# AVES – Automated Vehicle Safety and Security Analysis Framework

Giedre Sabaliauskaite
iTrust Centre for Research in Cyber Security, Singapore University of Technology and Design
Singapore
giedre@sutd.edu.sg

Lin Shen Liew
iTrust Centre for Research in Cyber Security, Singapore University of Technology and Design
Singapore
linshen_liew@sutd.edu.sg

Fengjun Zhou
iTrust Centre for Research in Cyber Security, Singapore University of Technology and Design
Singapore
fengjun_zhou@sutd.edu.sg

## ABSTRACT

Automated Vehicle (AV) safety and cybersecurity is an important issue that has to be adequately addressed to ensure that AVs are ready to drive on public roads, and that they are able to safely and efficiently coexist with other motorized and non-motorized traffic participants. So far, there are numerous challenges, such as lack of international standards, software and hardware limitations, absence of methods for integrated safety and security analysis, etc. This paper proposes a novel approach, AVES Framework, for systematic, model-based, integrated AV safety and cybersecurity analysis. AVES Framework adheres to road vehicle development lifecycle and is consistent with international and national standards. It is a flexible method and may be used to analyze any AV regardless of its automation and connectivity level. Furthermore, several relationship matrices and a Safety and Cyber Security Deployment (SCSD) Model, inspired by the Quality Function Deployment method, are used in AVES Framework for relationship analysis and decision making with respect to safety and cybersecurity requirements, measures, and system components.

## KEYWORDS

automated vehicle, safety, cybersecurity, ISO 26262, SAE 3016, SAE 3061, TR 68, Quality Function Deployment

**ACM Reference Format:**
Giedre Sabaliauskaite, Lin Shen Liew, and Fengjun Zhou. 2019. AVES – Automated Vehicle Safety and Security Analysis Framework. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

## 1 INTRODUCTION

Automated vehicles (AVs) are gradually turning into reality, thanks to the rapid advancement of Internet of Things and Artificial Intelligence. Expectations are high, among those motivating the development of AVs, that the road users will get to enjoy better mobility and increased safety on the road.


*Conference'17, July 2017, Washington, DC, USA*

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

However, can we trust AVs? Are AVs safe, secure, and ready to efficiently coexist with other motorized (motorbikes, buses, etc.) and non-motorized (pedestrians, bicyclists, etc.) traffic participants?

Recent accidents involving AVs have raised some doubts about the AV safety. Security is another important concern, since in addition to failures AVs are vulnerable to cyberattacks [4, 5, 7, 11, 14]. A successful attack could lead to various safety, operational, financial, or privacy losses [2]. This indicates that AV safety and cybersecurity are inter-dependent, and therefore should be analyzed in a consistent and integrated way.

In AVs, driving automation is implemented using the Automated Driving System (ADS) – the hardware and software collectively capable of performing automated driving functions [2]. There are numerous challenges related to ADS safety and cybersecurity analysis. Firstly, there are five levels of driving automation, as defined by the SAE J3016 standard [1], ranging from driver assistance (level 1) to full driving automation (level 5). An AV can be designed to perform at one or several driving automation levels. More precisely, multiple ADS applications – features – can be implemented in a single AV, each associated with a particular level of driving automation and operational environment [2].

In addition, AVs can operate in isolation, or can communicate with other vehicles, road infrastructure, and personal devices. Based on connectivity level, we can define two types of AVs: autonomous AVs (AVs that operate in isolation from other vehicles, using their internal sensors to "see" the environment) and Extended Automated Vehicles (ExAVs) (AVs that extend beyond the physical boundary of the road vehicle and consist of road vehicle, off-board systems, external interfaces and the data communication between AV and off-board systems [8]).

Furthermore, ADS has numerous design constraints, as described in [13]. Six classes of constraints have been identified, such as performance, predictability, storage, thermal, power, and others. These constraints have to be considered during AV safety and security analysis.

Finally, there is a lack of international standards for addressing AV safety and security due to the novelty of AV domain. Available standards are not sufficient for highly automated vehicles [10]. Furthermore, they treat safety and security separately.

ISO 26262 [9] and ISO/PAS 21448 [10] have been developed for addressing road vehicle safety needs. Two types of safety are defined for road vehicles: functional safety (ISO 26262) and Safety Of The Intended Functionality (SOTIF) (ISO/PAS 21448). Functional safety is the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electric/electronic systems; SOTIF

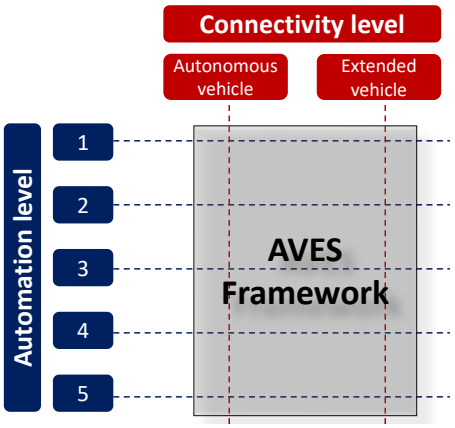


**Figure 1: AVES Framework scope.**

– absence of unreasonable risk due to hazards caused by intended functionality (e.g. inability of the function to correctly comprehend the situation) or performance limitations [10]. Both of these standards are primarily developed for vehicles that could include some driver assistance system, however, are not sufficient for highly automated vehicles [10].

To address vehicle security needs, the SAE J3061 standard has been developed [2]. It defines cybersecurity 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 higly automated vehicle cybersecurity analysis. ISO and SAE are currently jointly developing ISO 21434 [3] standard, which will replace SAE J3061 in 2019.

In Singapore, a technical reference TR 68 for autonomous vehicles has been published in 2019 [16]. It consists of four parts, which include basic AV behaviours (Part 1), safety (Part 2), cybersecurity (Part 3), and vehicular data (Part 4). In this standard safety and security are considered separately as well.

How can we analyze AV safety and cybersecurity in a consistent and integrated way throughout entire vehicle development lifecycle, taking into consideration the aforementioned challenges?

We propose a new approach AVES – Automated Vehicles Safety and Security Analysis Framework. It consists of several stages, distributed across AV development lifecycle, which facilitate AV safety and cybersecurity analysis. Four relationship matrices and a Safety and Cyber Security Deployment (SCSD) Model are used by the AVES Framework to help in decision making and managing AV safety and cybersecurity.

The remainder of this paper is structured as follows. Section 2 presents an overview of the AVES Framework. Relationship matrices and SCSD Model are described in Section 3. Finally, Section 4 concludes the paper and describes our future work.

## 2 AVES FRAMEWORK

AVES Framework is developed with the intent to achieve the following objectives: firstly, it should be consistent with the aforementioned international and national road vehicle safety and security standards; secondly, it must adhere to vehicle development lifecycle; lastly, it should enable integrated Safety and Cyber Security (S&CS) analysis of an AV at any vehicle automation and connectivity levels, as depicted in Fig. 1.

Fig. 2 shows the main stages of the AVES Framework, which are described in more detail in Table 1. As we can see from Fig. 2 and Table 1, AVES Framework consists of 11 stages distributed throughout the entire vehicle lifecycle, which includes concept, product development, production, operation, service, and decommissioning phases.

AVES Framework starts with development of high-level AV specifications (Stage 1) at concept phase, needed for high-level safety and cybersecurity analysis, requirement specification and risk evaluation (Stage 2), and measure selection (Stage 3) (see Fig. 2). Once we are satisfied with the outcome of the analysis at the concept phase, we can move to the product development phase and perform similar activities at a more detailed and technical level (Stages 4-6).

Integrated AV safety and cybersecurity analysis, performed in Stages 2 and 4, is based on the System-Theoretic Process Analysis (STPA) [12]. Its description is out of scope of this paper.

There are feedback loops between stages, as shown in Fig. 2, to address the changes/modifications that have to be performed in previous stages. For example, if we are not able to select a satisfactory set of safety and security measures to implement safety and security requirements in Stage 3, we need to return to Stage 2 and modify the requirements. If we are not able to do so using the existing AV design (specifications developed in Stage 1), we need to return to Stage 1 and modify AV design. After that, it is necessary to repeat Stages 2 and 3.

Finally, at the end of product development phase, once the S&CS analysis is completed and risk level is acceptable, we are able to construct the SCSD Model (Stage 7), which is the main source of information for analyzing AV safety and security during subsequent AV lifecycle phases, such as production, operation, service, and decommissioning (AVES Stages 8-11). During these phases, we normally do not have full access to the information from concept and product development phases. Thus, SCSD Model could provide a sufficient amount of information required for S&CS analysis in these phases.

## 3 RELATIONSHIP MATRICES AND SCSD MODEL

Relationship matrices and SCSD Model are inspired by the principles of Quality Function Deployment (QFD) [6]. QFD was developed in Japan in 1960s as a systematic method for structured product planning and development. Fundamentally, QFD is a process or methodology that utilizes a series of matrices to transform qualitative customer requirements into detailed engineering specifications hence plans so that the end product can satisfy those requirements. Besides proven effective in reducing development time and cost, QFD is also a tool useful for recording the considerations/decisions made during the product development process, which may facilitate cross-functional communication and discussion [6].

QFD matrix, namely House of Quality (HoQ), displays the relationships between dependent (WHATs) and independent (HOWs)

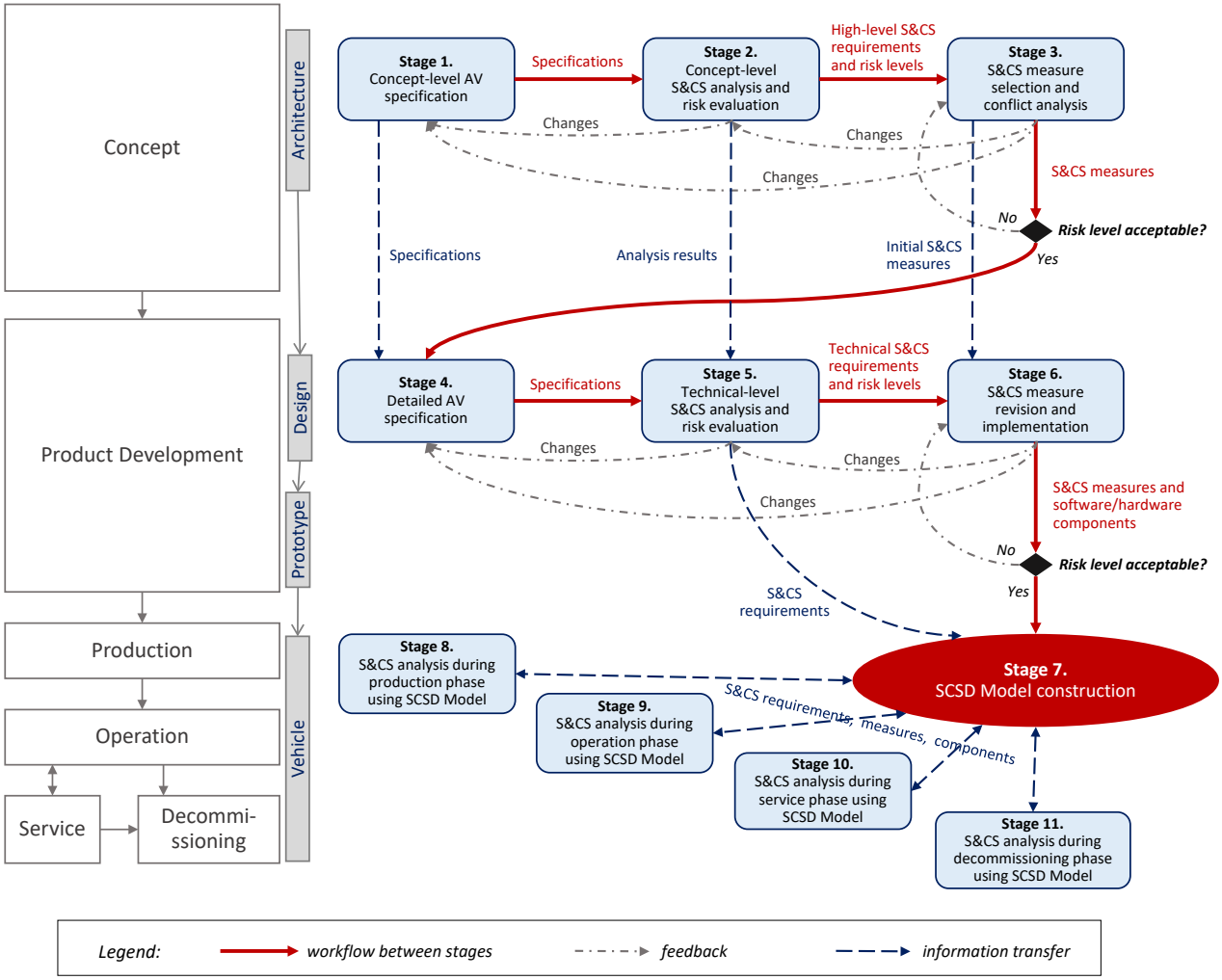


**Figure 2: Stages of the AVES Framework.**

variables. WHATs are included as rows of HoQ, while HOWs – as columns.

Typically, QFD process begins with defining the customer requirements and mapping them on the design requirements using a relationship matrix. Such a matrix helps to select design requirements. Then, cascading matrices could be constructed to map design requirements to engineering design, engineering design to product characteristics, and so on.

We use QFD-style matrices in AVES Framework for relationship analysis and decision making with respect to safety and cybersecurity requirements, safety and security measures, and system components.

Five matrices are used in AVES Framework:

- Matrix 1: S&CS Requirement Conflicts – helps to analyze relationships between safety and cybersecurity requirements;
- Matrix 2: S&CS Requirement Coverage – helps in selecting safety and cybersecurity measures to satisfy S&CS requirements;
- Matrix 3: S&CS Measure Relationships – helps to analyze relationships between safety and cybersecurity measures;
- Matrix 4: S&CS Measure Implementation – helps to assign software/hardware components to safety and cybersecurity measures;
- SCSD Model: a meta-matrix, which incorporates Matrices 1-4.

The workflow of Matrices 1-4 is shown in Fig. 3, and the SCSD Model structure is depicted in Fig. 4. Matrix 1 is constructed in AVES Stages 2 and 5, while Matrices 2, 3 and 4 – Stages 3 and 6. Finally, SCSD Model is constructed in Stage 7.

As we can see from Fig. 3, there is a correlation between Matrices 1-4: a matrix's column headers (the HOWs) shall conditionally become the subsequent matrix' row headers (the WHATs). Furthermore, there are feedback loops to previous matrices to enable revision of the input information, if necessary. For example, if the conflicts between safety and cybersecurity measures cannot be solved in Matrix 3, it is necessary to return to Matrix 2 and select

**Table 1: Summary of 11 stages of AVES Framework**

| Stage No. | Title | Description | Lifecycle phase |
|---|---|---|---|
| 1 | Concept-level AV specification | AV specifications (descriptions, diagrams, etc.), needed for performing S&CS analysis in Stage 2, are prepared. | Concept |
| 2 | Concept-level S&CS analysis and risk evaluation | AV S&CS analysis is performed using the specifications defined in Stage 1 as an input. Hazards and threats are identified, their risk levels are evaluated, and high-level S&CS requirements are defined. Matrix 1 is used to analyze conflicts between requirements. | |
| 3 | S&CS measure selection and conflict analysis | S&CS measures are selected based on high-level requirements defined in Stage 2, and the analysis of possible conflicts between S&CS measures is performed. Matrix 2 is used to facilitate measure selection, while Matrix 3 – to analyze relationships between measures, and Matrix 4 – to assign system components to measures. Matrix construction can be skipped if there is no sufficient information on S&CS measures and components available yet. | |
| 4 | Detailed AV specification | Detailed models and descriptions, needed for performing S&CS analysis in Stage 5, are developed, using AV design documentation and information received from Stages 1 and 3. | Product development |
| 5 | Technical-level S&CS analysis and risk evaluation | AV S&CS analysis is performed using the specifications defined in Stage 4 and high-level analysis results from Stage 2. Hazards and threats are identified, their levels are evaluated, and technical S&CS requirements are defined. Matrix 1 is used to analyze conflicts between requirements. | |
| 6 | S&CS measure revision and implementation | S&CS measures are selected based on technical S&CS requirements defined in Stage 5; the analysis of possible conflicts between S&CS measures is performed. Matrix 2 is used to facilitate measure selection, while Matrix 3 – to analyze relationships between measures, and Matrix 4 – to assign software/hardware components to measures. | |
| 7 | SCSD Model construction | SCSD (Safety and Cyber Security Deployment) Model is constructed based on the artefacts of previous stages. (SCSD model is explained in Section 3) | |
| 8,9, 10,11 | S&CS analysis using SCSD Model | The SCSD Model is used to handle any hazards or security threats, which might occur after product development phase has been completed. | Production, Operation, Service and Decommissioning. |

another set of measures that satisfy the safety and cybersecurity requirements, and then to analyze the relationships of newly selected measures in Matrix 3.

The following subsections include detailed description of all matrices.

## 3.1 Matrix 1

Matrix 1 is constructed in AVES Stages 2 and 5, where AV hazards and threats are identified, their risks are evaluated, and S&CS requirements are defined. The S&CS requirements are to be both row headers and column headers of Matrix 1, as shown in Fig. 5. This matrix serves to capture the relationships that exist between requirements, using symbols shown in Table 2. Note that each cell (i.e. intersection of row and column) may be empty or contain only one symbol. The additional rows appended to Matrix 1, as depicted in Fig. 5, are described in Table 3.

This matrix is used in the following way. All safety and cybersecurity requirements, identified in the analysis phase, are included as rows and columns of Matrix 1. Information about their risk level is added at the bottom of the matrix. Then, we choose each requirement from the rows and go through all the requirements, listed in the columns, and analyze if there are any conflicts between them. Identified conflicts are recorded in the matrix using "X" symbol.

**Table 2: Symbols used in Matrix 1 to denote the relationships between requirements**

| Symbol | Definition |
|---|---|
| X | The requirement (row header) is conflicted by another requirement (column header). |

At the end of conflict analysis, the total number of conflicts of each requirement is recorded at the bottom of the matrix. The final step is to revise the results and decide which requirements to include for implementation, depending on their risk levels and number of

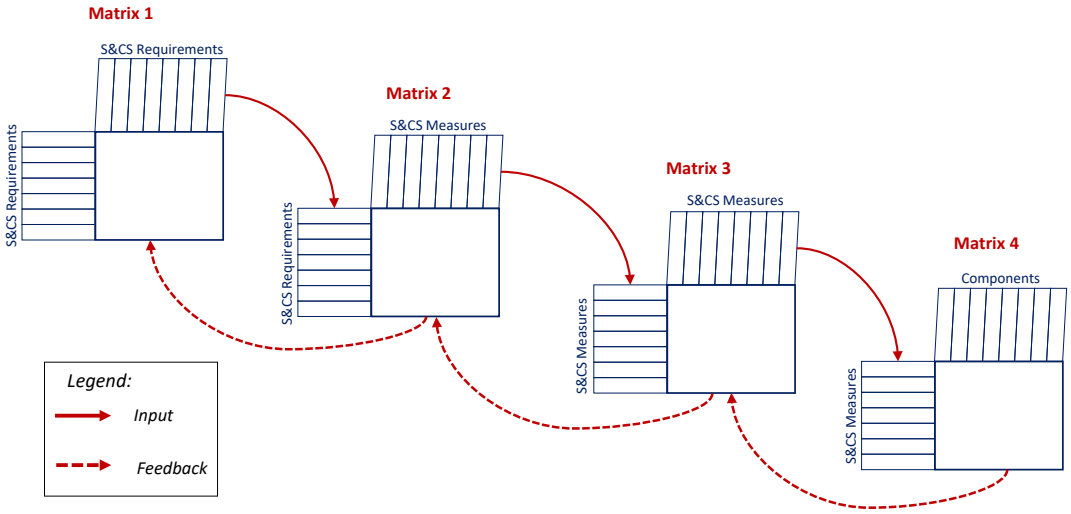


**Figure 3: Correlation between Matrices 1-4.**

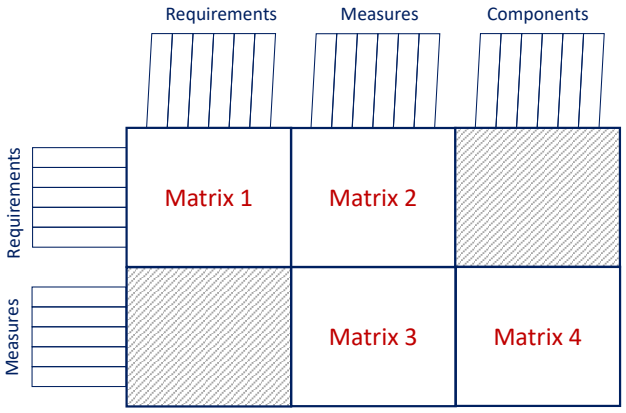


**Figure 4: Graphical representation of SCSD Model.**

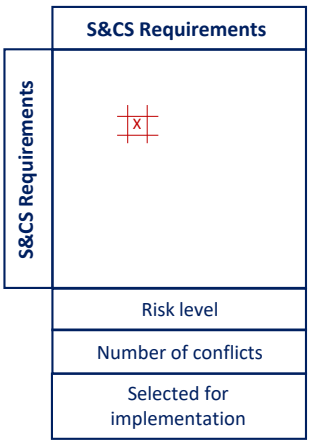


**Figure 5: Matrix 1.**

**Table 3: Description of the additional rows of Matrix 1**

| Row | Description |
|---|---|
| Risk level | Each cell must contain a symbol that represents the risk level of the corresponding requirement. |
| Number of conflicts | Each cell must contain a number that shows how many "X" the corresponding column (in Matrix 1) has. |
| Selected for implementation | The cell must be marked with a tick if the corresponding requirement is judged to be selected for implementation. Its corresponding *Risk level* and *Number of conflicts* are used as judging criteria. |

conflicts with other requirements. The requirements, selected for implementation, should have no or minimum/acceptable number of conflicts with other requirements. Otherwise, it is necessary to revise the requirements and then repeat their conflict analysis.

It might be difficult to identify conflicts among high level safety and security requirements in the concept phase. In such cases, Matrix 1 is still a useful tool for making the selection of requirements for implementation based on their risk level. However, Matrix 1 is particularly useful in product development phase for analysing conflicts between technical safety and cybersecurity requirements, which include technical details.

## 3.2 Matrix 2

Matrix 2 is constructed in AVES Stages 3 and 6 to help in selecting safety and security measures. The requirements, selected for implementation from Matrix 1, and the S&CS measures are to be row headers and column headers of Matrix 2, respectively, as shown in Fig. 6. This matrix is intended to capture the relationships that

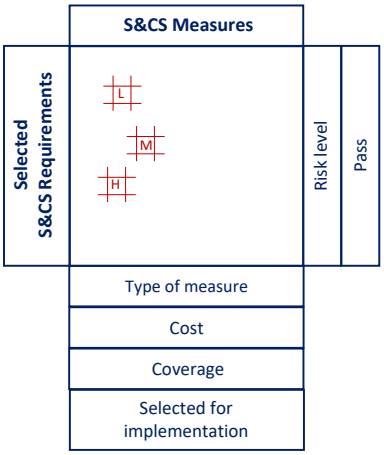


**Figure 6: Matrix 2.**

**Table 4: Symbols used in Matrix 2 to denote the relationships between requirements and measures**

| Symbol | Definition |
|---|---|
| L | The measure is 1-30% effective in satisfying the requirement. |
| M | The measure is 31-60% effective in satisfying the requirement. |
| H | The measure is 61-100% effective in satisfying the requirement. |

**Table 5: Description of the additional rows of Matrix 2**

| Row | Description |
|---|---|
| Type of measure | Each cell may contain up to three symbols, namely "P", "D" and "C", which signify that the corresponding measure is preventive, detective and corrective respectively. |
| Cost | Each cell must contain a number that shows the cost required for implementing the corresponding measure. |
| Coverage | Each cell must contain a number that shows how many "H" the corresponding column (in Matrix 2) has. |
| Selected for implementation | The cell must be marked with a tick, if its corresponding measure is judged to be selected for implementation. Its corresponding *Type of measure*, *Cost* and *Coverage* are used as judging criteria. |

exist between requirements and measures, using symbols shown in Table 4. The additional rows and columns appended to Matrix 2, as depicted in Fig. 6, are described in Tables 5 and 6 respectively.

**Table 6: Description of the additional columns of Matrix 2**

| Column | Description |
|---|---|
| Risk level | Each cell must contain a symbol that represents the risk level of its corresponding *requirement*. |
| Pass | The cell must be marked with a tick, if its corresponding *requirement* is judged to be adequately satisfied. The judging criteria are: i) the effectiveness of measures (which have been selected for implementation) in satisfying the corresponding *requirement*; ii) the corresponding risk level.<br>Note that this column, once filled, is intended to allow the analysts to quickly spot which requirements are not yet adequately satisfied by the selected set of measures. If the number of unsatisfied *requirements* is significant, then the selected set of *measures* should be revised and this column be updated accordingly. |

Matrix 2 is used to make a decision regarding S&CS requirement satisfaction using the S&CS measures. If a requirement can be satisfied by the measure (shown by column headers), then at their corresponding cell (i.e. intersection of corresponding row and column) of Matrix 2, its degree of satisfaction must be indicated. The degree of satisfaction shows how effective the measure is in mitigating specific failures or attacks addressed by the S&CS requirements. For more details, see Table 4.

Once the analysis of all the requirements is finished, it is necessary to determine which measures should be selected for implementation, based on several criteria, such as cost of the measure and coverage. Once the selection of the measures is completed, we fill in the "Pass" column; this column is intended to conclude the requirements satisfaction analysis. Ideally, all the requirement should have a tick in the "Pass" column. If that is not possible, at least the requirements with high risk level should be satisfied.

## 3.3 Matrix 3

Matrix 3 is constructed after Matrix 2 is completed in AVES Stages 3 and 6. It is useful for analyzing relationships between safety and security measures. The S&CS measures, selected for implementation (acquired from Matrix 2), are to be both row headers and column headers of Matrix 3, as shown in Fig. 7. This matrix serves to capture the relationships that exist between measures, using symbols shown in Table 7. The additional rows appended to Matrix 3, as depicted in Fig. 7, are described in Tables 8.

In Matrix 3, if a measure complements (or conflicts) another measure, then notation "O" (or "X") is placed at their corresponding cell (i.e. intersection of corresponding row and column), as defined in Table 7.

At the end of relationship analysis, the total number of supports and conflicts for each measure are recorded at the bottom of the matrix. If there are any conflicts, they have to be analysed and solved by returning to Matrix 2 and modifying the list of selected measures, and then repeating relationship analysis using Matrix 3.

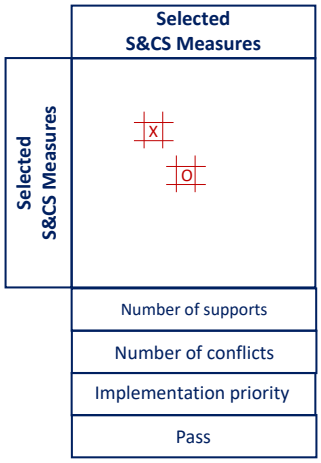


**Figure 7: Matrix 3.**

**Table 7: Symbols used in Matrix 3 to denote the relationships between measures**

| Symbol | Definition |
|---|---|
| X | The measure (row header) is conflicted by another measure (column header). |
| O | The measure (row header) is supported by another measure (column header). |

**Table 8: Description of the additional rows of Matrix 3**

| Row | Description |
|---|---|
| Number of supports | Each cell must show the number of "O" Matrix column (in Matrix 3) contains. |
| Number of conflicts | Each cell must show the number of "X" its corresponding column (in Matrix 3) contains. |
| Implementation priority | Each cell must contain a number that signifies the degree of priority of the corresponding measure. For example, 1 means highest priority; the greater the number, the lower the priority. The degree of priority is determined according to the risk levels of the requirements that can be satisfied by the corresponding measure. |
| Pass | The cell must be marked with a tick, if the corresponding measure is judged to be acceptable. The judging criteria are: i) the balance between corresponding *Number of supports* and *Number of conflicts*; ii) the corresponding priority. |

The number of supports ("O") in Matrix 3 shows the overlaps among measures. It could help identify redundant measures. The analysis is concluded using "Pass" row (see Tables 8 for more details).

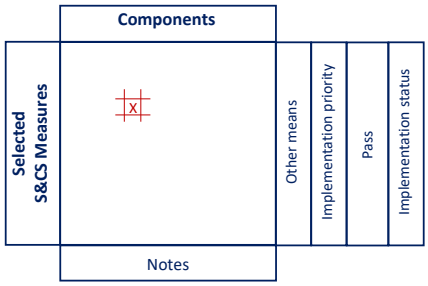


**Figure 8: Matrix 4.**

**Table 9: Symbols used in Matrix 4 to denote the relationships between measures and components**

| Symbol | Definition |
|---|---|
| X | The component is required for implementing the measure. |

**Table 10: Description of the additional row of Matrix 4**

| Row | Description |
|---|---|
| Notes | Each cell may include properties of the corresponding component, which are deemed worth mentioning – e.g. constraints and limitations. |

## 3.4 Matrix 4

Matrix 4 is aimed at recording and tracking the implementation status of safety and security measures, selected for implementation in Matrix 3. Matrix 4 is constructed in AVES Stages 3 and 6. While construction of Matrix 4 may be skipped in AVES Stage 3 if implementation details are unavailable, it must be performed in AVES Stage 6 so that the SCSD Model could be built in Stage 7.

The S&CS measures (acquired from Matrix 3) and the ADS components (such as hardware and software) are to be row headers and column headers of Matrix 4 respectively, as shown in Fig. 8. This matrix serves to capture the relationships that exist between measures and components, using symbols shown in Table 9. The additional rows and columns appended to Matrix 4, as depicted in Fig. 8, are described in Tables 10 and 11 respectively.

Note that not all the measures are related to software or hardware components. Some of them might be implemented using other means, e.g. activities, which have to be described in "Other means" column of Matrix 4.

This matrix can be used when preparing for measure implementation, as well as during the implementation process. During preparation phase, it is a useful tool for making decision on software/hardware component selection for measure implementation. The results are recorded in "Pass" column, as described in Table 11. During implementation phase, Matrix 4 can help to track current status of implementing each measure. "Implementation priority" column shows which measures should be implemented first, while

**Table 11: Description of the additional columns of Matrix 4**

| Column | Description |
|---|---|
| Other means | Describes other means, e.g. activities, used to implement measures. |
| Implementation priority | This column is the transpose of row "Implementation priority" of Matrix 3. |
| Pass | The cell must be marked with a tick if the corresponding measure has been assigned appropriate component(s) to make it viable. |
| Implementation status | Each cell must contain a percentage value (e.g. 0-100%) that represents the progress of implementing the measure. The entire column is to be periodically updated. |

"Implementation status" indicates the progress of implementing each measure (see Table 11 for more details).

### 3.5 SCSD Model

The fifth matrix is the the meta-matrix – SCSD Model, which incorporates Matrices 1-4 into one model, as shown in Fig. 4. SCSD Model is constructed in AVES Stage 7 at the end of AV product development phase, using the data of Matrix 1 from AVES Stage 5, and Matrices 2-4 from AVES Stage 6.

As mentioned in Section 2, SCSD Model is particularly useful in production, operation, service, and decommissioning phases of AV development lifecycle, when the detailed information from concept and product development phases is no longer available. In these phases, SCSD Model could be used to provide a sufficient amount of information required for S&CS analysis.

There is a similar model, Six-Step Model (SSM), proposed in [15] for analysis of safety and security of cyber-physical systems, by utilizing a collection of matrices to model the interrelationships among six different dimensions of CPS – i.e. functions, structure, failures, safety countermeasures, attacks, and security countermeasures.

We performed a case study, in which we constructed SSM of an AV. The findings of the case study revealed that construction of SSM was time consuming and some of the information, captured in SSM, was redundant. We used these findings as an input for developing SCSD Model.

The SSM is a more complex model compared to SCSD Model; SSM requires 6 hierarchies while SCSD Model – 3 hierarchies; SSM is composed of 21 relationship matrices while SCSD Model – 4 relationship matrices. Furthermore, SSM is not tailored to fit the AV development lifecycle.

## 4 SUMMARY AND CONCLUSIONS

This paper proposes a novel approach, AVES Framework, for unified, systematic, model-based AV safety and cybersecurity analysis.

AVES Framework adheres to road vehicle development lifecycle, and it may be used to analyze any AVs regardless of their automation and connectivity levels. To the best of authors' knowledge, there are no similar approaches proposed yet.

Another novel point of this work is using principles of QFD for safety and cybersecurity analysis, in particular, for relationship analysis and decision making with respect to safety and cybersecurity requirements, safety and security measures, and system components. Four relationship matrices and a meta-matrix, SCSD Model, are constructed throughout the stages of AVES Framework.

This is an initial paper including an overview of AVES Framework's stages and models. Further work will include detailed description and validation of the AVES Framework.

## REFERENCES


[1] 2016. *SAE J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems.* SAE International.

[2] 2016. *SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.* SAE International.

[3] Under development. *ISO/SAE AWI 21434, Road Vehicles – Cybersecurity engineering.* International Organization of Standardization, ISO.

[4] C. W. Axelrod. 2017. Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles. In *2017 13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT).* 1–6. https://doi.org/10.1109/CEWIT.2017.8263141

[5] C. W. Axelrod. 2017. Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks. In *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT).* 1–6. https://doi.org/10.1109/LISAT.2017.8001966

[6] L. Cohen. 1995. *Quality Function Deployment: How to Make QFD Work for You.* Addison-Wesley. https://books.google.com.sg/books?id=3wBUAAAAMAAJ

[7] M. Hashem Eiza and Q. Ni. 2017. Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. *IEEE Vehicular Technology Magazine* 12, 2 (June 2017), 45–51. https://doi.org/10.1109/MVT.2017.2669348

[8] ISO 20077 2017. *Road Vehicles – Extended vehicle (ExVe) Methodology* (2 ed.). Standard. International Organization for Standardization.

[9] ISO 26262 2018. *Road Vehicles – Functional Safety* (2 ed.). Standard. International Organization for Standardization.

[10] ISO/PAS 21448 2019. *Road Vehicles âĂŞ Safety of Intended Functionality* (1 ed.). Standard. International Organization for Standardization.

[11] I. Ivanov, C. Maple, T. Watson, and S. Lee. 2018. Cyber security standards and issues in V2X communications for Internet of Vehicles. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018.* 1–6. https://doi.org/10.1049/cp.2018.0046

[12] Nancy G. Leveson. 2012. *Engineering a Safer World: Systems Thinking Applied to Safety.* The MIT Press.

[13] Shih-Chieh Lin, Yunqi Zhang, Chang-Hong Hsu, Matt Skach, Md E. Haque, Lingjia Tang, and Jason Mars. 2018. The Architectural Implications of Autonomous Driving: Constraints and Acceleration. *SIGPLAN Not.* 53, 2 (March 2018), 751–766. https://doi.org/10.1145/3296957.3173191

[14] Jonathan Petit and Steven E Shladover. 2015. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems* 16, 2 (2015), 546–556. https://doi.org/10.1109/tits.2014.2342271

[15] G. Sabaliauskaite, L. S. Liew, and F. Zhou. 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 (June 2018), 160–169.

[16] TR 68 2019. *TR 68. Autonomous vehicles. Parts 1-4.* Technical Reference. Enterprise Singapore.