig. 6. Assessment of Attack Paths (for the Example of Opening the Car)

specialized equipment, the cost incurred by performing the attack event (low – middle – high) and the time it takes to complete the action (short – middle – long) (compare Fig. 6).

An approach to estimate the probability of success of an attacker, i.e. based on the number of people who usually fall to phishing or the frequency of user inattentiveness referring to pocket picking etc., is using the "What-If" technique recommended by Garcia (2005). Thus, the potential impact of different misuse scenarios can be estimated. Additionally, security critical paths can be identified by assessing the potential severity of consequences of a successful attack. Thus, the attack paths can be sorted by relevance for the MAS.

3.6 Safety and security requirements

In the first step of this generic approach, technical-functional requirements are the basis for the development of the CS of MAS for vehicles. From this, (mis)use cases and sequences respectively are generated. As shown in the FTA and ATA, the design of the interfaces is the core requirement to ensure system functionality. Especially in the process from giving a permission to the translation of the digital command into the physical unlocking of the vehicle, the digital key represents the most sensitive asset to protect in the ecosystem, since its possession enables direct access to at least one vehicle.

In order to mitigate physical and IT risks for configuring a safe and secure design, the results from FTA and ATA can be used to derive additional requirements for the design of the mobile access subsystems and processes.

4. Conclusion and outlook

Within this paper, a first generic approach is developed that integrates safety and security scenarios in the design of MAS. Initially, the differentiation between safety and security analysis was explained and different configurations of MAS design were outlined.

Although there are already initial approaches to conduct an integrated consideration of safety and security, i.e. by Lichte and Wolf (2018) or Aven (2007), it has not yet been applied to MAS. In this context, the analysis and evaluation of various configurations with specific boundary conditions represent a particular challenge. Schwerdtfeger (2018) suggested that checklists can be used to assess MAS but these do not allow a holistic consideration of safety and security risks due to different paths of accident and attack vectors.

The steps of this approach include the definition of the configuration space, safety and security use cases with related misuse cases and the assessment of risks using fault and attack trees, respectively. Non-standard scenarios are revealed that demand further detailed analysis concerning security and safety criticality.

As a result, the approach can support the safe and secure design of CPS, especially MAS. The exemplarily conducted specific MAS analysis shows that especially the secure administration and transfer of the digital key are critical functions that have to be protected with appropriate measures.

However, a disadvantage is that only the level of vulnerability for basic MAS units is assessed. The actual risk of an individually configured system must be evaluated separately.

In future work, a risk assessment of all feasible system configurations should be conducted according to the presented procedure. Overall, the understanding of the use cases and the scope of misuses are an important framework for completing a successful risk assessment.

References

Abrahamsen, E., Gould, K., Aven, T., Kaufmann, M. and T. Rosqvist (2015). A framework for selection of strategy for management of security measures. Journal of Risk Research 1–14.

Becker, W., Stradtmann, M., Botzkowski, T., Böttler, L., Voigt, K.-I., Müller, J. M. and J. W. Veile (2018). Ökonomische Risiken von Industrie 4.0, Wiesbaden, Springer Gabler Verlag.

Bertsche, B. and G. Lechner (2004). Zuverlässigkeit im Fahrzeug- und Maschinenbau: Ermittlung von Bauteil- und Systemzuverlässigkeit, Heidelberg and Berlin, Springer-Verlag.

BSI (2020). https://www.bsi.bund.de, Bundesamt für Sicherheit in der Informationstechnik.

CC Portal (2020). https://www.commoncriteriaportal.org/cc/, Common Criteria Recognition Arrangement.

Cockburn, A. (2000). Writing Effective Use Cases. Addison Wesley.

Fazel, L. (2014). Akzeptanz von Elektromobilität, Chemnitz, Springer Gabler Verlag.

flinkey (2020). https://www.flinkey.com/, WITTE Digital

Garcia, M. L. (2005). Vulnerability Assessment of Physical Protection Systems. Sandia National Laboratories, Burlington, Elsevier.

Geisberger, E. and M. Groy (2012). Agenda CRS. Integrierte Forschungsagenda Cyber-Physical Systems, Acatech Studie, München: acatech.

Gerling, M. (2017). Vom Barcode zu Mobile Commerce – Moderne Handels-IT stellt Kundennutzen in den Mittelpunkt, München, Carl Hanser Verlag.

Ingolsby, T. R. (2016). Attack Tree-based Threat Risk Analysis. Amenaza Technologies Limited, a vendor whitepaper.

Kecher, C., Salvanos, A. and R. Hoffmann-Elbern (2017). UML 2.5: Das umfassende Handbuch, Bonn, Rheinwerk-Verlag.

Kim, S. & Hong, J.-Y. & Kim, S. & Kim, S.-H. & Kim, J.-H. and J. Chun (2014). Restful Design and Implementation of Smart Appliances for Smart Home. In: 2014 IEEE 11th International Conference on Ubiquitous Intelligence & Computing.

Klipper, S. (2015). Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010, 2nd edition, Wiesbaden, Springer-Verlag.

Knight, M. (2007). Wireless security – How safe is Z-wave? IET & Computing & Control Engineering Jounal. December/January 2006/2007: 18-23.

Kofler, B, Zingsheim, A., Gebeshuber, K. Widl, M., Aigner, R., Hackner, T., Kania, S., Kloep P. and F. Neugebauer (2018). Hacking & Security: Das umfassende Handbuch, Bonn, Rheinwerk-Verlag.

Lee, E. A. (2008). Cyber Physical Systems: Design Challenges, Electrical Engineering and Computer Sciences, University of California at Berkerley, Technical Report No. UCB/EECS2008-8.

Lichte, D. and Wolf, K.-D. (2018). A Study on the Influence on Uncertainties on Physical Security Risk Management, In: Proceedings of ESREL 2018: Safety and Reliability – Safe Societies in a Changing World (Haugen, S. et al.), CRC Press.

Meyer, J.U. (2019). Digitale Gewinner: Erfolgreich den digitalen Umbruch managen, Göttingen, BusinessVillage-Verlag.

Möller, A., Michahelles, F., Diewald, S. and L. Roalter (2012). Update Behavior in App Markets and Security Implications: A Case Study in Google Play, In: Research in the LARGE: Proceedings of the 3rd International Workshop. Held in Conjunction with Mobile HCI/[ed] Benjamin Poppinga, 2012, pp. 3-6.

Nicklas, J.-P., Momrot M., Winzer P., Lichte, D., Marchlewitz, S. and K.-D. Wolf (2016). Use Case based Approach for an Integrated Consideration of Safety and Security Aspects for Smart Home Applications. IEEE 11th International Conference on Systems Engineering, June 12th-16th, Kongsberg, Norway.

Ostrom, L. T., Wilhelmsen, C. A. (2019). Risk Management: Tools, Techniques and their Application, 2nd edition. Hoboken (New Jersey), Wiley.

Ritz, F. (2018). Betriebliches Sicherheitsmanagement: Aufbau und Entwicklung widerstandsfähiger Arbeitssysteme, Stuttgart, Schäffer Poeschl Verlag.

Sarijari, M. A., Abdullah, M. S., Lo, A. and R. A. Rashid (2014). Experimental Studies of the ZigBee Frequency Agility Mechanism in Home Area Networks. In: 3rd IEEE International Workshop on Global Trends in Smart Cities, goSMART 2014. Proc. Intern. Conf., Edmonton, Canada.

Schelewsky, M. (2018). Die eierlegende Wollmilch-App – Nutzeranforderungen an mobile Informations- und Buchungssysteme für öffentliche unter intermodale Verkehrsangebote und Stand der technischen Entwicklung, Wiesbaden, Springer Gabler Verlag.

Schneider, B. (1999). Attack Trees. Dr. Jobbs Jounal (24) 12, 21-29.

Schwerdtfeger, A. (2018). Konzeption und Evaluierung eines Prozesses zur ganzheitlichen Sicherheitsbewertung von Mobile-Access-Systemen, Wuppertal, Bergische Universität Wuppertal.

Steidl, B. (2012). Die Auswirkungen des Near Field Communication Übertragungsstandards auf das bargeldlose Bezahlen mit Mobiltelefon – dargestellt am Beisipel CardMobile, Multimediaarchiv, Hochschule Mittweida.

Terje A. (2007). Reliability Engineerung & System Safety, Volume 92, Issue 6, pp. 745-754.

Wheeler, E. (2001). Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Waltham, Syngress.

Zio, E. (2012). An introduction to the basics of reliability and risk analyses. Series in Quality, Reliability and Engineering Statistics, Vol. 13, World Scientific.