# Use Case based Approach for an Integrated Consideration of Safety and Security Aspects for Smart Home Applications

Jan-Peter Nicklas, Michel Mamrot, Petra Winzer
Product Safety and Quality Engineering
University of Wuppertal
Wuppertal, Germany
{nicklas, mamrot, winzer}@uni-wuppertal.de

Daniel Lichte, Stefan Marchlewitz,
Kai-Dietrich Wolf
Institute for Security Systems
Velbert, Germany
{lichte,marchlew,wolf}@iss.uni-wuppertal.de

***Abstract*—An increasing number of Cyber Physical Systems is used in different areas of applications like smart grid, smart factory or smart home. This paper demonstrates a first approach for an integrated consideration of safety and security for Cyber Physical Systems in a System of Systems by a use case based model for smart home applications. To realize a safe and secure operation of Cyber Physical Systems in System of Systems a high number of elements, relations and functions have to be taken into account. A Systems Engineering based approach will be introduced in this paper to deal with this complexity. The approach consists of a SysML based model which is associated with a procedure to ensure the safe and secure design of Cyber Physical Systems. Defined safety use cases will be used in a following security analysis and assessment. By harmonizing security assessment and safety use cases the integrated consideration is accomplished. The results can be used for an early technically solution neutral design planning.**

***Keywords*—System of Systems; Cyber-Physical Systems; Smart Home; Use Case Models; Safety; Security**

## I. INTRODUCTION

Cyber Physical Systems (CPS) have recently become more and more important. CPS are mechatronic systems and consist of sensors, actuators, an embedded intelligence and the ability to communicate with other CPS [1]. Obviously, the focus on research in CPS areas like development and applications is rising [2]. Applications of CPS are diverse, e.g. advanced automotive systems, environmental control or smart structures [3], like e-health, smart home, smart factories, micro grids etc. [2]. In this article smart home applications like smart infrastructures are focused on, since smart home applications are a growing market [4, 5]. Furthermore, smart home can be defined as an intelligent environment. This environment is able to apply and acquire knowledge about the inhabitants, their surroundings and other parameters in order to adapt and meet predefined goals [6,7]. Thereby different CPS can work together in such smart home applications. As a result these applications can be described by systems thinking as a System of Systems (SoS) of CPS. To provide a successful and accepted performance it is a primary challenge to maintain safe and secure operation of these CPS in SoS for smart home applications [2], since safety and security requirements are most important [8]. To construct a single system adequately safe and secure is a difficult task, because of inherent goal conflicts [9]. For example a secure locking of a door lock in a smart home to protect against intrusion and a safe unlocking in case of an accident to allow access for rescuers. If several CPS are considered simultaneously, this task is getting even more difficult, because of the high number of resulting CPS combinations and accompanied use cases. Frequently, interfaces or technical standardization approaches for communication are focused on in CPS research. Yet these approaches are not harmonized as the interoperability of billions of connected devices has to be realized [5, 10, 11]. The detailed level and discipline specific focus of these approaches do not allow a sufficient adaption of the design of the SoS. Hence there is a need for a first overview regarding an integrated consideration of CPS in SoS in context of safety and security features. [12] demands such a model for single CPS.

Many different and divergent aspects have to be considered for an integrated approach. For example the following aspects can be named [13]:

- Hazards (fire, electrical shock) through electronic devices or unauthorized access.
- Malfunctions of safety-relevant systems (e.g. smoke detectors, locking systems, e-health etc.).

Therefore, a new use case specific model will be presented in this article. With the help of use cases different aspects will be investigated and integrated into a SysML based model. First the state of the art is described to illustrate the safety and security challenges, since an integrated consideration of safety and security factors is missing yet. Afterwards a first simplified model focusing on the CPS in the SoS based on use cases is build up. Overlapping use cases (by time and location) are investigated in the procedure and supported by the model for a safe and secure design. Finally, results are summarized and discussed.

## II. STATE OF THE ART

In the scientific context, safety and security are often defined as a deliberate threat (security) and an unwanted hazard (safety) [14]. Safety functions are designed to protect users from hazards, e.g. an accident. Security functions protect

the system and its contents against attacks like an intentional misuse. The variety of components and their IT-based networking lead to a growing number of safety and security requirements, which have to be fulfilled by functions.

Focusing on CPS the variety and diversity of requirements, components and functions is more and more growing [3]. Often these functions are in a fundamental goal conflict. For reasons of safety, redundancies are designed to ensure safety in dangerous situations. Simultaneously these redundancies should not be implemented for reasons of security, because they result in additional attack vectors. Consequently, safety and security functions affect each other.

Additionally, system complexity is increasing. Complexity is defined by the number and diversity of elements, relations as well as dynamics [15], e.g. due to networked systems. This results for example in additional required security functions to avoid an intrusion into the SoS. Complexity is described, beside the diversity of elements, by the high number of participating systems. In turn systems, which carry out tasks independent of each other, as well as together for a limited period of time, can be considered as a System of Systems or SoS [16]. According to [16] the SoS of CPS will be defined in this article as a virtual SoS. The characteristics of a virtual SoS are [16, S.405]:

- No central management and no overarching agreed-upon purpose.
- No consistent configuration or maintenance of the SoS as a whole system.
- Individual constituent system will be configured and managed.

These systems themselves consist of a variety of components for example authentication, locking and control, which implement various safety- and security-related functions. As there is no central management or consistent configuration of such a virtual SoS an integrated safety and security considering model is needed.

The single use cases of the CPS allow an extensive description of the safety-related behavior of the CPS themselves. These use cases do not describe the behavior of the SoS consisting of different collaborating CPS. To focus on a comprehensive description of safety and security aspects and resulting goal conflicts, intersection points between the CPS have to be investigated. These intersection points have to be defined by CPS specific use cases, which can be postulated [17]. Certainly, these do not contain the needed information.

In order to reach a defined level of safety and security, different methods and concepts can be used, e.g. TSM or GlobalPlatform for security architectures or risk analysis to estimate a safety level. Although specific methods for safety or security exist, an integrated, simultaneous consideration of both aspects is not possible yet [18, 9] or only for software related aspects [13].

Safety and security aspects need an interdisciplinary understanding for CPS as well as CPS in SoS. Many existing approaches lack a common understanding [9]. Focusing on complexity Systems Engineering (SE) can handle these challenges [19] as it is about “creating effective solutions to problems and managing the technical complexity of the resulting developments” [20]. SE includes a system model for handling complexity with an interdisciplinary procedure. However many different SE-based approaches were developed. In [21] a first common model for SoS was developed and combined with a procedure. This new Generic Systems Engineering (GSE) based procedure consists of a standardized procedure using the modules “analysis” (problem identification and system analysis), “target definition” (problem localization) and “design” (recommendations) [22]. These modules have to be arranged problem-specific. Different GSE based approaches are used, e.g. for requirements engineering [23] or for the design support for autonomous robots [21, 19]. However, the existing system model, which was introduced in [21] does not support the specific combination of CPS in SoS which is needed for an integrated safety and security consideration as well as a standardized notation. Therefore, a SysML-based approach will be used. Based on its diagrams and standardized notations, an integration in the existing common GSE model of thinking can be realized.

In summary, the following challenges were identified:

- No standardized model for SoS (of CPS) for safety and security aspects.
- Missing description of the virtual SoS and its behavior by the CPS specific use cases.
- Difficulties in handling diverging high level use cases caused by inherent complexity.

To deal with these challenges, the approach for an integrated consideration of safety and security aspects for smart home applications will be developed and introduced in the following section.

## III. Approach

In order to fulfil complex tasks of system analysis and further development, a Systems Engineering based approach is introduced [24]. This new GSE based approach is shown in Fig. 1. The proposed procedure is combined with a safety and security integrated system model for smart home applications. In step A the SoS and its scope has to be focused upon by using the GSE-module “analysis”. This analysis is initially realized by the CPS use cases. Certainly hazardous behavior of the SoS can only be identified via a combination of use cases, e.g. by time and location intersection points. Step B is used for the safety use case definition based on SysML notation and diagrams. This is combined with the GSE target definition module. Through the support of the GSE based analysis module the safety use cases and related attack scenarios are identified in step C to secure a safe operation of the SoS. The security analysis based on the derived safety use cases is necessary, as every safety use case possibly creates new attack vectors. This ensures the extensive analysis of goal conflicts between safety and security. Finally, the harmonization of safety and security is carried out in step D. As a result, design recommendations can be derived based on the GSE-module “design”.

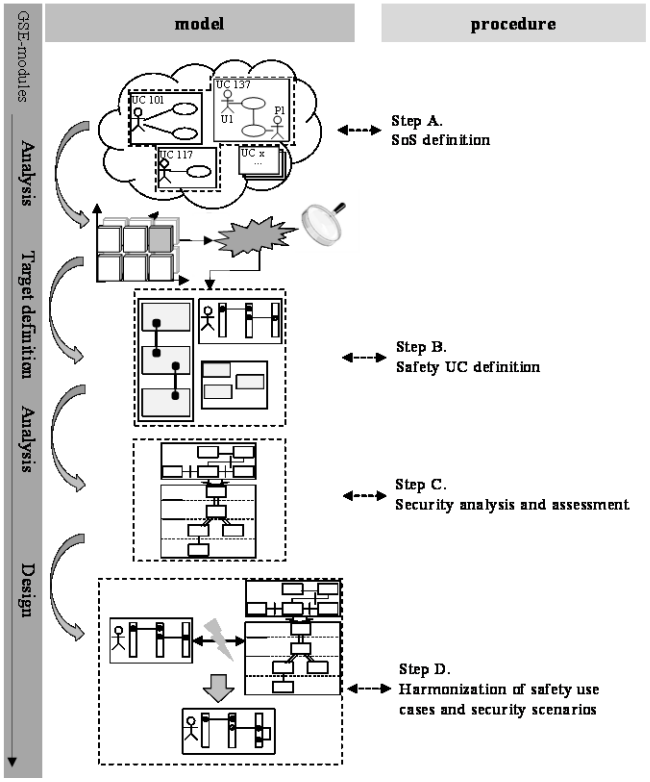


Fig. 1. Approach

Following, the four step based approach will be explained in detail.

A. SoS definition

In a first step, which is based on systems thinking, the system scope has to be limited. This limitation of a complex sociotechnical system like the proposed SoS into its subsystems and users is needed to handling the systems' complexity [25]. With this limitation, systems and interacting users are focused on. In this article an example based on four different systems will be used:

- Autonomous vacuum cleaner (AVC),
- Smart wristband (SWB),
- Intelligent door lock (IDL) and
- Communication hub (CH).

In addition, the communication hub is understood as a part of the SoS and not as a central management as it only enables the communication between the systems. With the help of these systems the identified challenges and use cases have to be derived. A typical use case description includes pre-conditions, post-conditions, primary flow and an alternative or exception flow [26]. Therefore, a predefined template, like shown in [19] is suitable. Different possible use cases are shown in Fig. 2.

These use cases have to be analyzed regarding safety risks. The challenge is to identify every hazard resulting from an interaction of two or more CPS. This interaction is depicted by the intersection points with regard to time and location. For example, the use case analysis determines that the use cases "IDL1-locking" and "IDL2-unlocking" (see Fig. 2) cannot overlap.

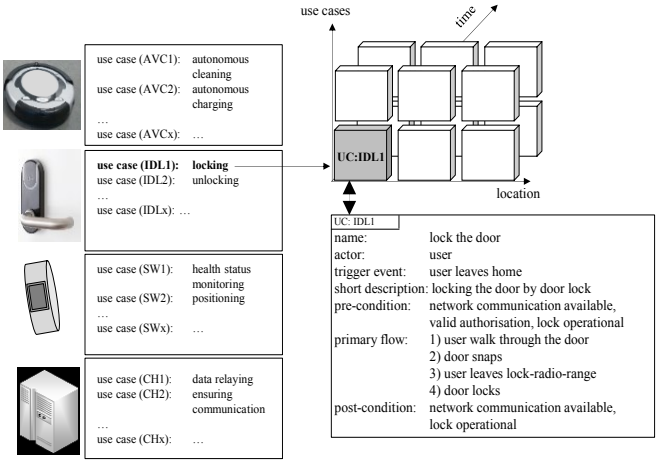


Fig. 2. Use cases and combination

In addition, "AVC1-autonomous cleaning" and "AVC2-autonomous charging" will not be focused on, as the autonomous vacuum cleaner has to be charged by a charging station. These use cases cannot overlap either. In the following exemplary application these four use cases will be used:

- Use case "AVC1-autonomous cleaning"
- Use case "SW1-health status monitoring"
- Use case "SW2-position tracking"
- Use case "CH2-ensuring communication"

By the combination of the use cases the virtual SoS is formed out of the autonomous vacuum cleaner, the smart wristband and the communication hub.

For the identified intersecting use cases, respectively the new CPS in SoS, a risk analysis has to be performed. This risk analysis is state of the art and therefore not focused on below. Here, the risk is defined in a quantitative or qualitative way as a function of the severity, the exposure, the occurrence and the controllability [27].

By this procedure the risk is assessed for the corresponding use case (Step B). As a result potential risks were identified for the following steps (Step B-D) to achieve a sufficient safe and secure SoS.

B. Safety use case definition

With the result of step B safety use cases are defined. The goal of the safety use cases is derived from the risk analysis in step B. In the example of the combined use cases "AVC1" and "SW2" the collision between the user and the AVC should be avoided. Therefore, a new use case "AC" (avoid collision) is defined. The following Fig. 3 shows the storyline of this use case.

| Saftey UC: AC | |
|---|---|
| name: | avoid collision |
| actor: | user |
| trigger event: | falling below safety distance |
| short description: | avoid collision between user and „AVC“ |
| pre-condition: | user wearing „SWB“, „AVC“ operational, network-communication available |
| primary flow: | 1) recognize direction of user<br>2) adapt direction of „AVC“ to regain safety distance |
| Alternative flow: | 1) recognize direction of user<br>2) adapt direction<br>3) collision |
| post-condition: | user wearing „SWB“, „AVC“ operational, network-communication available |

Fig. 3 Safety use case "AC"

Unlike the use case “IDL1-locking” (see Fig. 2) the safety use case “AC” has an alternative flow, that includes a possible collision. Therefore it is necessary to consider another safety use case which focuses on the resulting hazard of the collision. In consequence the safety use case “emergency” is equally defined and documented.

To describe the interaction of the safety use cases a sequence diagram is used. Sequence diagrams are based on the predefined use cases [17]. The use cases will be depicted and considered in the safety sequence diagram. Here, the needed message exchange to describe the functionality of the safety scenario is shown [28].

In the example the alternative flow from safety use case “AC” is represented by the first two sequence steps of the diagram. The other part illustrates the steps of the subsequent safety use case “emergency”. A rescue alert will be triggered and “IDL” will open if the health status of the user is critical (see Fig. 4).

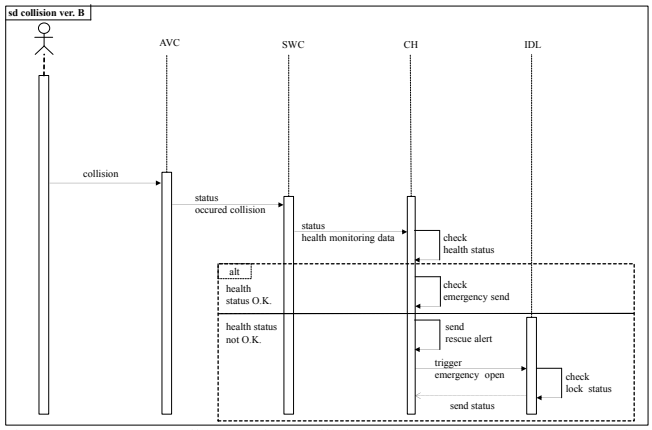


Fig. 4. Sequence diagram for “collision” from safety UC: AC and safety UC: emergency

The technical safety relevant information flow of the involved CPS “AVC”, “SWC”, “CH” and “IDL” is determined by an internal block diagram (see Fig.5). In addition to the logical task-orientated sequence the internal block diagram allows the description of information flow. Therefore, a design support of the specific CPS and further security analysis is prepared. The specific use case based communication scheme can be depicted by the flow of information. Fig. 5 presents the information flow through the radio communication port “RC”. The direction of the information flow becomes apparent. Likewise, redundancies can be defined.

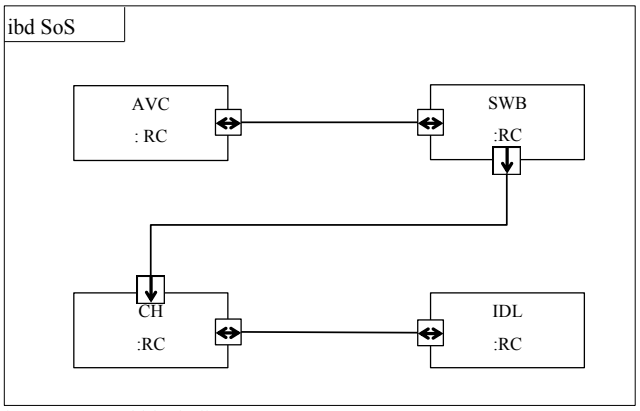


Fig. 5. Internal block diagram

Based on the internal block diagram a security analysis and assessment is prepared in step C.

C. Security analysis and assessment

In step C the needed security measures for preventing the intended occurrence of threats as results of the safety use case by an outside attacker are defined. The goal is to describe barriers between components, that show necessary limitations of information flow and encryption of communication between the components of the SoS. Both information can be used to extend the structure of the solution of the safety use case by adding security barriers and hierarchic structures.

Therefore, the SoS is analyzed via a security assessment based on attack scenarios. The most important results of these scenarios are goals and methods of the attack. The safety use case derived in step B is used to define the goal of the attack. The attack goal that results from the exemplary safety use case is gaining access to the home. Feasible attack paths and methods are deduced by the diagrams of the SoS defined in step B, which show involved CPS and information flows between them. The description of use cases and attack paths can make the integration of further SoS components necessary. The resulting simplified attack scenarios are summarized in attack trees, which were introduced by [29].

Fig. 6 shows five resulting scenarios defined by the SoS information flow of the use cases. Following, a qualitative assessment is conducted on the SoS considering the developed security scenarios. The assessment includes a ranking regarding the probability of occurrence (PO) and goal achievement (PG) based on the attack trees shown in Fig. 6. As scenario $S_5$ is very unlikely in terms of PO and PG, it is excluded from further analysis.

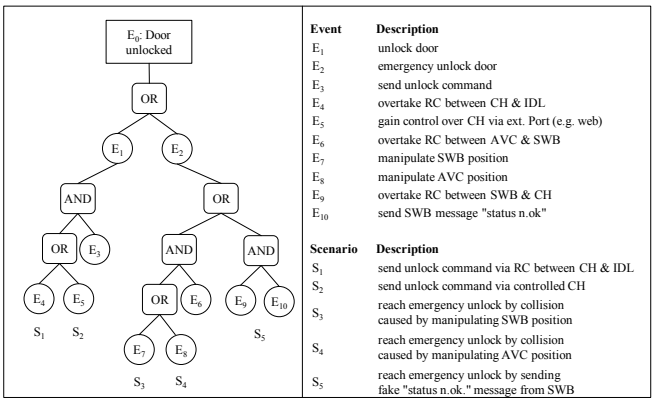


Fig. 6. Attack tree

As a result of the security analysis the attack vectors of the probable scenarios ($S_1$-$S_4$) have to be investigated. This shows where barriers are needed to secure the considered SoS for the specific use case. The simplified block diagram in Fig 7 depicts this.

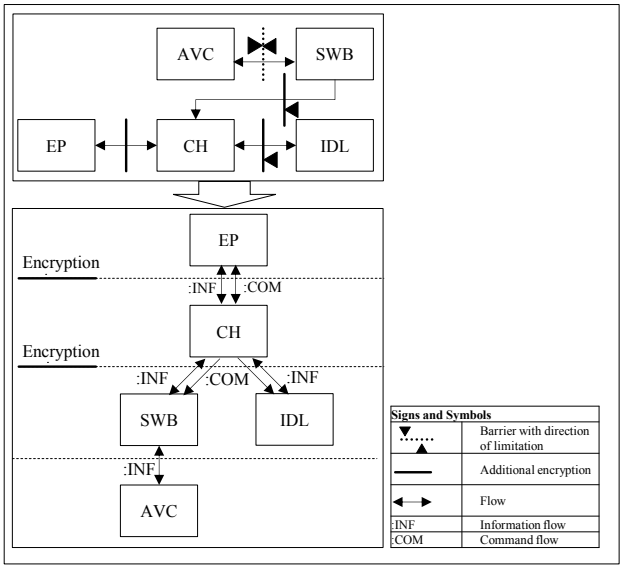


Fig. 7. security ibd and communication flow

These barriers describe the limitation of flowing information or needed encryption. Additionally, a hierarchic diagram can be established by analyzing the proposed limitation of the direction of commands and information flow between the components of the SoS.

D. Harmonization of safety use cases and security scenarios

In the last step, the results of B and C will be matched to expose and solve the safety-security goal conflicts related to the analyzed safety use case. As a result, Fig. 8 shows a harmonized sequence diagram to achieve an adequate safety and security level. The analysis of information and command flow leads to changed connections in the sequence diagram. In the explained example, the connection of "SWB" and "AVC" is identified as security critical. Therefore, the check tasks "check health status" and "check send emergency" have to be executed by the "CH". The activity "send rescue alert" is additionally realized by the "CH". As a result, the sequence diagram "sd collison vers. B" is recursively adjusted.

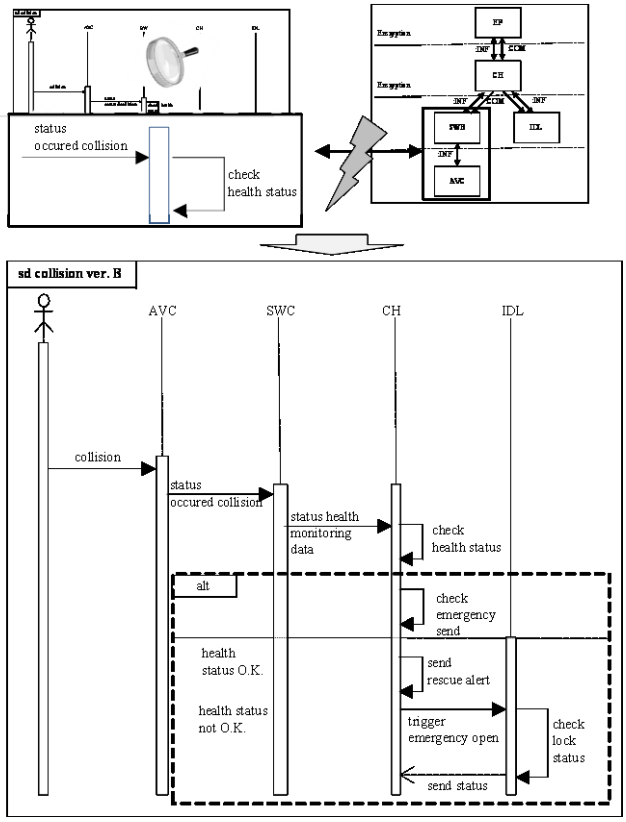


Fig. 8. Harmonization of safety use case and security analysis

As a result an integrated safety and security consideration for the SoS based on the use cases is derived. On the one hand possible goal conflicts between safety and security functions are revealed. On the other hand the method enables a designing process that solves these conflicts. Due to the high degree of abstraction, early and technically solution neutral design can be planned.

## IV. Conclusion and Outlook

In this article a first use case based approach was developed, which integrates safety use cases and resulting security scenarios for a widespread overview. First the problem was considered and the state of the art regarding smart home and SoS was outlined. Obviously, existing models and approaches do not focus on an integrated safety and security view. Simultaneously the security of smart home systems has to be considered in a more detailed way with regard to users and experts. Hence this article proposes an approach based on Systems Engineering to analyze and harmonize safety and security at the same time. The four steps of the approach include use case definition, safety use case definition, security scenario analysis and harmonization. Additionally, an example illustrates, how the concurrent single steps can contribute to a safe and secure model of the SoS, which is enhanced in every step of the procedure. In the first step, use cases were defined and combined by time and location for the identified systems of the SoS. These combinations were analyzed. Step B

comprised the definition of the resulting safety use cases to avoid risks. They were described by storyline, internal block diagram and sequence diagram in SysML based diagram types [30]. The security analysis in step C identified attack goals as a result of the safety use cases and establishes attack scenarios based on attack trees. The probabilities of occurrence and goal achievement of the attack scenarios are qualitatively assessed and security structures containing the limitation of communication and encryption were derived. The resulting security structure was compared to the safety use case in the last step D. Occurring goal conflicts were solved by adapting the sequence diagram of the safety use cases.

Thus, a first viewpoint for an integrated safety and security based model was introduced. A generalization of the developed approach has to be investigated by further research. For the virtual SoS additional CPS combinations have to be examined. It is of particular interest to investigate the safety and security implementation for other SoS classifications, e.g. directed SoS [16]. It has to be tested if the developed safety and security integrated model can be used for other SoS applications, e.g. smart factories. Furthermore, a quantification of the inherent safety and security goal conflicts has to be realized. By the interdisciplinary character of the different application types, a common model of thinking seems to the useful [22]. In consequence the SysML based diagrams have to be used for an integration into a common model of thinking like proposed in [21].

## REFERENCES


[1] R. Anderl, R. Picard, and K. Albrecht, "Smart Engineering for Smart Products," in M. Abramovici and R. Stark, "Smart Product Engineering". Proceedings of the 23rd CIRP Design Conference, Bochum, Germany, March 11th-13th, 2013. Heidelberg: Springer Verlag, 2013, pp.1-10.

[2] E. Geisberger and M. Broy, "agenda CPS. Integrierte Forschungsagenda Cyber-Physical Systems," Acatech STUDIE März 2012. München: acatech, Deutsche Akademie der Technikwissenschaften, 2012.

[3] E. A. Lee, "Cyber Physical Systems: Design Challenges," Electrical Engineering and Computer Sciences, University of California at Berkeley. Technical Report No. UCB/EECS-2008-8.

[4] A. Hoberg, C. Piele, and J. Veit, "Mobiles Lernen für Smart Home / Smart Grid," in HMD Praxis der Wirtschaftsinformatik. June 2013, Vol. 50 Issue, 3 pp.80-94.

[5] S. Kim, J.-Y. Hong, S. Kim, S.-H. Kim, J.-H. Kim, and J. Chun, "RESTful Design and Implementation of Smart Appliances for Smart Home," 2014 IEEE 11th International Conference on Ubiquitous Intelligence & Computing and 2014 IEEE 11th Conference on Autonomic & Trusted Computing and 2014 IEEE 14th International Conference on Scalable Computing and Communications and Associated Symposia/Workshops, IEEE:2014, pp.717-722.

[6] N. Saito and D. Menga, "Ecological Design of Smart Home Networks," Woodhead Publishing/ Elsevier, Cambridge, MA, 2015.

[7] C. Yang, B. Yuan, Y. Tian, Z. Feng, and W. Mao, "A Smart Home Architecture Based on Resource Name Service," IEEE 17th International Conference on Computational Science and Engineering 2014, pp. 1915-1920.

[8] A. Wong, et al., "Safety and security concerns among Singapore elderly towards home monitoring technologies in smart home," Proceedings of ergonomic trends from the east, Kitakyushu(Japan), CRC Press Taylor & Francis Group, 2008.

[9] D. Lichte, S. Marchlewitz, P. Winzer, and K.-D. Wolf, "Safety- und securityrelevante Zielkonflikte in automobilen Sicherungssystemen," in K.-D. Wolf (ed.): Tagungsband innosecure - Kongress für Innovationen in den Sicherheitstechnologien, 22.-23.04.2015, Velbert-Heiligenhaus, S. 211-221.

[10] M. Knight, "Wireless security – How safe is Z-wave?" in IET& Computing & Control Engineering Journal. December/January 2006/2007., S. 18-23.

[11] M. A. Sarijari, M. S Abdullah, A. Lo, and R. A. Rashid, "Experimental Studies of the ZigBee Frequency Agility Mechanism in Home Area Networks," 3rd IEEE International Workshop on Global Trends in Smart Cities. goSMART 2014. Edmonton, Canada.

[12] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber-Physical Systems," Proceedings of the IEEE, Vol.100, No.1, January 2012.

[13] C. W. Axelrod, "Managing the Risks of Cyber-Physical Systems," IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2013, pp. 1-6.

[14] J. Beyerer, J. Geisler, A. Dahlem, and P. Winzer, "Sicherheit: Systemanalyse und –Design," acatech diskutiert: Sicherheitsforschung – Chancen und Perspektiven. Springer Verlag, Berlin, 2010.

[15] C. M. Meyer, "Integration des Komplexitätsmanagements in den strategischen Führungsprozess der Logistik," Haupt, 2007.

[16] J. Holt and S. Perry, "SysML for Systems Engineering. A Model-Based Approach," IET Professional Applications of Computing. 2nd Edition. Stevenage, UK: IET, 2014.

[17] A. Cockburn, "Writing Effective Use Cases," Addison Wesley, 2000.

[18] GlobalPlatform Card Technology, Security Upgrade for Card Content Management, Card Specification v2.3 – Amendment E Version 1.0.1.3, 2015.

[19] M. Mamrot, S. Marchlewitz, J.-P. Nicklas, and P. Winzer, "Using Systems Engineering for a Requirement-Based Design Support for Autonomous Robots," IEEE International Conference on Systems, Man, and Cybernetics, October 5-8, 2014, San Diego, CA, USA, pp. 3146-3151.

[20] R. Stevens, P. Brook, K. Jackson, and S. Arnold, "Systems Engineering: Coping with Complexity," Hemel Hempstead: Prentice Hall, 1998.

[21] S. Marchlewitz; J.-P. Nicklas, and P. Winzer, "Using Systems Engineering for Improving Autonomous Robot Performances," IEEE 10th International Conference on System of Systems Engineering, San Antonio, TX, USA, 17.-20. 5.2015, pp. 65-70.

[22] P. Winzer, "Generic System Description and Problem Solving in Systems Engineering," Accepted article for inclusion in a future journal issue. IEEE Systems Journal, 2015.

[23] J.-P Nicklas and P. Winzer, "Approach for Using Requirements Engineering in Collaborative Networks," in S.M. Dahlgaard-Park, J.J. Dahlgaard, (eds.), Entering the Experience Economy from product quality to experience quality, Proceedings of the 17th QMOD-ICQSS International Conference on Quality and Service Sciences, ICQSS 2014.

[24] M. Mamrot and P. Winzer, "Approach for Structuring the Product Environment for a Systematic Analysis of Field Data," IEEE 8th International Conference on System of Systems Engineering (SoSE). Maui, Hawaii, USA 2013, pp. 1-6.

[25] E. R. Ashby, "An introduction to cybernetics," 2. impr. – London, Chapman & Hall, 1957.

[26] S. Friedenthal, A. Moore, P. Steiner, "A Practical Guide to SysML. The Systems Modeling Language," 3. Ed. Waltham, MA: Elsevier, 2015.

[27] ISO 12100:2011-3, Safety of machinery - General principles for design - Risk assessment and risk reduction.

[28] SysML V1.4 Specification Release September, 2015.

[29] B. Schneier, "Attack Trees," Dr. Dobbs Journal, vol. 24, no. 12, pp. 21–29, 1999.

[30] O. Alt, "Modellbasierte Systementwicklung mit SysML", München: Carl Hanser Verlag, 2012