Integrating Autonomous Vehicle Safety and Security

Giedre Sabaliauskaite

Centre for Research in Cyber Security (iTrust)
Singapore University of Technology and Design
Singapore 487372
Email: giedre@sutd.edu.sg

Jin Cui

Centre for Research in Cyber Security (iTrust)
Singapore University of Technology and Design
Singapore 487372
Email: jin_cui@sutd.edu.sg

***Abstract*—Safety and security are two inter-dependent key properties of autonomous vehicles. They are aimed at protecting the vehicles from accidental failures and intentional attacks, which could lead to injuries and loss of lives. The selection of safety and security countermeasures for autonomous vehicles depends on the driving automation levels, defined by the international standard SAE J3016. However, current vehicle safety standards ISO 26262 do not take the driving automation levels into consideration. We propose an approach for integrating autonomous vehicle safety and security processes, which is compliant with the international standards SAE J3016, SAE J3061, and ISO 26262, and which considers driving automation levels. It uses the Six-Step Model as a backbone for achieving integration and alignment among safety and security processes and artefacts. The Six-Step Model incorporates six hierarchies of autonomous vehicles, namely, functions, structure, failures, attack, safety countermeasures, and security countermeasures. It ensures the consistency among these hierarchies throughout the entire autonomous vehicle's life-cycle.**

Keywords–Autonomous vehicle; safety; security; ISO 26262; SAE J3016; SAE J3061; Six-Step Model; attack tree; fault tree.

I. INTRODUCTION

Autonomous Vehicles (AVs), the self-driving vehicles, are safety-critical Cyber-Physical Systems (CPS) – complex engineering systems, which integrate embedded computing technology into physical phenomena. Safety and security are two key properties of CPSs, which share the same goal – protecting the system from undesirable events: failures (safety) and intentional attacks (security) [1].

Ensuring the safety of autonomous vehicles, i.e., reducing the number of traffic crashes to prevent injuries and save lives, is a top priority in autonomous vehicle development. Safety and security are interdependent (e.g., security attacks can cause safety failures, or security countermeasures may weaken CPS safety and vice versa), therefore they have to be aligned in the early system development phases to ensure the required level of protection [1][2].

Although AVs could be considered to be smaller and/or less complex systems as compared to other CPSs, such as, e.g., power plants or water treatment systems, they face some unique challenges, which have to be taken into consideration when analyzing their safety and security.

Firstly, there are six different levels of driving automation ranging from no driving automation (level 0) to full driving automation (level 5), as described by the international standard SAE J3016 [3]. The levels describe who (human driver or automated system) performs the driving tasks and monitors the driving environments under certain environmental conditions. Thus, AV safety and security depend on the driving automation levels and the environmental conditions.

Secondly, the AV domain is relatively new, and therefore, there are no international standards for AV safety and security yet. Currently, the ISO 26262 standard, which describes functional safety of road vehicles, is being used for AV safety analysis [4]. However, it is not sufficient for AVs, as argued in [5][6]. ISO 26262 addresses the safety of each function, or item, of the vehicle separately, since the driver is responsible for everything what falls outside the item. However, in AV, it is necessary to ensure safety at all times, especially at the high automation levels, when there is no driver in the vehicle [5]. Thus, hazard analysis of AVs should have the broader scope and should analyze AVs functions together. Warg et al. proposed an approach to extend ISO 26262 and to add generic operational situation and hazard trees for comprehensive AV safety analysis [5].

To address vehicle security needs, the SAE J3061 standard has been developed [7]. It defines cyber-security lifecycle of cyber-physical vehicle systems. However, the security lifecycle, defined in SAE J3061, is analogous to the vehicle safety lifecycle described in ISO 26262, and therefore, it is not sufficient for AV cyber-security analysis.

How can we analyze AV safety and security throughout its entire life-cycle in a consistent way, and provide required level of protection?

In our previous work, we proposed a Six-Step Model for modeling and analysis of CPS safety and security [8][9]. It incorporates six dimensions (hierarchies) of CPS, namely, functions, structure, failures, safety countermeasures, cyber-attacks, and security countermeasures. Furthermore, it uses relationship matrices to model inter-dependencies between these dimensions. The Six-Step Model enables comprehensive analysis of CPS safety and security, as it utilizes system functions and structure as a knowledge base for understanding the effect of failures and attacks on the system.

In this paper, we propose an approach for AV safety and security analysis, which uses the Six-Step Model as a backbone for integrating and maintaining consistency among safety and security processes and artefacts. The Six-Step Model consolidated safety and security artefacts, developed throughout the entire AV life-cycle. The proposed approach is compliant with the international standards SAE J3016, SAE J3061, and ISO 26262.

 ISBN: 978-1-61208-605-7

The remainder of this paper is structured as follows. Section II describes preliminaries. The proposed approach is explained in Section III, and a Six-Step Model example is included in Section IV. Finally, Section V concludes the paper and describes our future work.

II. PRELIMINARIES

A. Autonomous Vehicles' Main Terms and Definitions

The real-time operational and tactical functions required to operate the vehicle in on-road traffic include lateral and longitudinal vehicle motion control, monitoring the driving environment, object and event response execution, maneuver planning, and enhancing conspicuity via lighting, signaling, etc. [3]. These functions are collectively called the Dynamic Driving Task (DDT) [3]. AVs perform entire or part of DDT depending of their automation level.

SAE International (SAE) has developed an international standard, SAE J3016 [3], to describe various levels of vehicle automation. The standard has been widely adopted by international organizations, such as the National Highway Traffic Safety Administration (NHTSA) [10].

There are six driving automation levels [3][10]:

- Level 0 – the human driver performs entire DDT.
- Level 1 – an automated system on the vehicle can assist the human driver to perform either the lateral or the longitudinal vehicle motion, while driver monitors the driving environment and performs the rest of DDT.
- Level 2 – an automated system performs the lateral and the longitudinal vehicle motion, while driver monitors the driving environment and performs the rest of DDT.
- Level 3 – an automated system can perform entire DDT, but the human driver must be ready to take back control when the automated system requests.
- Level 4 – there is no human driver; an automated system conducts the entire DDT, but it can operate only in certain environments and under certain conditions.
- Level 5 – there is no human driver; an automated system performs entire DDT in all environments and under all conditions that a human driver could perform them.

Level 3-5 vehicles are called the highly automated vehicles, since their automated systems (not a human driver) are responsible for monitoring the driving environment [10]. Furthermore, level 1-4 vehicles are designed to operate only in certain environments and under certain conditions, while level 5 vehicles - in all environments and under all conditions.

AV functions can be grouped into three main categories: perception (perception of the external environment/context in which vehicle operates), decision & control (decisions and control of vehicle motion, with respect to the external environment/context that is perceived), and vehicle platform manipulation (sensing, control and actuation of the vehicle, with the intention of achieving desired motion) [11][12]. A standard for describing AV functions and functional interfaces, SAE J3131, is currently under development.

AV structural architecture consists of two main systems: a) cognitive driving intelligence, which implements perception and decision & control functions, and b) vehicle platform, which is responsible for vehicle platform manipulation [11]. Each system consists of components, which belong to four major groups: hardware, software, communication, and human-machine interface [12][13].

B. A Six-Step Model

In our earlier work [8][9], we proposed a Six-Step Model to enable comprehensive CPS safety and security analysis (see Figure 1) . The model is constructed using the following six steps:

1) The first step is aimed at modeling the functional hierarchy of the system. The functions are defined using the Goal Tree (GT), which is constructed starting with the goal (functional objective) and then defining functions and sub-functions, needed for achieving this goal. A relationship matrix, F-F, is used to define the relationships between functions, which can be high, medium, low, or very low.
2) In the second step, system's structural hierarchy is defined using the Success Tree (ST) to describe system's structure as a collection of sub-systems and units. Furthermore, the relationships between structure and functions are defined using a relationship matrix S-F, as shown in Figure 1.
3) The third step is focused on safety hazard analysis. In this step, system's failures are identified and added to the model. In addition, the relationships between failures, system structure and functions are identified, and the corresponding relationship matrices – B-B, B-S, and B-F – are added to the model.
4) The fourth step focuses on security threat analysis. In this step, attacks are identified and added to the model along with the relationship matrices to describe relationships between attacks, failures, structure and functions. Relationship matrix A-B (attacks – failures) is used to determine which failures could be triggered by a successful attack. In the original version of the Six-Step Model [9], safety countermeasures have been identified in step 4, while attacks - in step 5. However, we decided to switch the places of these two steps in order to tackle system vulnerability (hazard and threat) analysis first, before moving to the countermeasure selection, as safety countermeasures can be used to detect and mitigate both the failures and the attacks. Thus, it is convenient to have attack identified before designing safety countermeasures.
5) In the fifth step, safety countermeasures are added to the model and their relationships are identified. Matrices X-A and X-B show the coverage of attacks and failures by safety countermeasures, where white rhombus indicates that the countermeasure provides low protection from attack/failure; gray rhombus - medium protection; black rhombus - full protection (see Figure 1).
6) Finally, in the last step, security countermeasures are added to the model and their relationships are established. Similarly to matrices X-A and X-B from the previous step, two new matrices Z-A and Z-B are added to define the coverage of attacks and failures by security countermeasures. The security

 ISBN: 978-1-61208-605-7

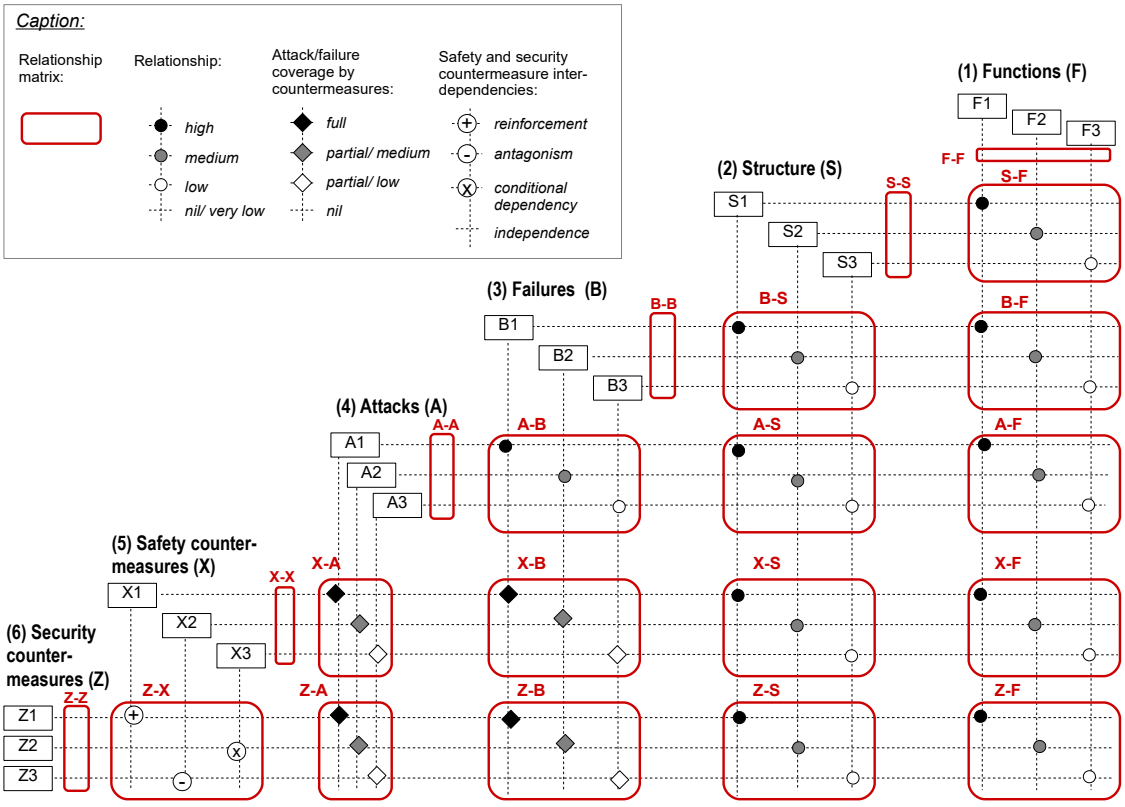

Figure 1. The Six-Step Model.

countermeasures, added in this step, could be used to protect the system from attacks and failures, not covered by the safety countermeasures. Furthermore, matrix Z-X is used to capture the inter-dependencies between safety and security countermeasures, such as reinforcement, antagonism, conditional dependency, and independence, as defined in [14].

After completion of steps 5 and 6, it is important to analyze if there were any changes made to system's structure, as some countermeasures might require the use of additional components, e.g., sensors or controllers. If the changes occur, it is necessary to return to the step 2 to add the new components, and then repeat steps 3-6.

The Six-Step Model, constructed throughout steps 1-6, interconnects six hierarchies of the systems (functions, structure, failures, attacks, and safety and security countermeasures) by forming a hexagon-shaped structure of their relationships, as shown in Figure 2. The relationships help to ensure alignment between these hierarchies. The hierarchies and relationships have to be maintained throughout the entire system's life-cycle to sustain their consistency and completeness.

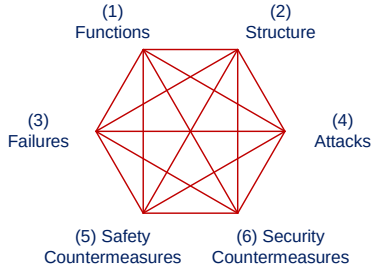

Figure 2. Relationships among hierarchies of the Six-Step Model.

C. AV Safety Analysis

The ISO 26262 standard [4] defines functional safety for automotive equipment applicable throughout the life-cycle of all automotive Electronic and Electrical (E/E) safety-related systems. It aims to address possible hazards caused by the malfunctioning behavior E/E systems. The safety process consists of several phases, such as concept, product development, and production, operation, service and decommissioning. Hazard Analysis and Risk Assessment (HARA) is performed during the concept phase, where hazardous events, safety risks and goals are identified. These goals are further refined into the safety requirements during the product development phase, and the safety countermeasures are designed and implemented.

ISO 26262 requires the presence of the human driver inside the vehicle to deal with the unexpected environments and conditions [5]. In high automation AVs, where no human driver is present, it is important to consider all driving environments and conditions. In [5], Warg et al. proposed a AV hazard analysis method, which extends vehicle safety analysis process defined by ISO 26262 [4]. It uses operational situation and hazard trees as a knowledge base of potential situations and hazards to investigate.

 ISBN: 978-1-61208-605-7

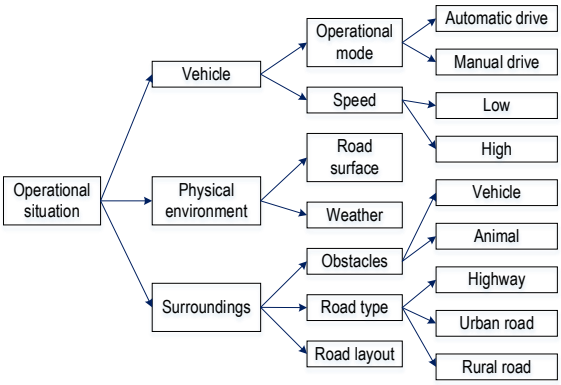

Figure 3. Generic situation tree example [5].

Figure 3 shows an example of an AV operational situation tree, borrowed from [5]. Three main aspects (tree leaves) are identified, namely, vehicle, physical environment, and surroundings, which a further refined into properties, e.g., speed is decomposed into high and low speed (see Figure 3).

Operational situations for use in the hazard analysis are composed by selecting and combining leaves from the tree. If no leaf is selected from a particular aspect, the situation is considered to be valid for all properties of that aspect. For level 5 vehicle, all operational situations have to be analyzed, while for level 1-4 vehicle – only a subset of operational situations, which includes the environment and driving conditions the AV is designed to operate in. Figure 3 shows an example of a high-level situation tree, which is further refined throughout safety lifecycle, as the new situations are identified.

The hazard tree is constructed similarly to the situation tree. Two main levels of hazards are identified: tactical and operative. Tactical hazard include foreseeable tactical mistakes, while operative hazards - hazard related to situation awareness, vehicle control, and environment. Each leaf of the tree represents a possible hazard that can be included in hazard analysis [5].

Once the situation and the hazard trees are completed, each hazard from the hazard tree is combined with each operational situation from the situation tree to form hazardous events. Subsequently, the risk assessment of these events is performed and an Automotive Safety Integrity Level (ASIL) is assigned. The risk assessment has to be updated any time a new or modified situations/hazards are added to the situation/hazard trees [5].

Hazardous events can be further refined using the Fault Tree analysis [13] in order to identify the conditions and events that could lead to these events. Fault tree refines top level hazardous event into intermediate events and basic events, which are interconnected by AND and OR logical operators. Bhavsar et al. [13] describe two fault trees for AVs: fault tree of failures related to vehicular components, and fault tree considering failures related to transportation infrastructure components. Safety risks are defined based on the results of the hazard and failure analysis, which are then used for defining AV safety requirements and, subsequently, developing safety countermeasures.

D. AV Security Analysis

SAE J3061 is a vehicle cyber-security standard, which was developed using the ISO 26262 standard as a base. Thus, both standards consist of similar phases. Security process, defined by SAE J3061, includes concept, product development, and production & operation phases. Threat Analysis and Risk Assessment (TARA) is performed during the concept phase, where threats, security risks, and security goals are defined. In the product development phase, security requirements are defined based on the security goals, and the security countermeasures are developed.

Attack tree analysis [7][15] is often used for performing TARA. It helps to determine the potential paths that an attacker could take to lead to the top level threat [7]. An attack tree is a graph, where the nodes represent attack events, and the edges - attack paths through system, which could be connected using AND and OR gates.

Behavior diagrams, such as Data-Flow Diagrams (DFD) [16] and Information-Flow Diagrams (IFD) [9] could be used for identifying the attacks to be included in attack trees analysis. DFDs include elements, such as processes, data flows, and data store, and are used to model data flows between software components. IFDs include units and information flows between them, and could be used to model information flows between software and hardware components, such as actuators, controllers, sensors, etc. In [9], we proposed a method for generating IFDs using the Six-Step model in order to identify possible attacks on CPSs.

III. Integrated Autonomous Vehicle Safety and Security Analysis Approach

This section proposes an approach for integrating AV development with safety safety and security engineering, which is compliant with the international standards SAE J3016, SAE J3061 and ISO 26262. The integration is achieved by the use of the Six-Step Model, which incorporates AV functions, structure, safety failures, security attack, and safety & security countermeasures. The Six-Step Model is the backbone for achieving integration and alignment among safety and security artefacts.

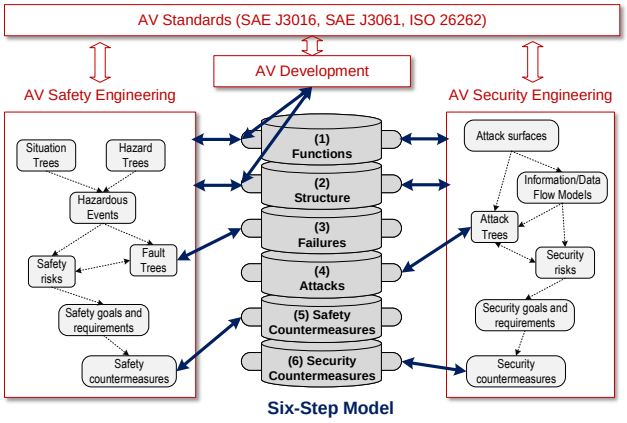

Figure 4. The Six-Step Model as a backbone for integrated AV safety and security analysis.

Figure 4 describes the proposed approach and shows the relationships between steps of the Six-Step Model and

various artefacts from AV development, safety engineering, and security engineering processes.

The steps of the AV Six-Step Model are performed in the following order:

- Steps (1) and (2). Autonomous driving functions and the systems (structure), which implement these functions, are defined during AV development process. As the result, AV functional and structural hierarchies are defined and added to the Six-Step Model, along with their relationships.
- Steps (3) and (4). These steps correspond to AV vulnerability (hazard and threat) analysis. On the safety side, HARA (as defined by ISO 26262) is performed in order to identify and evaluate hazardous events, and define AV functional safety requirements. Additional models, such as situation, hazard, and fault trees, are used to ensure that all autonomous driving related hazards are considered, as described in Section II-C. At the end of the hazard analysis phase, failures, which are considered in security requirements, are extracted from the fault trees and added to the the Six-Step Model (Step (3)). On the security side, TARA (as defined by SAE J3061) is performed in order to evaluate security threats and derive AV functional security requirements. The AV structural hierarchy, defined in step (2), could be used to define attack surfaces and construct information-flow models (see [9]), which helps to identify possible attacks and construct attack trees, as described in Section II-D. The risks associated with each attack are then evaluated and security requirements are defined. Similarly to failures, the attack, included in security requirements, are extracted from the attack trees and added to the Six-Step Model (Step (4)). The relationships between attacks, failures, functions, and structures, are also added to the Six-Step model.
- Steps (5) and (6). During these steps, safety and security countermeasures are selected and added to the model along with their relationships to remaining elements of the model. On the safety side, functional safety requirements are refined into technical requirements and corresponding countermeasures are designed for satisfying these requirements. Similarly, on the security side, functional security requirements are decomposed into technical requirements for security countermeasures. The countermeasures from both sides are added to the Six-Step Model to analyze their relationships to the remaining elements of the model. In particular, the matrices are useful to make sure that each countermeasure is really needed (addresses attacks/failures not completely covered by any other countermeasures, shown in matrices X-A, X-B, Z-A, and A-B), and that there are no contradictions among countermeasures (matrix Z-X).

The AV Six-Step Model, constructed during steps (1)-(6), is a backbone of AV vulnerability analysis. It supports three AV processes, namely, AV development, AV safety engineering, and AV security engineering, as shown in Figure 4. It enables integration of safety and security artefacts, developed throughout the entire AV life-cycle (such as failures, attacks, safety and security countermeasures) into AV function and structure hierarchies to assure their consistency and completeness.

The AV Six-Step Model has to be maintained throughout the entire AV life-cycle. This is particularly important for security, as new threats are continually identified and analyzed.

The following section shows a Six-Step Model example of an AV.

IV. Six-Step Model Example of an AV

The AV, described in this example, performs three main autonomous driving functions, i.e., perception, decision & control, and vehicle platform manipulation, as described in Section II-A. The perception function can be further decomposed into sensing, sensor fusion, localization, semantic understanding, and world model (see [11]). These functions are added at the top of to Six-Step Model and their inter-relationships are identified, as shown in Figure 5.

Due to space limitations, only an excerpt of the Six-Step Model is included in Figure 5. Furthermore, only the high degree relationships between elements are shown.

The main systems of AV, which implement driving automation functions, are: cognitive driving intelligence, vehicle platform, and communication system [11][12]. The cognitive driving intelligence includes on-board computer and external sensors for perception of environment, such as LIDAR, Radar, cameras, and ultrasound sensors [17]. No sensor type works well for all tasks and in all conditions, thus it is necessary to provide sensor redundancy and perform sensor fusion. A combination of LIDAR, Radar, and camera provides good coverage of AV tasks in most of the environmental conditions [17]. The vehicle platform includes controllers (ECUs), actuators, which implement the desired motion. The communication system includes in-vehicle and V2X (vehicle to vehicle, infrastructure, and humans) communication networks. In this example, only in-vehicle communication is considered. All these structural elements are added to model in step (2).

In steps (3) and (4), we included LIDAR failure and LIDAR attack. LIDAR is a laser sensor used in AVs for object detection. As we can see from Figure 5, the main function affected by either the LIDAR failure or attack is the sensing function. Furthermore, there is a strong relationship between LIDAR attack and failure, LIDAR attack is strongly related to Ethernet (i.e., an attacker can attack LIDAR through Ethernet).

Attacks on LIDAR and security countermeasures are summarized in [18]. An attacker could perform a relay attack (relaying the original signal sent from target vehicle LIDAR from another position to create fake echoes) or a spoofing attack (replaying objects and controlling their position) on LIDAR.

Radar is added to the model in step (5) as a safety countermeasure. In case of of LIDAR failure, Radar and camera will still be able to perform sensing of the driving environment.

Security countermeasures could include redundancy: multiple LIDARs, or V2X communication to compare measurements of target vehicle with other vehicles to detect inconsistencies [18]. However, due to high cost of LIDAR, multiple LIDARs are not considered in this AV. Furthermore, there is no V2X communication in this AV example. If the vehicle

 ISBN: 978-1-61208-605-7

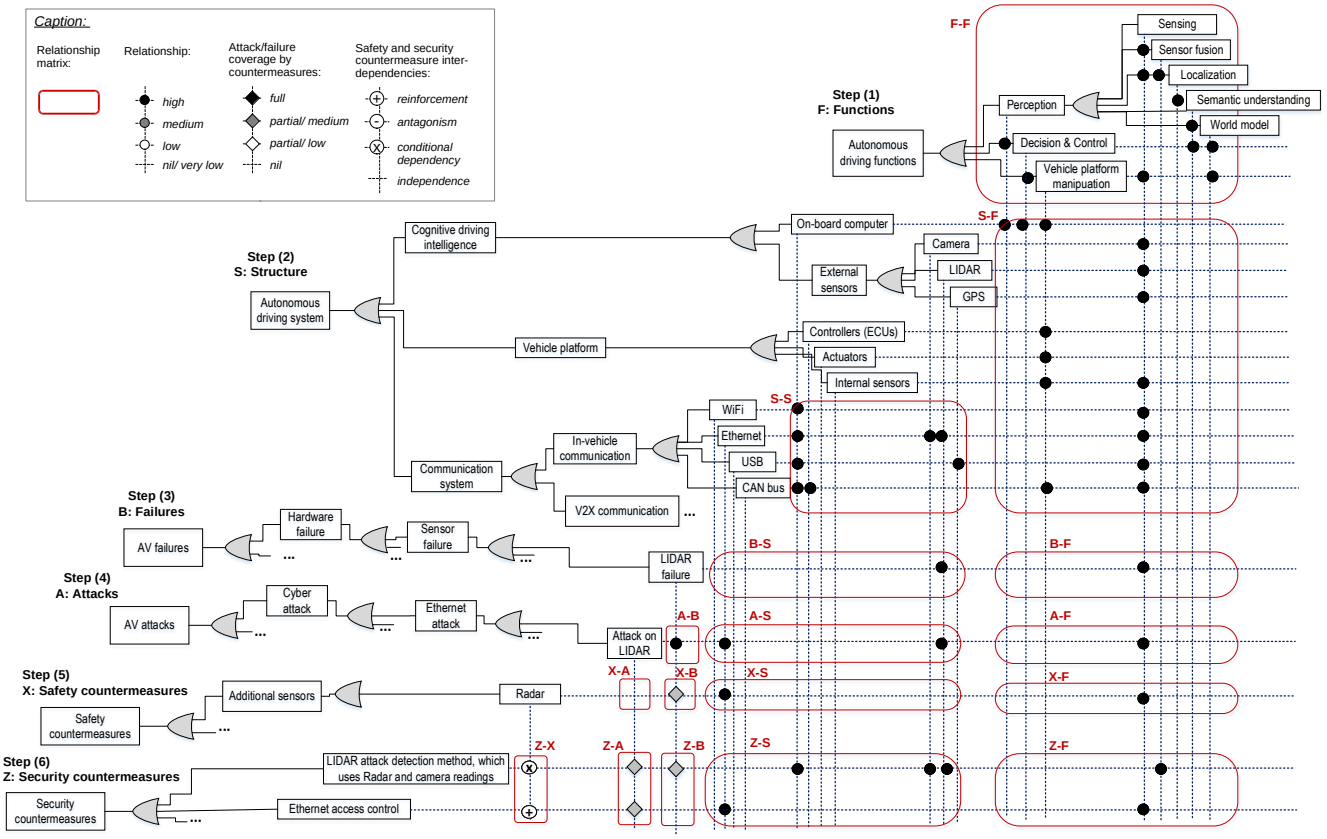

Figure 5. An example of AV Six-Step Model.

had V2X communication, LIDAR attacks could be detected by cross-comparing LIDAR reading of the nearby vehicles.

Various LIDAR attack detection and mitigation methods can be implemented inside on-board computer, e.g., LIDAR attacks can be detected by comparing LIDAR readings to Radar and camera reading, while shorter or randomized LIDAR scanning interval could help in preventing the attacks [18]. In Figure 5, a security countermeasure, "LIDAR attack detection method, which uses Radar and camera readings", is added. Additional countermeasure, "Ethernet access control", is used to prevent LIDAR attacks.

Matrices X-A, X-B, Z-A, Z-B, and Z-X are very useful for integrated safety and security analysis. X-B shows that Radar provides partial coverage of LIDAR failure, as Radar cannot fully replace LIDAR. Z-A and Z-B indicate that LIDAR attack detection method will be able to provide coverage not only for LIDAR attacks, but also failures, as it will detect corrupt LIDAR readings, which could happen in either case. Finally, Matrix Z-X shows the inter-dependencies between safety and security countermeasures. As we can see from Figure 5, Radar (safety countermeasure) and the LIDAR attack detection method (security countermeasure) share a conditional dependency (denoted by x), i.e., in order to implement the attack detection method, we need a Radar; while Radar and Ethernet access control mechanism reinforce each other.

As the new structural component, Radar, has been added to the model in Step (5), it is necessary to return to the step (2) to include it to AV structural hierarchy and to establish its relationships to the remaining elements of the model.

V. Conclusions and Future Work

In this paper, an approach for integrated autonomous vehicle safety and security analysis is proposed, which is compliant with the international standards SAE J3016, SAE J3061, and ISO 26262. It uses the Six-Step Model as a backbone for achieving and maintaining integration and alignment among safety and security artefacts throughout the entire autonomous vehicle's life-cycle. The Six-Step Model incorporates six hierarchies of autonomous vehicles, namely, functions, structure, failures, attack, safety countermeasures, and security countermeasures. An example of an autonomous vehicle Six-Step Model is included to demonstrate the usefulness of the proposed approach.

Future work will include the refinement of the proposed approach to facilitate its application in industry and the use by other researchers. We are currently building a software tool for constructing the Six-Step Model. Furthermore, we are exploring the possibility to integrate our approach with the safety analysis approach System-Theoretic Processes Analysis (STPA), which has been designed for evaluating the safety of complex systems [6]. We believe that a combination of these two approaches could help to achieve roadworthiness of the autonomous vehicles, and would contribute to the development of standards for autonomous vehicles.

 ISBN: 978-1-61208-605-7

REFERENCES

[1] G. Sabaliauskaite and A. P. Mathur, Aligning Cyber-Physical System Safety and Security. Cham: Springer International Publishing, 2015, pp. 41–53. [Online]. Available: https://doi.org/10.1007/978-3-319-12544-2_4

[2] L. Pièrre-Cambacédès and M. Bouissou, "Cross-fertilization between safety and security engineering," Reliability Engineering & System Safety, vol. 110, 2013, pp. 110 – 126.

[3] SAE J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems. SAE International, Sep. 2016.

[4] ISO26262-2:2011, Road Vehicles – Functional Safety – Part2: Management of Functional Safety. International Organization of Standardization, ISO, 2011.

[5] F. Warg et al., Defining Autonomous Functions Using Iterative Hazard Analysis and Requirements Refinement. Cham: Springer International Publishing, 2016, pp. 286–297. [Online]. Available: https://doi.org/10.1007/978-3-319-45480-1_23

[6] A. Abdulkhaleq et al., "A systematic approach based on stpa for developing a dependable architecture for fully automated driving vehicles," Procedia Engineering, vol. 179, no. Supplement C, 2017, pp. 41 – 51.

[7] SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. SAE International, Jan. 2016.

[8] G. Sabaliauskaite, S. Adepu, and A. Mathur, "A six-step model for safety and security analysis of cyber-physical systems," in the 11th International Conference on Critical Information Infrastructures Security (CRITIS), Oct 2016.

[9] G. Sabaliauskaite and S. Adepu, "Integrating six-step model with information flow diagrams for comprehensive analysis of cyber-physical system safety and security," in 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Jan 2017, pp. 41–48.

[10] Automated Driving Systems 2.0. A Vision for Safety. National Highway Traffic Safety Administration, NHTSA, U.S. Department of Transportation, Sep. 2017.

[11] S. Behere and M. Törngren, "A functional reference architecture for autonomous driving," Inf. Softw. Technol., vol. 73, no. C, May 2016, pp. 136–150. [Online]. Available: http://dx.doi.org/10.1016/j.infsof.2015.12.008

[12] S. Kato, E. Takeuchi, Y. Ishiguro, Y. Ninomiya, K. Takeda, and T. Hamada, "An open approach to autonomous vehicles," IEEE Micro, vol. 35, no. 6, Nov 2015, pp. 60–68.

[13] P. Bhavsar, P. Das, M. Paugh, K. Dey, and M. Chowdhury, "Risk analysis of autonomous vehicles in mixed traffic streams," Transportation Research Record: Journal of the Transportation Research Board, vol. 2625, 2017, pp. 51–61.

[14] L. Pièrre-Cambacédès and M. Bouissou, "Modeling safety and security interdependencies with bdmp (boolean logic driven markov processes)," in 2010 IEEE International Conference on Systems, Man and Cybernetics, Oct 2010, pp. 2852–2861.

[15] B. Schneier, Attack Trees. Wiley Publishing, Inc., Indianapolis, Indiana, 2015, in Book, Secrets and Lies.

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

[17] "Beyond the Headlights: ADAS and Autonomous Sensing," 2016, URL: http://woodsidecap.com/wp-content/uploads/2016/12/20160927-Auto-Vision-Systems-Report_FINAL.pdf [accessed: 2017-09-18].

[18] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," in Black Hat Europe, Nov. 2015.

 ISBN: 978-1-61208-605-7