POTENTIALS FOR THE INTEGRATION OF DESIGN THINKING ALONG AUTOMOTIVE SYSTEMS ENGINEERING FOCUSING SECURITY AND SAFETY

Tekaat, Julian; Kharatyan, Aschot; Anacker, Harald; Dumitrescu, Roman

Fraunhofer Research Institute for Mechatronic Systems Design IEM

ABSTRACT

The increasingly intelligent, highly complex, technical systems of tomorrow - for instance autonomous vehicles - result in the necessity for a systematic security- and safety-oriented development process that starts in the early phases of system design. Automotive Systems Engineering (ASE) as one approach is increasingly gaining ground in the automotive industry. However, this approach is still in a prototype stage. The consideration of security and safety within the early stages of systems design leads to so-called ill-defined problems. Such are not covered by ASE, but can be addressed by means of Design Thinking. Therefore we introduce an approach to combine both approaches. Based on this combination, we derive potentials in the context of the consideration of security and safety. Essential advantages are the possibility to think ahead of threat scenarios at an early stage in system design. Due to an incomplete database, this is not supported or only partially supported by conventional approaches. The resulting potentials are derived based upon a practical example.

Keywords: Systems Engineering (SE), New product development, Early design phases, Security & Safety, Design Thinking

Contact:
Tekaat, Julian
Fraunhofer Research Institute for Mechatronic Systems Design IEM
Product Engineering
Germany
julian.tekaat@iem.fraunhofer.de

Cite this article: Tekaat, J., Kharatyan, A., Anacker, H., Dumitrescu, R. (2019) 'Potentials for the Integration of Design Thinking along Automotive Systems Engineering Focusing Security and Safety', in *Proceedings of the 22nd International Conference on Engineering Design (ICED19),* Delft, The Netherlands, 5-8 August 2019. DOI:10.1017/dsi.2019.295

1 POTENTIALS FOR A COMBINATION OF AUTOMOTIVE SYSTEMS ENGINEERING AND DESIGN THINKING

New generations of vehicles are equipped with a variety of communication interfaces and automated driving functions such as distance and lane departure assistants. The resulting advantages go hand in hand with the challenge of protecting on-board electronics of these systems from external attacks (Miller and Valasek, 2015). Studies have demonstrated the vulnerability of vehicles with a steadily increasing degree of connectivity, automation and autonomy (Koscher *et al.*, 2010; Checkoway *et al.*, 2011; Miller and Valasek, 2013). Manufacturers and suppliers face a multitude of challenges such as the development of secure networked and automated vehicles (German Association of the Automotive Industry (VDA), 2015). The question arises how vehicles can be safely developed in context of security and safety. Relevant functions of these systems require a systematic as well as security- and safety-oriented design process, which starts in the early phases of system design (Bakirtzis *et al.*, 2018; Lukei *et al.*, 2016). A conventional approach for the systematic design is Systems Engineering (SE) (Walden *et al.*, 2015). A further development of SE is Automotive Systems Engineering (ASE) which represents a consistent adaptation to existing challenges in the automotive sector (Winner, 2013). ASE still has many fields of action for the design of safe and secure systems. The starting point in early phases of system design is the identification of use cases and requires the systemic consideration of security and safety aspects (Lukei *et al.*, 2016; Bakirtzis *et al.*, 2018). Respectively, formulated use cases have to address complex correlations out of system of systems (Nourian and Madnick, 2018). This leads to so called "ill-defined" problems. In order to overcome challenges of "ill-defined" problems considering system of systems, literature refers to Design Thinking (Tomita *et al.*, 2017). E.g. Plattner *et al.* (2016) say that Design Thinking is particularly suitable for reformulating challenges and for the analysis from different and previously non-obvious perspectives. As with ASE, Design Thinking as well has many fields of action. The aim of this paper is to show potentials for the integration of Design Thinking along ASE as shown in figure 1 – especially considering safety and security in system design. This approach was developed in the context of the Design Research Methodology (DRM) from Blessing and Chakrabarti (2009). It is the question which parts of Design Thinking can be integrated along ASE to address challenges in context of security and safety? The central idea is to address various challenges in the design of safe and secure systems. As experience indicates, the main advantage of the approach referring to the current state of research is the combined and early consideration of safety and security in systems design.

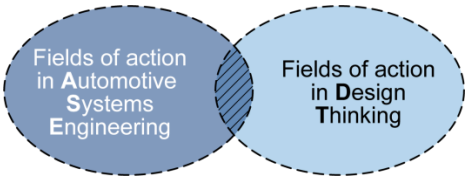

Figure 1. The paper's focus deals with the overlapping fields of action of automotive systems engineering and design thinking

This paper has been divided into five parts. The first part gives an introduction. The second part presents the current state of ASE in combination with the need for action in security- and safety-compliant system design. Section 3 provides an overview of related work. The fourth part introduces the solution approach. This includes the integration of Design Thinking along the ASE process (section 4.1) and an example based consideration of security and safety (section 4.2). Finally, a discussion is given and areas for further research are identified (section 5).

2 PROBLEM ANALYSIS

This section presents the current state of ASE. First, the topic is introduced followed by the need for action in security- and safety-compliant system design.

2.1 Automotive systems engineering (ASE)

In automotive industry there is a need for engineering methodologies that consider requirements holistically throughout the entire product development process, which effectively orchestrate all actors

https://doi.org/10.1017/dsi.2019.295 Published online by Cambridge University Press

and reduces the risk of errors developing during the early stage. SE, which results from avionics development, allows this through a holistic interdisciplinary way of thinking and acting. ASE, which is still in part very prototypical, adapts this success position for the automotive application domain and forms the basis for the successful development of vehicles in the future (Winner, 2013).

The so-called V-model (see figure 2) provides a central orientation for the basic approach of ASE (Maurer and Winner, 2013). The vehicle development process is initiated by the analysis of product requirements. This already comprehensive process step is confronted with further challenges like considering legal norms and standards (e.g. ISO 26262 (2011)) as well as security and safety aspects. While safety promotes the assurance of functional fulfilment (e.g. autonomous avoidance of obstacles) and thus accident prevention, security serves crime prevention and protects the system against external and malicious influences. The main difference is therefore the protection objective. Since safety reduces the risk of malfunctions to an acceptable level, security reduces risk for external attacks in defined interfaces. However, the integrative consideration of both fields of action is essential, since e.g. due to a successful remote takeover of the vehicle (security hazard), essential safety problems can arise (e.g. locking of the steering while driving). Due to the increasing functional performance of vehicles, the degree of networking and the associated high quantity of penetration possibilities, safety and security requirements are becoming increasingly relevant. They therefore need to be forecast and secured as early as possible in the development process.

As shown in figure 2, system design is based on the requirements analysis. On vehicle level, the initial specification of the vehicle is as solution-neutral as possible via a functional description and abstract logical elements. To address the entire product life cycle, application scenarios and use cases are developed. They analyse essential phases and specify the vehicle's required behaviour. Furthermore, in order to ensure safety and security requirements in particular, potential threats and hazards are identified by analysing misuse cases and their consequences. This is followed by the evaluation of threat scenarios and inherent hazards. With regard to security- and safety-oriented requirements as well as other requirements, test cases are developed, which serve as basis for verification and validation.

Following the system specification at vehicle level, the decomposition and detailed specification of assemblies take place. In the same way systems are designed and decomposed down to part level. This top-down methodology ensures the constancy of interfaces between systems, assemblies and parts.

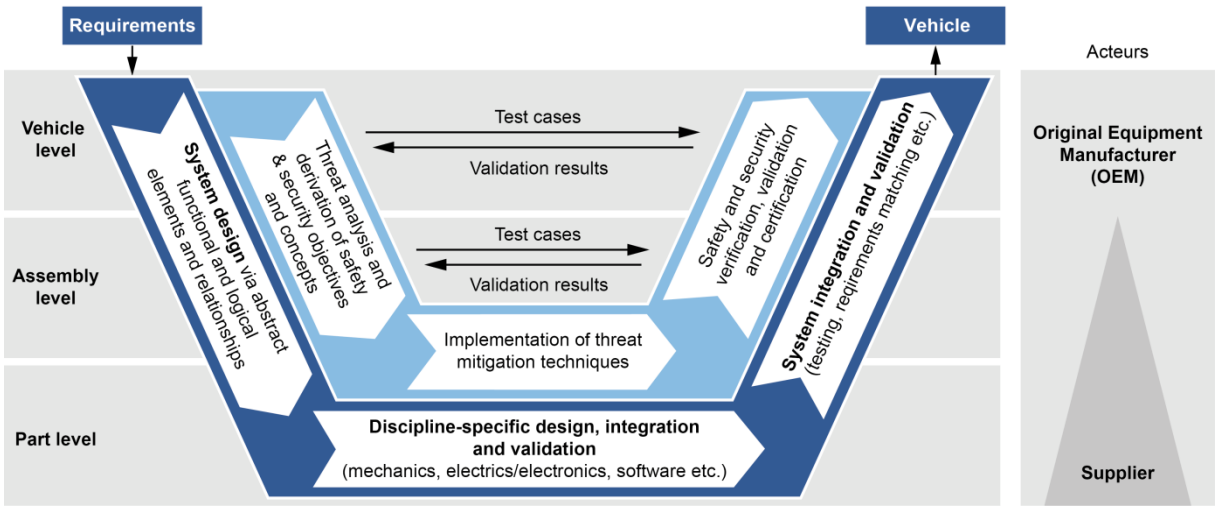

Figure 2. V-model for the security- and safety-focused development of vehicles as a combination of ISO 26262 (2011) and VDI 2206 (2004)

In the discipline-specific design, integration and validation are performed at component level. Among others, mechanical, electrical/electronic and software solutions are developed. The previously developed abstract safety concepts are further refined, implemented and validated at component level via testing. These tests include, e.g. initial penetration tests to simulate the intrusion of malicious attackers and to verify the preservation of protection goals. Subsequently, components are first integrated at assembly level and thereafter at vehicle level. In this process, continuous verification and validation is carried out through tests and comparison of previously specified requirements.

https://doi.org/10.1017/dsi.2019.295 Published online by Cambridge University Press

Since each integration step increases the number of systems and thus both the functions and the degree of networking and the number of interfaces, the potential attack possibilities as well as the probability of functional failures increase. It is therefore essential that comprehensive and target-oriented tests and simulations are carried out in order to validate the properties and behaviours of the integrated assemblies and the entire vehicle. The result of a successful system integration is the final vehicle.

2.2 Need for action in security- and safety-compliant system design

Since safety and security are two seemingly contradictory system features, security and safety are rarely considered in combination. E.g. Macher *et al.* (2015) state that automotive systems require appropriate systematic approaches that will support security-aware safety development. Another current challenge in ASE is the early identification of threat potentials. Instead of a proactive holistic system development, security and safety issues are often only addressed during the late system integration. This results in immense additional efforts due to unnecessary analysis and troubleshooting processes (Strafaci, 2008). An essential driver for the late consideration of security and safety issues are abstract functional and logical system descriptions at the early stages of system development. Fleming and Leveson (2015) propose an approach to integrate systems safety into SE during concept development. The authors' state, that stakeholder and engineers using their approach during the concept formation stage, can not only understand why hazardous behaviour might occur but also derive constraints and requirements that will prevent the hazards. Nevertheless, its application requires discipline specific knowledge, which can only be provided by specialists and only considers safety aspects.

At this early stage not all involved stakeholders and other factors or effects resulting out of threat scenarios are initially clear. Security and safety for systems with increasing degrees of connectivity, automation and autonomy have numerous and extensive variables, and different combinations of the variables will bring out different scenarios. Because of countless possible combinations, the developer is not able to imagine a clear goal for the system. In conventional SE, it is identified as an ill-defined problem. When designing a system that has such problem, it is often the case that a developer gradually grasps the situation, understands the problem and is able to make judgments while he proceeds with the design. In other words, the design must go on while taking into consideration "unknown contexts", as shown in Rumsfeld's Ignorance Management Framework (Israilidis *et al.*, 2013). "Unknown contexts" lead to ill-defined problems, which arise in this context because no early and consistent threat analysis has taken place or because the problem area has not been adequately analysed due to its complexity. To solve such problem Conway *et al.* (2017) say, the application of Design Thinking is an answer. Design Thinking is effective in inducing responses to "unknown contexts". These considerations result in the need for integrating Design Thinking along the early phases of ASE to address ill-defined problems. Literature looking at such combination is shown in the following section.

3 RELATED WORK

This section focusses on the current state to combine Design Thinking and SE to solve ill-defined problems. Related literature shows just a few general attempts to integrate Design Thinking. None of them deals with the consideration of security and safety issues. More often theoretical potentials of a hypothetical combination are derived. Therefore, the combination of Design Thinking and SE by Tomita *et al.* (2017) as well as derived advantages and disadvantages are shown.

Tomita *et al.* (2017) present an approach to handle ill-defined problems in societal systems by using Design Thinking within a structured SE process. They propose using the advantages of Design Thinking and SE to build a *Structured Design Thinking Framework* as an extension to the Data-Information-Knowledge-Wisdom (DIKW) model. The proposed framework complements the hard (SE) and soft (Design Thinking) approaches – which are typical for problem solving – to maximize the benefits of both. To address these targets the SE approach is used to model solutions and the Design Thinking approach addresses them as a whole. The authors are focussing on system of systems targeted at innovation and societal systems, which contain ill-defined problems in many disciplines. By incorporating a developed process containing the steps Issue, Problem Definition, Value Proposition, Ideation and Solution in addition to an activity flow, the framework is structured and designed to generate iterative thinking. Thereby the reproducibility of thinking processes which take place while solving problems using Design Thinking is improved as well as the utility of the output (Tomita *et al.*, 2017).

https://doi.org/10.1017/dsi.2019.295 Published online by Cambridge University Press

Tomita *et al.* (2017) are showing the feasibility and potentials of combining Design Thinking with SE. Nevertheless, the framework is designed to deal with societal systems instead of intelligent technical systems. Further the consideration of security and safety aspects is not part of their research.
Advantages of the combination of Design Thinking and SE are exemplarily shown by Lewrick *et al.* (2018) and Zhao (2015). Zhao (2015) studies the general mutual influence of Design Thinking and systems thinking as basis for SE. He investigates whether and how the approaches' principles and tools can jointly influence the performance of system development. Based on a survey a mixture of these tools is found in almost each system development activity. Advantages of Design Thinking are found in activities like identifying needs, developing solutions, considering alternatives and performing tests. SE has more analytical tools such as failure mode analysis and customer value chain analysis. Based on the high-perceived value of utilizing Design Thinking in SE activities - such as finding needs, discovering requirements and system functions, modelling and integrating systems - Zhao (2015) states that more Design Thinking tools and its principles are encouraged to put into practices. The biggest potentials out of a hybrid model are to incorporate the Design Thinking principle of "empathy" in discovering user/customer needs, requirements and system functions, the principle "creativity" in idealizing solutions as well as "efficiency" in modelling and systems integration (Zhao, 2015). Lewrick *et al.* (2018) add the advantages of clearly understanding a customer's problem and solving precisely this. Nevertheless, organizations have not taken the full advantage of combinative utilization of these principles in system development activities.
As a result there is no clear problem definition, no specific methodology to employ, and no right answer offered as a solution to address ASE, Design Thinking and the development of safe and secure systems in specific. The following approach offers starting points to close these gaps.

4 SOLUTION APPROACH

The following sections gives a short insight into Design Thinking and displays a hypothetical scenario for developing highly autonomous driving functions. Statements made in this section will be made in concrete terms on basis of this example. This is followed by an approach how to assign Design Thinking to the ASE process and partial models contained therein (section 4.1). Conclusive, an example based derivation of potentials to implement redundant system parts to accomplish e.g. safety or security in the automotive industry is shown (section 4.2).
We follow the **Design Thinking** interpretation according to Brenner and Uebernickel (2016): The micro-process contains five phases (cf. figure 4) which are run through iteratively to develop specific and stepwise more detailed prototypes. The first two phases of the micro-process *Empathize* and *Define* describe the problem space, the following three phases *Ideate*, *Prototype* and *Test* the solution space. Problem and solution space are run through accordingly an identical procedure. First of all, a multitude of aspects of the problem or the solution are worked out by divergent thinking. Subsequently, convergent thinking will work out a central result from the identified aspects. Thus a central problem definition results from the problem space, a possible solution from the solution space. The solution displays a possible prototype which is further specified as part of further iterations. This process will be combined with the ASE-process.
A **hypothetical scenario** to do so is illustrated in figure 3 and is described in the following. We are looking at the implementation of highly autonomous driving functions. Therefor systems are required which allow a precise and reliable environment detection. E.g. a camera system is developed to sense the environment and transmit data for further analysis. As is often the case with today's vehicles, the camera system is placed behind the windscreen. Due to its high safety relevance, this camera system respectively its function "detect environment" needs a monitoring to detect mud on the windshield by comparing the picture with another e.g. radar or lidar sensor element or a redundant picture of second camera at a different position on the windshield. This monitoring in software is there by developed with a high ASIL rating. A detection leads to degrade the camera, to activate the wiper or to switch to an alternative sensor (radar/lidar) for the time to handover the vehicle to the driver or to stop the car controlled on a safe place. This results in the hypothetical example that redundant elements must be developed and implemented within the framework of system integration.
In context of an early identification of possible hazards and the consequences for surrounding systems, an alternative position would otherwise have been defined which would not lead to such problematic interrelationships. The following approach shall give advantages for this field of action.

https://doi.org/10.1017/dsi.2019.295 Published online by Cambridge University Press

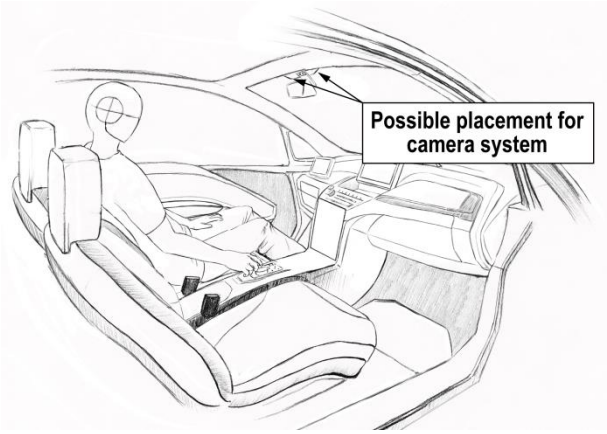

Figure 3. Hypothetical scenario for highly autonomous driving functions

4.1 Integration of design thinking along the ASE process

This section links the Design Thinking process with ASE artifacts. These artifacts have been used in workshops while applying the presented approach. Figure 4 displays a section of the ASE V-model presented in section 2 allocated under the Design Thinking process. The approach only considers the early phase – *system design*. The subsequent phases of *discipline specific design, integration and validation* as well as *system integration and validation* are not part of this approach. But precisely to consider and integrate security and safety, partial models and correlations from the two later phases are integrated in the early phase of *system design*.

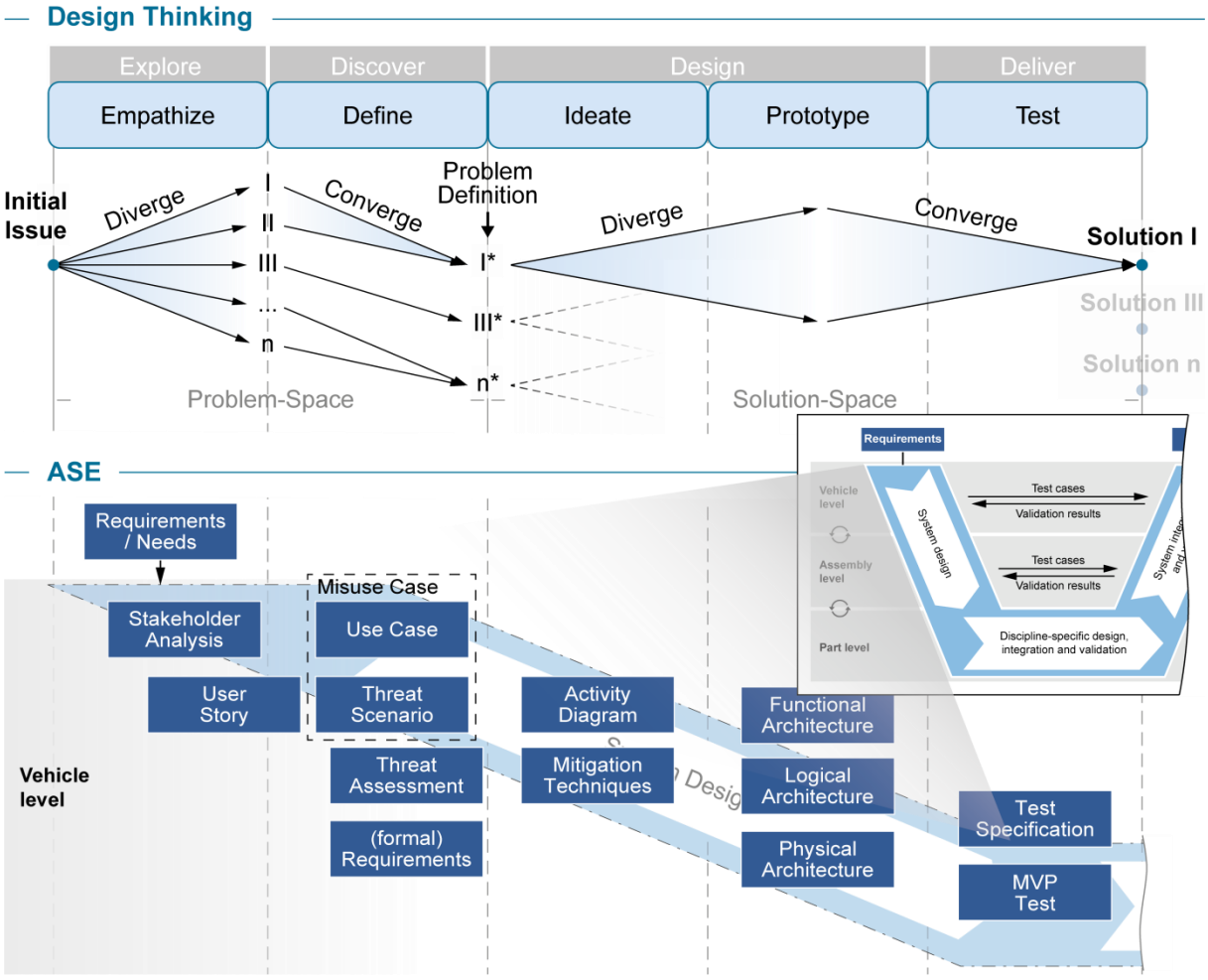

Figure 4. Synergies of the design thinking and automotive systems engineering process for the derivation of safety and security hazards

https://doi.org/10.1017/dsi.2019.295 Published online by Cambridge University Press

The partial models and their viewing order reflect the current status of ASE and are based, among others, on work by Gausemeier *et al.* (2014), Winner (2013) as well as on projects with industrial partners in the automotive industry. Based on the realisation of an autonomous driving function, sequence and meaning of individual partial models are briefly described.
Initially in the ASE process, system's *needs* and *informal requirements* are collected. They reflect the customer's view and demands on a system and thus form the input to obtain a *stakeholder analysis*. The output of the latter is usually a *user story*. This story describes the overall context of the system under consideration from the user's point of view. In case of an autonomous driving scenario e.g. the user's journey to work is described. These aspects help to build a common knowledge about the initial (problem) situation and help to **empathize** in the sense of Design Thinking.
In the following the *user story* is concretized with a multitude of *use cases*. For a secure and safe systems design, we already assign *threat scenarios* to the individual *use cases at this point*. The combination of *use case* and *threat scenario* results in a misuse case. Further, the threat's severity on a *use case* is assessed on basis of a *threat assessment*. The ongoing formulated system's *requirements* lead to *formal requirements*. These partial models assist the **definition** of considered facts.
The following *activity diagram* serves as a further partial model for the representation of correlations – the system's activities are brought into sequence. For the identified misuse cases, *mitigation techniques* are also described in another model. In our example e.g. the redundant design of a camera can be under investigation. The *activity diagram* and *mitigation techniques* help to describe first solution ideas in sense of an **ideation**.
The following partial models serve for further concretization of a **prototype**. They describe the system's *functional*, *logical*, and *physical* correlations.
Finally, based on this knowledge a *test case* specification is defined, which leads to the final partial model, the *test* description and execution of a *minimal viable product* (MVP). These are assigned to the last Design Thinking phase of **testing**. On the partial models' basis, the required knowledge and information for system design can be documented and used for the integration of threat cases in terms of security and safety. Figure 4 already assigns the individual partial models to the Design Thinking phases. Resulting synergies are described in the following subsection.

4.2 Example-based derivation of potentials for the consideration of security and safety

In this section the combined approach of Design Thinking and ASE is described. It summarizes the iterative proceeding, the holistic view of relationships and the formal documentation using phases and partial models of both approaches. Figure 5 illustrates individual aspects and partial models from workshops obtained while applying the approach. The model-based illustration was chosen for a clearer and simpler presentation of the original sketchy workshop results.
We started with the problem area. The first phase *Empathize* serves the initial understanding and thus the gaining of insights (I - n) into a singular challenge. For example the design of safe and secure highly autonomous driving functions. As we go through this phase, a multitude of divergent aspects are identified which have to be taken into account. For this purpose, tools are used to identify needs and to consider alternatives. The documentation of such is carried out in the partial models *informal requirements*, *needs*, *stakeholder analysis* and *user story* assigned to the phase.
The developed aspects are be further concretized in the second phase of the problem area *Define* in order to make a selection for further consideration. In the classic Design Thinking approach, insights from the first phase are used to reformulate the initial issue. In context of this approaches' systematic security and safety design, however, this convergence by means of identified insights only takes place to a certain extent. Much more results are used for the analysis and evaluation of threat potentials. First, further information is recorded by means of *use cases* and the description of *threat scenarios*. Consistent insights are then summarized into influencing factors.
In the given example, the functionality of an autonomous vehicle is partially made available by a camera behind the windscreen. The function "detect environment" is described within a *use case*, to concretize the *user story* of an autonomous trip to the user's workplace. As one impact, bad weather conditions and dirty roads are analysed. This leads to the description of a *threat scenario*, which will help to identify the threat of contamination. This trivial procedure allows a much earlier identification than using the conventional approach during the system integration. In practice, there are many of such cases which could be prevented by simply describing detailed framework conditions and

https://doi.org/10.1017/dsi.2019.295 Published online by Cambridge University Press

appropriate investigation. The derivation of or exemplary threat by deriving requirements from the *use case's* functions is displayed in figure 5. The late and thereby costly development and implementation of redundant components can be avoided.

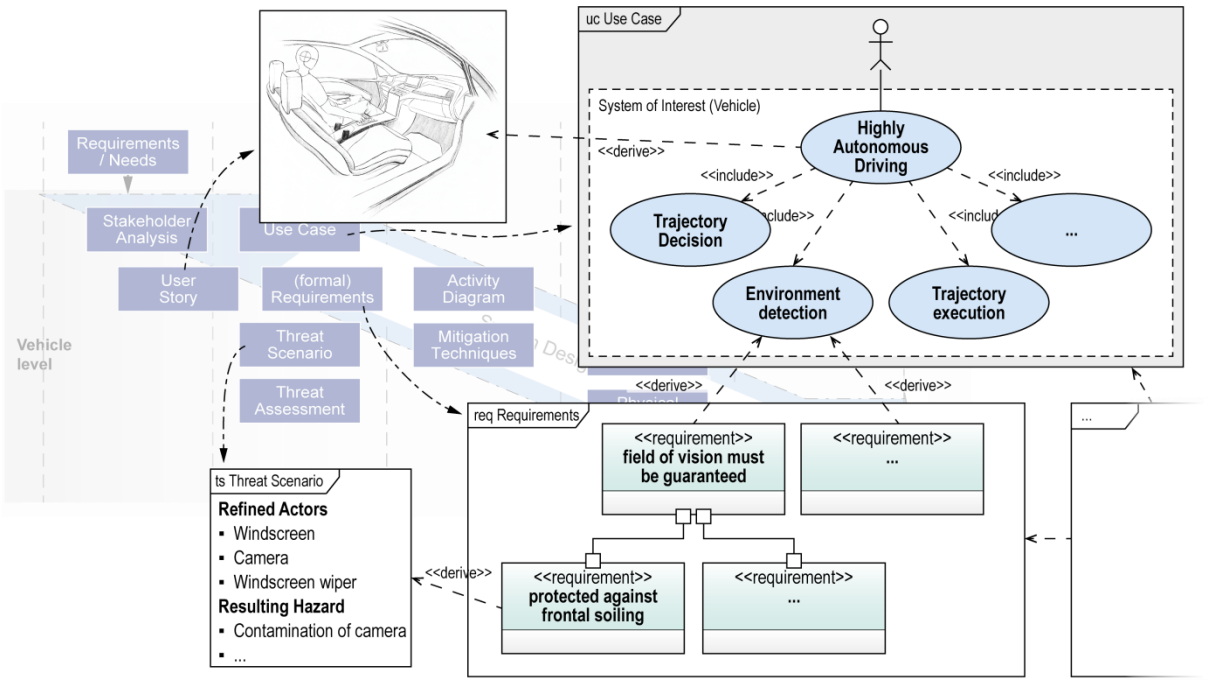

Figure 5. Exemplary illustration of the derivation of threat scenarios out of use cases and requirements within the early stages of systems design

The threat described in detail served only as an example. In the following steps, an evaluation of all resulting threats according to classic security and safety analysis procedures (see e.g. ISO 26262 or ISO 21434) is carried out. In this way, the individual threats can be classified according to their relevance. The arising influencing factors (I* - n*) represent the problem area's result. It contains an evaluated collection of newly identified and consolidated *threat scenarios* for system design.

Within the solution space the system will be concretized further. Each identified scenario is considered separately. Thereby influences and dependencies between respective scenarios must be taken into account in terms of ASE (cf. Section 2). Accordingly, the explanations only describe the consideration of the single exemplary scenario. In *Ideate*, the solution space for individual threat scenarios is spanned. For this purpose, the *activities* of the mentioned scenario - contamination of camera - and initial ideas for *mitigation techniques* are documented. One possible solution could be the replacement of the camera system to avoid a redundant design of system parts. But also the use of alternative technologies or solutions for environmental awareness were considered. For example, concepts for the use of infrastructure were included. Based on this information, assigned partial models of the *logical, functional* and *physical architecture* are used in the *Prototype* phase for the further elaboration and specification of the system in context of a threat scenario. Up to this point, the knowledge about a potential system and associated threats will again diverge. In the final phase of *Test*, the MVP resulting from the created models is tested converging with regard to security and safety. The developed results then serve as input for a new iteration loop, starting with the problem area.

The sequential run of the individual phases described, corresponds to an ideal type of process. In practical use of system development, a variety of additional information for already completed partial models results, which are recursively supplemented and the resulting correlations are analysed as well. Further, there will also occur design decisions and threats based on security and safety at a later point in time than shown here. These will lead to addition iterative adaptions of partial models, until the *discipline specific design, integration and validation* as well as the *system integration and validation* can be processed. This adoption is optimally supported by the application of the Design Thinking procedure.

https://doi.org/10.1017/dsi.2019.295 Published online by Cambridge University Press

5 CONCLUSION & DISCUSSION

New generations of vehicles require an efficient and systematic developed in context of security and safety. In particular, existing ill-defined problems due to the changing focus from the pure system to the consideration of influencing factors and relationships in a system of systems as well as additional factors such as the integration of security and safety result in this need for action. This is where manufacturers and suppliers face the challenge to develop secure networked and autonomous vehicles and to test their vulnerability in context of security and safety.

A new approach to meeting these challenges is ASE, which still has prototype status due to its novelty. ASE adapts the success position of SE for the automotive application domain and forms the basis for the successful development of vehicles and inherent subsystems in future. Key features are the holistic consideration of requirements throughout the entire product development process as well as the effective orchestration of all actors and thereby, among other things, reduce the risk of development errors at an early stage. Nevertheless, the early consideration of security and safety faces the challenge of unknown influencing factors and thus a non-existent database for a systematic security- and safety-oriented development process that starts in the early phases of system development.

To cope with this discrepancy we propose an approach integrating Design Thinking along ASE focusing security and safety. The aim of our approach was to identify potentials by means of deriving early required partial models in the design process. One major advantage was the combined consideration of security and safety aspects. This and other aspects enabled the integration of various disciplines and also non-expert stakeholders. The approach provides a starting point for the discussion of potential threats on the basis of e.g. the user story and integrated use cases. All in all, the approach of integrating Design Thinking along ASE allows an appropriate consideration of the elusive and complex topic of systematic design in the context of security and safety. Context difficult to imagine in a system or system of system context is developed successively and iteratively. This leads to a more targeted analysis of threat scenarios as well as their discovery.

Further action is needed in the consideration of later phases in product development in context security and safety. The results presented are based on an initial development and thus reflect the very early phases of a system design. In order to identify necessary adjustments to the approach for later stage in development, the following V-model phases must be considered more concretely. In addition, there is a need for further action in the provision of necessary documentation options for new or adapted partial models. Further concretization and definition of individual partial models in this context can ensure better consistency, completeness and traceability of the results.

REFERENCES

Bakirtzis, G., Simon, B.J., Fleming, C.H. and Elks, C.R. (2018), *Looking for a Black Cat in a Dark Room: Security Visualization for Cyber-Physical System Design and Analysis*, available at: http://arxiv.org/pdf/1808.08081v2.

Blessing, L.T.M. and Chakrabarti, A. (2009), *DRM, a design research methodology*, Springer, London.

Brenner, W. and Uebernickel, F. (Eds.) (2016), *Design Thinking for Innovation: Research and Practice*, 1st ed. 2016, Springer International Publishing, Cham.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T. and others (2011), "Comprehensive experimental analyses of automotive attack surfaces".

Conway, R., Masters, J. and Thorold, J. (2017), "From Design Thinking to Systems Change", *Royal Society of Arts* (London, UK).

Gausemeier, J., Rammig, F.J. and Schäfer, W. (Eds.) (2014), *Design Methodology for Intelligent Technical Systems: Develop Intelligent Technical Systems of the Future, Lecture Notes in Mechanical Engineering*, Springer Berlin Heidelberg, Berlin, Heidelberg.

German Association of the Automotive Industry (VDA) (2015), *Automation: From Driver Assistance Systems to Automated Driving*, Magazine - Automation, Berlin.

ISO 26262 (2011), *Road vehicles: Functional safety, ICS 01.040.43; 43.040.10 No*. International Organization for Standardization.

Israilidis, J., Lock, R. and Cooke, L. (2013), "Ignorance Management", *Management Dynamics in the Knowledge Economy*, Vol. 1 No. 1, pp. 71–85.

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. and Savage, S. (2010), "Experimental Security Analysis of a Modern Automobile", in *IEEE Symposium on Security and Privacy (SP)*, 2010: 16 - 19 May 2010, Berkeley/Oakland, California, Oakland, CA, USA, 5/16/2010 - 5/19/2010, IEEE, Piscataway, NJ, pp. 447–462.

https://doi.org/10.1017/dsi.2019.295 Published online by Cambridge University Press

Lewrick, M., Patrick, L. and Leifer, L. (2018), *The Design Thinking Playbook: Mindful Digital Transformation of Teams, Products, Services, Businesses and Ecosystems*, John Wiley and Sons, Hoboken, New Jersey.
Lukei, M., Hassan, B., Dumitrescu, R., Sigges, T. and Derksen, V. (2016), "Requirement analysis of inspection equipment for integrative mechatronic product and production system development: Model-based systems engineering approach", in *10th Annual International Systems Conference proceedings*, April 18-21, 2016, Hyatt Regency Grand Cypress, Orlando, Florida, USA, Orlando, FL, USA, 4/18/2016 - 4/21/2016, IEEE, Piscataway, NJ, pp. 1–7.
Macher, G., Sporer, H., Berlach, R., Armengaud, E. and Kreiner, C. (2015), "SAHARA: A security-aware hazard and risk analysis method".
Maurer, M. and Winner, H. (2013), *Automotive Systems Engineering*, Springer Berlin Heidelberg, Berlin, Heidelberg.
Miller, C. and Valasek, C. (2013), "Adventures in automotive networks and control units", *Def Con*, Vol. 21, pp. 260–264.
Miller, C. and Valasek, C. (2015), "Remote Exploitation of an Unaltered Passenger Vehicle", available at: http://www.ioactive.com/labs/resources-white-papers.html5 (accessed 7 March 2019).
Nourian, A. and Madnick, S. (2018), "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet", *IEEE Transactions on Dependable and Secure Computing*, Vol. 15 No. 1, pp. 2–13.
Plattner, H., Meinel, C. and Leifer, L. (Eds.) (2016), *Design thinking research: Making design thinking foundational, Understanding innovation*, Springer, Cham, Heidelberg, New York, Dordrecht, London.
Strafaci, A. (2008), "What does BIM mean for civil engineers", *CE News, Tranportation*, No. 127.
Tomita, Y., Watanabe, K., Shirasaka, S. and Maeno, T. (2017), "Applying design thinking in systems engineering process as an extended version of DIKW model".
VDI 2206 (2004), *Design methodology for mechatronic systems*,Vol. 03.100.40; 31.220, Beuth Verlag, Düsseldorf.
Walden, D.D., Roedler, G.J., Forsberg, K., Hamelin, R.D. and Shortell, T. M. (Eds.) (2015), *Systems engineering handbook: A guide for system life cycle processes and activities ; INCOSE-TP-2003-002-04*, 2015, 4. edition, Wiley, Hoboken, NJ.
Winner, H. (2013), "Challenges of automotive systems engineering for industry and academia", in *Automotive Systems Engineering*, Springer, pp. 3–15.
Zhao, Y.-Y. (2015), "Towards innovative system development: A joint method of design thinking and systems thinking".

https://doi.org/10.1017/dsi.2019.295 Published online by Cambridge University Press