Hybridization of safety and security for the design and validation of autonomous vehicles: where are we?

Martin Boyer

IRT SystemX, Palaiseau, France. E-mail: martin.boyer@irt-systemx.fr

Théo Chelim

IRT SystemX, Palaiseau, France. E-mail: theo.chelim@irt-systemx.fr

Jeremy Sobieraj

IRT SystemX, Palaiseau, France. E-mail: jeremy.sobieraj@irt-systemx.fr

More and more ground transports are being used (vehicles, trucks, buses, taxis...) and they remain one of the most dangerous means of transport in the world. However, vehicles are increasingly connected and autonomous with the aim of making travel safer, cleaner and more efficient. They are now able to share and communicate information between themselves and their environment in real time, helping to reduce accidents, traffic congestion and greenhouse gas emissions. These vehicles are Cyber-Physical Systems (CPS), i.e. systems made up of mechanisms that capable of controlling physical entities. In order to guarantee the robustness of such systems, they must meet two main criteria: safety and security. However, safety and security are currently dealt with independently. The reasons for this are both historical and normative. One idea is therefore to combine these two criteria in order to obtain the most robust vehicle possible. In this article, we propose to highlight recent advances in the combined study of safety and security, focused on the autonomous vehicle. To do this, we have carried out a preliminary analysis of the existing situation and a cartographic study listing the articles dealing with this combination. Various qualitative and quantitative analyses of the existing situation are present in the literature, generally focused on CPS. Then, based on this study, we grouped the articles according to two categories: those highlighting the interests and possibilities of such a combination and those presenting hybrid methods in detail.

Keywords: Autonomous vehicles, Safety, Security, Cyber-Physical Systems, Validation, ITS.

1. Introduction

1.1. *Safety*

Safety concerns accidental and unintentional events. In the case of the autonomous vehicle, we can cite the failures related to the infrastructure (weather or road conditions...) and to the components (sensor or actuator failure, failure of the communication system ...). Thus, in the automotive field, the role of the ISO 26262 *Road vehicles - Functional Safety* standard (The International Organization for Standardization (2011)), based on the IEC 61508 standard (IEC (2005)), has the role of defining the requirements and providing the correct operational safety practices throughout the vehicle cycle.

1.2. *Security*

Security concerns intentional events like malicious attacks. In the case of the autonomous vehicle, through its connections with its environment, we speak of cybersecurity because the attacker has several entry points to try to access the various contents and equipment of the vehicle. Thus, this type of vehicle must meet the following security criteria:

- Authenticity: make sure the data comes from the original source;
- Availability: ensure that the data exchanged or services are available at all times;
- Integrity: ensure that the data or services have not been tampered;
- Confidentiality: ensure that unauthorized users do not access the data.

In the automotive field, the role of the SAE J3061 *Cybersecurity guidebook for cyber-physical vehicle systems* standard (SAE International (2016)) is to define the requirements and best practices in the field of security. The ISO 21434 *Road vehicles - Cybersecurity engineering* standard (The International Organization for Standardization (2016)), currently under approval, uses the principles of SAE J3061 to provide more complete documentation.

Proceedings of the 31th European Safety and Reliability Conference.
Edited by Bruno Castanier, Marko Cepin, David Bigaud and Christophe Berenguer
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0_output

1.3. *Discussions*

The study of safety and security was done independently. This is particularly due to the history of these two concepts. In fact, safety in systems has quickly become essential in many fields (aeronautics, aerospace, automotive, nuclear. . .).

As for security, it is a term whose objective has evolved very quickly over time with the evolution of robotics and then with the generalization of digital, where the concept of cybersecurity appeared. Today, if the aeronautics and automotive sectors have designed safe systems, the notion of security is not as solid. Computer attacks are more and more present in companies. In addition, the use of electronics and external connections in the automotive world increases the possibilities of attacking vehicles. Among these attacks, the Jeep attack by researchers Chris Valasek and Charlie Miller led the Chrysler company to recall nearly 1,500,000 vehicles. This attack has become a symbol of the need to take cybersecurity into account in systems.

The idea of offering a system that is both safe and secure appears naturally. The implementation of this idea quickly encountered some difficulties as the approaches of the two communities are different. Moreover, the authors of Huber et al. (2018) proposed an exploratory survey of automotive experts showing that the vast majority study these aspects independently. Thus, we carried out a cartographic study in order to highlight several hybrid security and safety approaches, focused in the design and validation of the autonomous vehicle.

2. Mapping study : methodology

The study of systems combining safety and security is becoming more and more numerous, particularly in the context of Cyber-Physical Systems. Thus, it is necessary to group together the relevant articles for our study. As we said previously, we have chosen to focus on the field of autonomous vehicles. However, the objective of this part is also to highlight articles proposing a mapping, focused on hybrid security / safety approaches in larger areas.

Eight articles of this type were selected and each offer several articles classified according to different categories : Pietre-Cambacedes and Bouissou (2013); Kriaa et al. (2015); Chockalingam et al. (2017); Abulamddi (2016); Lisova et al. (2019); Lyu et al. (2019); Mashkoor et al. (2020); Kavallieratos et al. (2020). Kavallieratos et al. (2020), takes six of the remaining seven articles to put in place the most complete and detailed classification to date. Thus, from these articles and our research (until April 2020), we retained about 40 articles related to the field of autonomous vehicles. These articles were studied in detail in order to determine the methods and tools proposed and to analyze them, and to discuss on the advances around the security / safety hybridization for the autonomous vehicles. The articles were divided into three categories:

- Highlighting the interests and possibilities of hybridization and proposals for improving standards;
- Methods for security / safety design and analysis;
- Security risk assessment taking into account the Safety assessment. These methods will not be detailed in this article (Islam et al. (2016); Monteuuis et al. (2018); Sabaliauskaite et al. (2018)).

3. Interests and possibilities

Several articles highlight the interest of combining safety and security. The study of this combination is far from recent. Indeed, Simpson et al. (1998) seems to be one of the first articles to discuss the interest of combining the two aspects. However, the concept of security mentioned remains quite distant from that approached for autonomous vehicles (cybersecurity). In the context of cybersecurity, we find this notion essentially from 2010. In Sangchoolie et al. (2018), the authors have set up various attacks which have an influence on the safety of the vehicle by violating the initial requirements. In addition, they highlight the fact that security countermeasures can have a negative impact on safety countermeasures and vice versa.

One of the recurring criticisms comes from the lack of concepts and recommendations on security / safety coordination, particularly in the automotive field Robinson-Mallett et al. (2015). Schoitsch et al. (2016) insists on the need to consider the two aspects together in design, where the requirements can be contradictory. Burton et al. (2012) highlights the lack of concept of ”intentional fault” in the ISO 26262 standard. Schmittner and Ma (2015) offers a framework to meet the ISO 26262 and ISO 15408 standards, thus moving towards a more cooperative approach. It is necessary to specify that since, ISO 26262 has been revised (2018) and evokes the concept of safety and its potential combination with security. There is still no proposed framework for combining the two approaches. Since that date, the V-cycle has been analyzed in order to seek the synergies of these two approaches, in compliance with the automotive standards ISO 26262 and ISO 21434. The dependencies are more numerous in the right part of the cycle, rather concerning the verification and validation aspects Skoglund et al. (2018).

Several applications in the automotive field, respecting the combination, have been proposed.

In Larson et al. (2013), the authors propose a security / safety classification of the ECUs of a vehicle. Sojka et al. (2014) tested and validated an AUTOSAR module prototype. The attacks did not then have any major consequences on the module but they highlight not to study these requirements independently. Popov (2015) offers a combined security / safety analysis on an ASIL D certified device. From a stochastic modeling, we can return a risk probability of cyber attacks. The authors of Amorim et al. (2017) proposed a risk reduction measure, based on a case study on an ASIL C certified component. Finally, in Wei et al. (2016), the authors started from the HAZOP safety risk analysis method to include security notions. From a case study, they defined a set of additional keywords to perform an exhaustive analysis, making it possible to locate potential security vulnerabilities.

All of these articles show that beyond the interest of combining security and safety, it becomes necessary to do so and initial approaches have been proposed based on several case studies. We will now analyze in detail 10 methods allowing this hybrid study under different aspects (design, analysis, evaluation).

4. Methods for security / safety design and analysis

4.1. *Steiner and Liggesmeyer method*

In Steiner and Liggesmeyer (2013), the authors propose to complete the safety analysis by adding security aspects in order to obtain a system more robust to attacks. For this, they use Component Fault Trees (CFTs), extension of Fault Trees, taking into account in addition the system components and their reuse.

First, for each component of a system, we model a CFT. Then, the CFTs are extended to take into account the concept of safety. For this, the STRIDE security method is used to list the possible threats. If an event potentially linked by an attack is found, we extend the CFT by adding an OR gate to which we attach the safety event. We thus obtain a CFT containing security and safety events.

The next step is the qualitative safety analysis. For this, we will determine the Minimal Cut Set (MCS) of the CFT. MCS are then classified into three categories: single security events, single security events and mixed events.

A quantitative safety analysis can also be carried out if the qualitative analysis is insufficient. First of all, we assign a probability (P) to each initial event. Not having sufficient data for the security events, a rating (R) is assigned in this case. For each category presented previously, we will determine an order of importance of the MCS, based on the probabilities and ratings.

4.2. *Extension of CARDION method*

In Ito (2014), the author proposes an extension of his own method called CARDION Ito and Kishida (2014), which initially aims to perform risk analysis, adapted to the automotive world. In this extension, a consideration of threats has been added. The method was illustrated on a case study of ACC (Adaptive Cruise Control). Just like CARDION, its extension includes the same four stages in which the notion of security is inserted :

- Propose a sketch of the system: the objective is to schematically describe the static and dynamic aspects using respectively UML class and state-transition diagrams for example. This thus makes it possible to facilitate the search for dangers / threats but also to have a certain exhaustiveness for the validation of the system;
- Decomposition of objectives: application of the KAOS method (presented in more detail in the part 4.6);
- Application of guide words for each objective: use of guide words related to the notation of time and space, from the HAZOP method (Griffiths (1984));
- Search for dangers and threats: from the previous steps, we deduce a set of dangers and threats by looking for potential failures or vulnerabilities.

4.3. *SysML-sec*

In the European project EVITA (Henniger et al. (2009)), a modeling environment for both safe and secure systems has been proposed. Called SysML-Sec, it is an extension of the SysML modeling language (Mann (2009)), usable via the *toolkit* TTool (Pedroza et al. (2011)). It covers all stages of the vehicle's life cycle.

The articles Apvrille and Roudier (2014), Apvrille and Roudier (2015) and Roudier and Apvrille (2015) present the SysML-sec method, which includes the following steps:

- Definition of requirements: use of security-related criteria (confidentiality, integrity, authenticity...);
- Implementation of attack graphs: these are more enriched versions than attack trees;
- Implementation of the hardware architecture: definition of the architecture and functions of the system as well as their communication links;
- Implementation of the software architecture: definition of components from block diagrams and state machine;

- Prototyping of software components: possibility to generate executable code for experimentation.

4.4. *FMVEA*

While FMEA is widely used for safety risk analysis, Schmittner et al. (2014) and Schmittner et al. (2014) propose the FMVEA method (*Failure Mode, Vulnerabilities and Effect Analysis*), using the initial method, with a new notion of vulnerability. It thus aims to define the potential dangers and threats of the system.

The analysis flowchart has been revised to add the concept of security. For each component, anomalies and their effects on the system are identified in parallel for each point of view (safety and security). This information is then grouped together to deduce the severity of the final effect as well as the potential causes, vulnerabilities and attackers. Finally, the frequency or probability of occurrence of these anomalies is determined.

The cause-effect chain has also been enriched with the concept of security. The notion of attacker and vulnerability was then added to define the causes from a safety point of view, which could have consequences on the final effect in the component.

Moreover, Schmittner et al. (2015) proposed a comparison between FMVEA and CHASSIS (also a method for defining requirements), through an automotive case study. This comparison raised limitations for each of the two methods. Indeed, the CHASSIS method treats the two aspects of safety and security but in an independent way. The FMVEA method requires a very good knowledge of threats and vulnerabilities on components to be applied properly.

4.5. *SAHARA*

SAHARA (*Security-Aware Hazard Analysis and Risk Assessment*) (Macher et al. (2015)) is a risk and threat analysis method. The objective is to combine the main methods from the automotive world, namely HARA for safety and STRIDE for security. This thus makes it possible to review the autonomous vehicle design methodology to take into account both approaches at the same time.

All the threats obtained via STRIDE are classified using a security level $SecL$ (ranging from 0 to 4), calculated from : the necessary ressources (R), the knowledge level (K) and the threat level (T). We then retain all the threats whose criticality level (T) is greater than or equal to three and we deduce its security level $SecL$. Then, on the basis of these results and the list of risks obtained via the HARA method (with an ASIL level), the safety elements with security impact are retained.

To illustrate this method, a case study on the automotive system BMS (*Battery Management System*). Compared to a simple application of HARA, SAHARA identified 34% more dangerous cases.

4.6. *KAOS*

In Ponsard et al. (2016), the authors decide to contribute in the *Requirements Engineering* (RE) development stage, to define and manage the requirements from a safety and security point of view. For this, they propose to use an approach *Goal-Oriented Requirements Engineering* (GORE). The choice of the method called KAOS (*Keep All Objective Satisfied*) was then chosen because it presents good documentation on both security and safety aspects. This method was then used in an automotive case study.

In KAOS, it is possible to define objectives under several levels of abstraction. Thus, it is possible to refine high level objectives so that they become operational objectives. KAOS consists of four main models:

- The goal model (Why ? How ?): tree of objectives where we define the goals of the system and the potential conflicts between these goals;
- The object model (On what ?): allows to highlight the links between the elements involved in the defined objectives;
- The agent model (Who ?): definition of the agents of the system and their characteristics;
- The operational model (What to do ? When ?): defines the link between the objectives and the agents to meet the requirements.

The authors then proposed an extension of the *Objectiver* tool (Respect-IT (2007)), using the KAOS method, in order to define security / safety objectives and conflicts.

4.7. *Extension of STPA method*

STPA (*System-Theoretic Process Analysis*) is a safety-oriented risk analysis method. An extension called STPA-sec Young and Leveson (2013) has been proposed to take into account security concepts. In Schmittner et al. (2016), the authors highlight the limitations of this method and solutions for improvement.

The STPA-sec method is based on the STAMP theory (*Systems-Theoretic Accident Model and Processes*) where it is considered that accidents are related to a lack of control rather than a failure of the system.

The method consists of four steps :

- Definition of the purpose of the analysis: definition of system limits and identification of losses, dangers and security constraints;

- Modeling of the control structure: it contains the controller and the controlled processes, as well as the actors, sensors and control actions;
- Identification of dangerous control actions: they can be identified in four different ways (not given, incorrectly given, bad timing or order, stopped too early or stayed too late);
- Identification of loss scenarios: determination of security and / or safety causes that led to a dangerous control action.

The authors put forward two limitations of this method. First of all, the advice in the first step, for identifying loss scenarios, is difficult to apply. In addition, there is a lack of consideration of security, in particular undesirable elements external to the control model which are not included in the model.

In an extension of STPA-sec, called STPA-SafeSec (Friedberg et al. (2017)), two main areas of improvement are proposed:

- The implementation of a terminology for safety and security aspects by using the terms used in STPA and STPA-sec, in order to avoid any ambiguity;
- Tips for designing attack scenarios that can influence control actions, allowing for a more complete analysis.

4.8. *SGM*

In Dürrwang et al. (2017), the authors propose the SGM method (*Security Guide-word Method*), which aims to provide safety concepts on the risk analysis method proposed in ISO 26262. The method contributes in two of the risk analysis steps.

After the identification of dangerous situations of the system, one proceeds to the integration of security using a set of information (threat and fault identifiers, guide words, function and system concerned...).

After the classification of dangers, we proceed in the same way with the threats. For each fault, we associate all the possible dangers. Then, the fault is evaluated from the danger with the highest ASIL. This allows for a worst case scenario, in the event that the attacker leads to the most critical situation. From this analysis, we can deduce the necessary security requirements.

To highlight the interest of the SGM method, the authors proposed to evaluate it on the basis of 30 full-time employees, distributed as follows:

- Safety experts from the automotive world (14);
- Security experts from the automotive world (9);
- University doctoral students (7).

Based on precision, productivity, sensitivity and efficiency criteria, the study shows that security experts using SGM have better results than safety experts. In addition, we also notice that university doctoral students using SGM obtain better results than safety experts.

4.9. *Six-Step Model*

In Sabaliauskaite et al. (2017), the authors present the Six-Step-Model method (SSM). It allows the maintenance and integration of consistency between processes and aspects of safety and security on an autonomous vehicle. It is made up of six stages. Each element of a step is associated with an element of another step in order to establish a link with different levels of importance. The steps are as follows :

- Functions: definition of function and sub-functions from an objective function;
- Structures: definition of the structure of the system in the form of subsystems and units;
- Failures: definition of the various system failures;
- Attacks: definition of the different attacks possible on the system;
- Safety countermeasures: definition of safety countermeasures;
- Security countermeasures: definition of security countermeasures.

Thus, for a given function, it is possible to associate it with subsystems (or units), with a set of failures, attacks, security and safety countermeasures. The relationships between each of these stages can also be nuanced. For example, we can define whether there is a dependence or antagonism between a security countermeasure and a safety countermeasure.

In Sabaliauskaite and Adepu (2017) and Sabaliauskaite et al. (2018), the authors have also proposed applications of this model on a high-level autonomous vehicle in compliance with the requirements of ISO 26262 (safety), SAE J3061 (security) and SAE J3016 (autonomy levels). A more advanced, recent and complete version is presented in Cui et al. (2019) (in this article, the SSM method is called S&S). In Sabaliauskaite et al. (2019), the authors propose to combine this method with CESAM (*CESAMES Systems Architecting Method*).

4.10. *AVES framework*

In Sabaliauskaite et al. (2019), the authors propose the AVES framework, making it possible to cover the entire life cycle of an autonomous vehicle, while respecting safety and security

- Steps 1 to 3 correspond to the design of the vehicle (implementation of its architecture);
- Steps 4 to 6 correspond to its development to reach a prototype;

- Steps 7 to 11 correspond to the implementation to the final product (production, operation, service and decommissioning).

At the end of the implementation of the prototype, a system is obtained with an acceptable level of risk. An SCSD (*Safety and Cybersecurity Deployment*) model is designed to facilitate the analysis of this system from a safety and security point of view. This model is made up of four matrices linked together by a common characteristic. Each of these matrices are designed at key stages of AVES and have the following objectives :

- Matrix 1 - Requirements conflicts (steps 2 and 5 of AVES): each requirement is compared with the other defined requirements. We determine if there is a conflict between two requirements. In addition, for each of the requirements, the level of risk and the number of conflicts are determined. This makes it possible to determine which ones will be chosen for the implementation, namely those containing no or few conflicts (with an acceptable number of conflicts and an acceptable level of risk);
- Matrix 2 - Coverage of needs (steps 3 and 6 of AVES): for each couple (requirement, measure), we define a level of satisfaction of the measure on the requirement (low, medium or high). For each requirement, we take its level of risk, to which we add an element determining whether the requirement is considered to be sufficiently satisfied. For each measure, we determine its type (if its goal is related to prevention, detection or correction), its cost, its coverage (its effectiveness against the requirements) and if it is selected for implementation;
- Matrix 3 - Relationship between measures (steps 3 and 6 of AVES): for each pair of measures, it is determined whether they complement each other or if they are in conflict. Thus, for each measure, we determine its level of conflict, complementarity, priority for implementation and whether this measure is considered acceptable;
- Matrix 4 - Implementation of measures (steps 3 and 6 of AVES): a measure is associated with one or more components necessary for its implementation. For each component, its constraints and limitations are determined. For each measure, additional information is given such as the other means to implement this measure, the implementation priority, a percentage of progress of the implementation (to be updated periodically) and an element determining whether the measure has been assigned to the appropriate components to make it viable.

5. Conclusions

Based on a state of the art, focused on the autonomous vehicle, it can be seen that many studies show a real interest in this hybridization and the first solutions are provided to overcome the lack of this combination in current standards.

Many methods, mainly focused on risk and threat analysis, show one thing in common: we use existing safety methods where we add security concepts, in order to propose autonomous vehicles that are more resistant to failures and attacks. Others offer several threat assessment solutions, in the same way as security with ASIL, which allows the two assessments to be crossed, especially when a component can be affected by both a failure and a threat, for example. In addition, some complete method for the vehicle life cycle through risk analysis and assessment have been proposed.

However, the vehicle will be resistant to what it has been told to resist, and the design of safety and security countermeasures is little discussed. More precisely, it is a question of determining how to approach the notion of countermeasure. Indeed, a security (resp. safety) countermeasure will not be robust enough to respond to threats (resp. failures). Two solutions are then possible:

- A countermeasure designed from the start in response to failures and threats;
- Two independent countermeasures communicating with each other.

Despite this point, the proposed methods make it possible to imagine the autonomous vehicle of tomorrow: more robust and accepted by society.

Acknowledgement

This work was funded by the IRT SystemX. Authors are listed alphabetically by last name.

References

Abulamddi, M. F. H. (2016). A Survey on Techniques Requirements for Integrateing Safety and Security Engineering for Cyber-Physical Systems. *International Journal of Computer Science & Engineering Survey*.

Amorim, T., H. Martin, Z. Ma, C. Schmittner, D. Schneider, G. Macher, B. Winkler, M. Krammer, and C. Kreiner (2017). Systematic pattern approach for safety and security co-engineering in the automotive domain. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Apvrille, L. and Y. Roudier (2014). Towards the model-driven engineering of secure yet safe embedded systems. In *Electronic Proceedings in Theoretical Computer Science, EPTCS*.

Apvrille, L. and Y. Roudier (2015). Designing safe and secure embedded and cyber-physical systems with

SysML-Sec. In *Communications in Computer and Information Science*.

Burton, S., J. Likkei, P. Vembar, and M. Wolf (2012). Automotive functional safety = safety + security. In *ACM International Conference Proceeding Series*.

Chockalingam, S., D. Hadžiosmanović, W. Pieters, A. Teixeira, and P. van Gelder (2017). Integrated safety and security risk assessment methods: A survey of key characteristics and applications. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Cui, J., G. Sabaliauskaite, L. S. Liew, F. Zhou, and B. Zhang (2019). Collaborative Analysis Framework of Safety and Security for Autonomous Vehicles. *IEEE Access*.

Dürrwang, J., K. Beckers, and R. Kriesten (2017). A lightweight threat analysis approach intertwining safety and security for the automotive domain. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Friedberg, I., K. McLaughlin, P. Smith, D. Laverty, and S. Sezer (2017). STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*.

Griffiths, R. (1984). HAZOP and HAZAN: Notes on the identification and assessment of hazards. *Journal of Hazardous Materials*.

Henniger, O., A. Ruddle, H. Seudié, B. Weyl, M. Wolf, and T. Wollinger (2009). Securing vehicular on-board IT systems: The EVITA project. In *VDI/VW Automotive Security Conference*.

Huber, M., M. Brunner, C. Sauerwein, C. Carlan, and R. Breu (2018). Roadblocks on the Highway to Secure Cars: An Exploratory Survey on the Current Safety and Security Practice of the Automotive Industry. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

IEC (2005). IEC 61508 : Functional safety of electrical/electronic/ programmable electronic safety-related systems.

Islam, M. M., A. Lautenbach, C. Sandberg, and T. Olovsson (2016). A risk assessment framework for automotive embedded systems. In *CPSS 2016 - Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Co-located with Asia CCS 2016*.

Ito, M. (2014). Finding Threats with Hazards in the Concept Phase of Product Development. In *Communications in Computer and Information Science*.

Ito, M. and K. Kishida (2014). An approach to manage the concept phase of ISO 26262. In *Journal of Software: Evolution and Process*.

Kavallieratos, G., S. Katsikas, and V. Gkioulos (2020). Cybersecurity and safety co-engineering of cyber-physical systems - A comprehensive survey. *Future Internet*.

Kriaa, S., L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand (2015). A survey of approaches combining safety and security for industrial control systems.

Larson, U., P. Phung, and D. Nilsson (2013). Vehicle ECU classification based on safety-security characteristics.

Lisova, E., I. Šljivo, and A. Čaušević (2019). Safety and Security Co-Analyses: A Systematic Literature Review.

Lyu, X., Y. Ding, and S. H. Yang (2019). Safety and security risk assessment in cyberphysical systems.

Macher, G., A. Höller, H. Sporer, E. Armengaud, and C. Kreiner (2015). A combined safety-hazards and security-threat analysis method for automotive systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Mann, C. (2009). A Practical Guide to SysML: The Systems Modeling Language. *Kybernetes*.

Mashkoor, A., A. Egyed, and R. Wille (2020). Model-driven Engineering of Safety and Security Systems: A Systematic Mapping Study.

Monteuuis, J. P., A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien (2018). SarA: Security automotive risk analysis method. In *CPSS 2018 - Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Co-located with ASIA CCS 2018*.

Pedroza, G., L. Apvrille, and D. Knorreck (2011). AVATAR: A SysML environment for the formal verification of safety and security properties. In *2011 11th Annual International Conference on New Technologies of Distributed Systems, NOTERE 2011 - Proceedings*.

Pietre-Cambacedes, L. and M. Bouissou (2013). Cross-fertilization between safety and security engineering.

Ponsard, C., G. Dallons, and P. Massonet (2016). Goal-oriented co-engineering of security and safety requirements in cyber-physical systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Popov, P. T. (2015). Stochastic modeling of safety and security of the e-Motor, an ASIL-D device. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Respect-IT (2007). KAOS Tutorial.

Robinson-Mallett, C., B. Kaiser, and J. Meyer (2015). Safety and Security for Networked Vehicles. *Auto Tech Review*.

Roudier, Y. and L. Apvrille (2015). SysML-Sec: A model driven approach for designing safe and secure systems. In *MODELSWARD 2015 - 3rd International Conference on Model-Driven Engineering and Software Development, Proceedings*.

Sabaliauskaite, G. and S. Adepu (2017). Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security. In *Proceedings of IEEE International Symposium on High Assurance Systems Engineering*.

Sabaliauskaite, G., S. Adepu, and A. Mathur (2017). A six-step model for safety and security analysis of cyber-physical systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Sabaliauskaite, G., J. Cui, L. S. Liew, and F. Zhou (2018). Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems. In *Proceedings - 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems and 19th International Symposium on Advanced Intelligent Systems, SCIS-ISIS 2018*.

Sabaliauskaite, G., J. Cui, L. S. Liew, and F. Zhou (2019). Modelling safe and secure cooperative intelligent transport systems. In *Advances in Intelligent Systems and Computing*.

Sabaliauskaite, G., L. S. Liew, and J. Cui (2018). Integrating Autonomous Vehicle Safety and Security Analysis Using STPA Method and the Six-Step Model. *International Journal on Advances in Security 11*(1&2), 160–169.

Sabaliauskaite, G., L. S. Liew, and F. Zhou (2019). AVES – Automated vehicle safety and security analysis framework. In *Proceedings - CSCS 2019: ACM Computer Science in Cars Symposium*.

SAE International (2016, jan). *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*.

Sangchoolie, B., P. Folkesson, and J. Vinter (2018). A Study of the Interplay between Safety and Security Using Model-Implemented Fault Injection. In *Proceedings - 2018 14th European Dependable Computing Conference, EDCC 2018*.

Schmittner, C., T. Gruber, P. Puschner, and E. Schoitsch (2014). Security application of Failure Mode and Effect Analysis (FMEA). In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Schmittner, C. and Z. Ma (2015). Towards a framework for alignment between automotive safety and security standards. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Schmittner, C., Z. Ma, and P. Puschner (2016). Limitation and improvement of STPA-Sec for safety and security co-analysis. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Schmittner, C., Z. Ma, E. Schoitsch, and T. Gruber (2015). A case study of FMVEA and CHASSIS as safety and security co-analysis method for automotive cyber-physical systems. In *CPSS 2015 - Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Part of ASIACCS 2015*.

Schmittner, C., Z. Ma, and P. Smith (2014). FMVEA for safety and security analysis of intelligent and cooperative vehicles. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Schoitsch, E., C. Schmittner, Z. Ma, and T. Gruber (2016). The Need for Safety and Cyber-Security Co-engineering and Standardization for Highly Automated Automotive Vehicles.

Simpson, A., J. Woodcock, and J. Davies (1998). Safety through Security. In *Proceedings of the 9th International Workshop on Software Specification and Design, IWSSD 1998*.

Skoglund, M., F. Warg, and B. Sangchoolie (2018). In search of synergies in a multi-concern development lifecycle: Safety and cybersecurity. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*.

Sojka, M., M. Kreč, and Z. Hanzálek (2014). Case study on combined validation of safety & security requirements. In *Proceedings of the 9th IEEE International Symposium on Industrial Embedded Systems, SIES 2014*.

Steiner, M. and P. Liggesmeyer (2013). Combination of Safety and Security Analysis - Finding Security Problems That Threaten The Safety of a System. *SAFECOMP 2013 - Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security*.

The International Organization for Standardization (2011). Road vehicles — Functional safety. *ISO 26262 (revised in 2018)*.

The International Organization for Standardization (2016). Road vehicles – Cybersecurity engineering.

Wei, J., Y. Matsubara, and H. Takada (2016). Hazop-based security analysis for embedded systems: case study of open source immobilizer protocol stack. In *Studies in Systems, Decision and Control*.

Young, W. and N. Leveson (2013). Systems thinking for safety and security. In *ACM International Conference Proceeding Series*.