Security Assurance Cases for Road Vehicles: an Industry Perspective

Mazen Mohamad  
University of Gothenburg  
Gothenburg, Sweden

Alexander Åström  
Volvo Cars  
Gothenburg, Sweden

Örjan Askerdal  
AB Volvo  
Gothenburg, Sweden

Jörgen Borg  
Volvo Cars  
Gothenburg, Sweden

Riccardo Scandariato  
University of Gothenburg  
Gothenburg, Sweden

ABSTRACT

Assurance cases are structured arguments that are commonly used to reason about the safety of a product or service. Currently, there is an ongoing push towards using assurance cases also for cybersecurity, especially in safety critical domains, like automotive. While the industry is faced with the challenge of defining a sound methodology to build security assurance cases, the state of the art is rather immature. Therefore, we have conducted a thorough investigation of the (external) constraints and (internal) needs that security assurance cases have to satisfy when used in the automotive industry. This has been done with 28 participants and in the context of two large automotive companies located in Europe: Company A is a passenger car manufacturer, while Company B is a truck manufacturer. An extended version of this paper is available online at https://arxiv.org/abs/2003.14106.

CCS CONCEPTS

• Security and privacy → Software security engineering.

KEYWORDS

security, assurance cases, automotive

1 INTRODUCTION

Similarly to safety, a security assurance case (SAC) can be described as a structured set of arguments that are supported by evidence, e.g., collected from the results of the validation and verification activities [4]. In our analysis of the literature, we have found that the related work has not investigated the constraints and requirements around high-impact technical decisions such as how to structure a security case, how to collaborate with suppliers on security cases, how to effectively update a security case, and so on. This work is motivated by the urgency that is perceived by the automotive industry with respect to implementing security cases, due to the emergence of several standards and regulations and the necessity for compliance. We call these the external drivers that impose constraints on how SAC should look like. Accordingly, we formulate the first research question as: RQ1 – What are the constraints for SAC coming from regulations and standards in the automotive markets of EU, US, and China? The development of a strategy for SAC is also perceived by the automotive companies as an opportunity to improve their cybersecurity development process. Also, such methodology should integrate with the product life-cycle. As such, we have investigated these internal drivers. Accordingly, we formulate the second research question as: RQ2 – What are the needs and opportunities related to SAC in the automotive industry?

In a collaboration between one academic institution and two OEMs, we have performed a study to answer the above research question. Accordingly, this paper has two main contributions. First, we have performed a systematic study of the security-relevant regulations and standards in the automotive domain. In this analysis, we have identified the explicit and implicit constraints laid out by such documents with respect to security cases. The analysis is performed by a pool of industrial security experts (working in two panels) who are also members of several standardization committees and, hence, know how to interpret these documents, which are, at times, somewhat fuzzy. Second, we have performed an empirical study with a significant number of stakeholders that are affected either directly (e.g., as prospective producers) or indirectly (e.g., as prospective consumers) by security cases. By applying rigorous methods from the field qualitative research, we have systemati-

2 RESEARCH METHODOLOGY

As shown in Table 1, this study involved a total of 28 participants. RQ1. Concerning the analysis of the standards and regulation, Company A maintains a knowledge base of relevant documents as part of their security governance framework. This knowledge base consist of standards, regulations, guidelines, best practices, etc applicable for various markets. Furthermore, this knowledge base
covers both current and upcoming trends. Such knowledge base is fairly complete, at least for the most relevant markets (e.g., US, EU, China), and represented the pool of documents we have analyzed in order to answer RQ1. In particular, in this study we prioritize new regulations and standards that will soon come into effect and focus on the markets mentioned above. The filtered documents have been analyzed for explicit references to security assurance cases or their parts. We also looked for implicit relationships to SAC.

RQ2. To understand the internal needs for security assurance cases in the automotive industry, we used a three-steps method.

Pre-study. The goal of the pre-study was to assess the overall industrial expectations with regards to SAC. In particular, the pre-study reflects the point of view of the security leaders in the two companies participating to this investigation. In each company and independently from each other, a panel of experts performed a series of brainstorming meetings. The goal of the brainstorming was to form a consensual opinion of how the SAC should 'look and feel', within each company and from the perspective of security people. The results of the two panels were compared and merged into a single list of requirements and constraints. The panels consisted of R&D personnel with expertise in both security and safety. As a consequence, these groups of people were very homogeneous and might not have been aware of the full spectrum of needs and expectations in their two large companies. Therefore, we decided to perform a larger study (comprising a workshop and a series of interviews), involving a larger and more diverse set of stakeholders.

Workshop. Due to resource constraints, the workshop was conducted at Company B only. We invited stakeholders from different backgrounds and different parts of the organization. In total, we had 12 participants and three moderators. We started the workshop with a presentation to introduce security assurance cases to the participant which did not have previous experience with them. We then divided the participants into three groups (that worked in parallel), making sure to spread similar roles and competences among the groups. We asked the groups to brainstorm for 45 minutes on usage scenarios for SAC, and to describe them as user stories, like “As a [role] I would use SAC for [usage]” [2]. We explicitly asked the participants to come up with real-life scenarios in the context of their company.

Prioritization and Interviews. At this step, we wanted to dig deeper and get a better understanding of the most important scenarios. Concerning the prioritization, we aimed at getting expert opinions on which usage scenarios are of most value to the company, from a security perspective. We sent out the scenarios collected from the workshop to 10 security experts and asked them to select the top five scenarios by assigning a rank from 1 to 5 to them, where 5 is assigned to the most valuable scenario for the company.

Afterwards, we selected the top five usage scenarios and identified a key stakeholder at company B for each. Finally, we conducted in-person interviews with these stakeholders. Note that at the interviews, a security expert from the company was also present as a facilitator of the discussion. The interviewees were selected based

| ID | Company | Role | RQ1 Analysis of docs | RQ2 Pre-study | Workshop | Prioritization | Interviews |
|----|---------|------|----------------------|--------------|----------|----------------|------------|
| 1  | Company A | Attribute Leaders | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2  | Company A | Regulatory experts | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3  | Company A | Safety experts | ✓ | ✓ | ✓ | ✓ | ✓ |
| 4  | Company A | Security R&D experts | ✓ | ✓ | ✓ | ✓ | ✓ |
| 5  | Company A | Product Owner Security | ✓ | ✓ | ✓ | ✓ | ✓ |
| 6  | Company A | Security Engineers | ✓ | ✓ | ✓ | ✓ | ✓ |
| 7  | Company B | Security expert | ✓ | ✓ | ✓ | ✓ | ✓ |
| 8  | Company B | Security expert | ✓ | ✓ | ✓ | ✓ | ✓ |
| 9  | Company B | Safety expert | ✓ | ✓ | ✓ | ✓ | ✓ |
| 10 | Company B | Security Engineer | ✓ | ✓ | ✓ | ✓ | ✓ |
| 11 | Company B | Software architect | ✓ | ✓ | ✓ | ✓ | ✓ |
| 12 | Company B | Principal Engineer | ✓ | ✓ | ✓ | ✓ | ✓ |
| 13 | Company B | Software Engineer | ✓ | ✓ | ✓ | ✓ | ✓ |
| 14 | Company B | Security Engineer | ✓ | ✓ | ✓ | ✓ | ✓ |
| 15 | Company B | Security Engineer | ✓ | ✓ | ✓ | ✓ | ✓ |
| 16 | Company B | Security Engineer | ✓ | ✓ | ✓ | ✓ | ✓ |
| 17 | Company B | Security Engineer | ✓ | ✓ | ✓ | ✓ | ✓ |
| 18 | Company B | Security expert | ✓ | ✓ | ✓ | ✓ | ✓ |
| 19 | Company B | Solution Train Engineer (STE) | ✓ | ✓ | ✓ | ✓ | ✓ |
| 20 | Company B | Solution Manager | ✓ | ✓ | ✓ | ✓ | ✓ |
| 21 | Company B | Functional Safety Assessor | ✓ | ✓ | ✓ | ✓ | ✓ |
| 22 | Company B | Component Owner | ✓ | ✓ | ✓ | ✓ | ✓ |
| 23 | Company B | Senior Legal Counsel | ✓ | ✓ | ✓ | ✓ | ✓ |
| 24 | Company B | Security expert | ✓ | ✓ | ✓ | ✓ | ✓ |
| 25 | Company B | Security Manager | ✓ | ✓ | ✓ | ✓ | ✓ |
| 26 | Company B | Security R&D | ✓ | ✓ | ✓ | ✓ | ✓ |
| 27 | University C | Researcher | ✓ | ✓ | ✓ | ✓ | ✓ |
| 28 | University C | Researcher | ✓ | ✓ | ✓ | ✓ | ✓ |
on the relevance of their expertise to the actors of the user stories in the corresponding usage scenarios. For example, the actor of one of our top usage scenarios is a legal risk owner, hence, we selected an interviewee who has extensive experience in law and has the role: senior legal counsel in Company B. In each interview, there was an interviewer (an author), an interviewee, and a security expert who acted as a discussion enabler (also an author). We recorded the interviews, and used the recordings to extract a transcript for each interview. These were then sent to the corresponding interviewees validation, and additional comments. We organized each interview into four parts, according to the following themes: (i) value – In the first part, we focus on the value that SAC might bring to the stakeholder in terms of, e.g., efficiency, and quality management; (ii) content and structure – The focus of this part is to get the interviewees’ technical opinions on how the content and structure of SAC should be, e.g., in terms of level of detail and types of claims; (iii) integration – This part is about understanding how SAC could be integrated with the current way of working, and whether it could fit in the current activities, or would require modifications to the process; and (iv) challenges and opportunities – The last part of the interview is about understanding the challenges and opportunities that the stakeholders foresee in applying SAC.

3 RQ1: EXTERNAL DRIVERS

The drivers include regulations, standards, best-practises, and guidelines. The intent of the analysis is to find the relation and the motivation of a SAC from these documents. We look at the current and upcoming documentation. We do not present a complete list, but rather look at the documents that may have a large impact on the industry. These are presented in Table 2.

Two of the analyzed documents explicitly mentions SAC: ISO/SAE 21434 DIS [5] and SAE J3061 [10]. The former gives requirements on a cybersecurity case and that it shall provide the arguments that cybersecurity is achieved. The latter states that a cybersecurity case provides evidence and argumentation that design and implementation is sufficiently secure.

The Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution (SELF DRIVE) Act [7] contains requirements stating that a Cybersecurity plan that includes various security activities shall be developed. It thus implies that it shall be possible to show that the plan also has been implemented. The SAC shall therefor contain the corresponding evidence and argumentation of how the security plan has been met, including confidence in process for incident handling. Similarly, for the Automated Driving Systems (ADS 2.0) [6] it is beneficial to show evidence that cybersecurity processes are followed and show that the company adheres to industry best practice. The authors of the (ADS 2.0) document encourage documentation of how cybersecurity has been reached, including design choices, analyses, testing, etc. The SAC shall therefor cover these aspects. The Automated Vehicles 3.0 [15] also indicates the benefit to show evidence that cybersecurity processes are followed and show that the company adheres to industry best practice, including design principles and incident handling. The SAC shall therefor contain the corresponding evidence and argumentation of how security has been considered and handled during design and confidence in processes for incidence handling.

There is a current initiative on UN level, prepared by a subgroup of the working group on Intelligent Transport Systems / Automated Driving (IWG ITS/AD) of WP.29, referred to as “UN Task Force on Cyber security and OTA issues” (TF-CS/OTA), to establish regulations and type approval on Cybersecurity for vehicles that includes vehicle categories: M (standard passenger vehicles) and N (trucks). This include “Regulation on uniform provisions concerning the approval of cyber security” [13] and “Regulation on uniform provisions concerning the approval of software update processes” [14]. For the former it can be seen as highly beneficial to show compliance and conformance to requirements in the regulation concerning process implementation and fulfillment as well as demonstration of performed verification activities and its outcome. The SAC shall therefor contain evidence and argumentation in regards to confidence in the implemented processes that shall cover the life-cycle of the vehicle to maintain an appropriate level of security. As well as product evidence and argumentation of an adequately secure product. The latter one contain requirements for demonstration of evidence of a secure update process. The SAC shall therefor contain evidence and argumentation in regards to confidence in the SW update processes in order to maintain an adequately secure product and acceptable level of risk.

For the privacy related documents (General Data Protection Regulation (GDPR) [3]; Security and Privacy in Your Car (SPY CAR) Act [8]; Chinese Information Security Technology – Personal Information Security Specification GB/T 35273 [11]; and California Consumer Privacy Act [12]), SAC can be beneficial in regards to showing compliance to regulation, processes, methods and technologies to secure handling of data. The SAC shall therefore contain evidence and argumentation in regards to confidence in both processes and implementation measures for handling private data.

SAC can also be beneficial in the China Cyber Security Law (CSL) [9] to show that the organization has sufficient policies and processes that handle cybersecurity. Including incident handling and secure handling of private data. The SAC shall therefor contain evidence and argumentation in regards to confidence in the post-production processes. The CSL is a high level law and more detailed requirements will exist through the Chinese strategy and framework on Intelligent and Connected Vehicles (ICV) [1]. With the same reasoning it can be beneficial with the ICV in regards to showing compliance and conformance to requirements and processes, methods and design/technology. The SAC shall therefor contain evidence and argumentation of confidence in the implemented measures and processes to maintain an adequately secure product and acceptable level of risk.

4 RQ2: INTERNAL NEEDS

4.1 Pre-study: Expectations of Security Leaders

The panels of security experts concluded that the internal needs of an OEM in regards to the use of security cases can be summarized as follows.

Secure product argumentation. Need to have an argumentation for adequately secure implementations of HW/SW E/E systems in their vehicle throughout their life-cycle. This can be used, among other things, to make release decisions.
Supporting evidence. The evidence should undergo a quality assurance process and should cover all the relevant parts included in the development, with sufficient detail for the critical parts.

Legal compliance. Comply to the legislation, regulations and type approvals on national and international levels, in order to be allowed to sell vehicles.

Supply chain. Manage collaboration between OEM and suppliers in terms of requirements, structure, aggregation and level of details for SAC constituents.

Standard conformance. Conform to standards, guidelines and best practices and implement state of the art processes and methods (in order to be competitive w.r.t. other OEMs).

Process harmonization. Existing development processes (e.g., agile) and product organization need to be harmonized with the processes and methods required by SAC.

4.2 Workshop to Identify Usage Scenarios

The workshop participants identified thirteen unique usage scenarios (US), which are listed below. These scenarios depict, in a narrative form, the broader set of needs and expectations of an OEM with respect to SAC. These scenarios cover a diverse set of stakeholders (10 different roles) within the OEM large organization. They also span over multiple phases of an automotive product’s life-cycle, which are: Requirements (US2, US9), Design (US4, US7), Development (US5, US8, US11), Testing (US3, US6, US10), Sales (US1), and Maintenance (US12, US13).

US 1 As a salesman, I would use top-level SAC to prove to our customers that the company has considered all relevant security aspects of the final product, and has enough evidence to claim that it has fulfilled them.

US 2 As a member of the compliance team, I would use detailed SAC to prove to authorities that the company has complied to a certain standard, legislation, etc., and show them evidence of my claim of compliance.

US 3 As a project manager, I would use SAC to make sure that a project is ready from a security point of view to be closed and shipped to production.

US 4 As a project manager, I would include SAC in my project plan. I would make sure the project has the needed resources and time for creating the case (argumentation, evidence collection, etc.).

US 5 As a project would use SAC to monitor the progress of my project when it comes to fulfillment of security requirements.

US 6 As a product owner, I would use SAC to make an assessment of the quality of my product from a security perspective, and make a roadmap for future security development.

US 7 As a product owner, responsible for handling threats and vulnerabilities, I would use SAC to evaluate the effect of new threats and vulnerabilities, and evaluate whether a change is needed.

US 8 As a member of the purchase team, I would include SAC as a part of the contracts made with suppliers, in order to have evidence of the fulfillment of security requirements at delivery time, and to track progress during development time.

US 9 As an action owner, I would use detailed and visual SAC to communicate with the risk owner, and decide how to update the product security in the right way (to know what to do)

US 10 As a system leader, I would use SAC to make an assessment of the quality of my system from a security perspective, and make a roadmap for future security development.

US 11 As a software developer, I would use SAC from previous similar projects as a guideline for secure development practices.

US 12 As a legal risk owner, I would use SAC in court if a legal case is raised against the company for security related issues. I would use the SAC to prove that sufficient preventive actions were taken.

US 13 As a member of the corporate communication team, I would use SAC as a reference to answer security related questions.

4.3 Prioritisation of Scenarios and Interviews

After the workshop, we sent the scenarios to experts and asked them to prioritize them based on the value the scenarios provide to the company. The result of the prioritization task is: US2 (33
The interviewees said that today, the security assurance in projects is mostly based on experience, and is done by providing evidence such as test reports for some claims. These claims are derived from projects’ requirements that are not put together in a structured way. The interviewees also stressed that what is done today is simply not sufficient given the rapid evolution of connectivity in the vehicles. Historically there has been “a trust in the physical shell (the cab) around the items in the vehicle,” but today these items are connected to the outside world, and can be a target for cyber attacks.

As per the interviewees, having SACs as a part of scoping projects, setting the milestones and deliverables, and connecting them to the development process, would be of great value to security assurance from a project management perspective. Additionally from a product point of view, having a holistic SAC which is updated by the related projects would give the product owner an understanding of how secure the product is at different time-points, e.g., after integrating changes from different projects.

Both interviewees agreed that SACs should be built on a product level rather than a project level. SACs should be integrated and built within projects, but only to contribute towards the product’s SAC. A product, however, may be big and complex, and may include items that are more interesting from a security perspective than others, e.g., Electrical Control Units (ECU) that are connected to the outside world in a vehicle. In this case there needs to be a severity assessment to focus on the right items.

The interviewees think that the SAC work can be integrated into the project manager’s and product owner’s work by capturing it in projects’ requirements. They emphasized that it is important to work on quality, e.g., security as a part of the development process, and not as a separate activity. The workload in the beginning will be high, but with time, there will be patterns that can be reused to build SAC with less effort.

When it comes to the challenges, the interviewees consider handling the complexity of the product (vehicle in this case), and finding right competences to be the main ones.

Interview on US2 – Compliance. The interview was conducted with a functional safety assessor who has a wide range of experience in compliance (participant 21 in Table 1).

“The security case can serve as an umbrella document for all the analysis documents. It can be used by an assessor to find the right documents in order to assess compliance to a standard.” (Participant 21)

In the current situation, the compliance team is only concerned with safety matters, as per the interviewee. The only involvement with security issues is when there is a breach which affects the product’s safety. The expectation is that SAC can serve as an umbrella document for all the analysis documents. Hence it can be used by an assessor to find related document to assess compliance to a certain standard.

The SAC should be created on a whole vehicle level, as per the interviewee. It needs, however, to be dividable in manageable pieces, i.e., pieces that can be managed by individuals. For compliance purposes, the authorities look at system level, hence, for every project that includes changes in the system, it is important to conduct an impact analysis to identify affected artefacts, and update the SAC accordingly.

How working with SAC can be integrated within the way of working of the compliance team depends much on how SACs are implemented. If they are integrated within the projects (as they should according to the interviewee), then the compliance team would have the responsibility of following them up throughout the project, as well as making sure that they are complete after the verification phase.

The interviewee considers the main challenge to be finding resources and competences to carry out the work related to creating, maintaining, assessing and supporting SACs.

Interview on US8 – Suppliers. The interview was conducted with a component owner in Company B, who is experienced in purchasing and working with suppliers (ID 22 in Table 1).

“[Working with SAC provides] An opportunity to catch up with suppliers, which in many cases have come further in thinking about security than the company.” (Participant 22)

Today, security assurance when working with suppliers is about making sure of the fulfillment of security requirement, and running test cases on a sample of the requirements. However, “there is an uncertainty to a large extent that the received software is secure”, as per the interviewee. However, safety critical functions, e.g., breaking, is handled differently. The suppliers are usually asked to show how requirements are broken down and implemented during regular review sessions, and in some cases provide safety cases, which are used to make sure the safety claims align with internal safety cases. The interviewee expects that SAC can be used in the same manner. Additionally, SAC can be used to communicate regarding security both with suppliers and internally, and as a supporting artifact for creating security requirements.

On the supplier’s side the cases should be built on the ECU level, followed by a threat-based level, according to the interviewee. Whereas the company-owned SACs should be on the complete vehicle level, and broken down to ECU level, which is contributed by the suppliers. An important aspect mentioned by the interviewee is the weighting of the claims based on severity.

Integrating SAC in the current way of working with suppliers would increase the workload, but there are no obvious conflicts, according to the interviewee. There is a need for tools to store, extract, and compare SACs. Additionally, a version handling tool is also required to keep track of the SACs and their changes. The interviewee also mentioned the need to use an exchangeable format when building the cases, on both ends (supplier and company), in order to compare and integrate them.
A challenge is to find and provide practical training on SAC in the industrial context. Another challenge mentioned by the interviewee is finding competent resources to SAC related work. The interviewee emphasized that based on the experience from safety, even when there is education about the cases, it was much more complicated when actual work was done.

*Interview on US12 – Legal.* The interview was conducted with a senior legal counsel at Company B (participant 23 in Table 1).

“An evidence based structured approach to argue about security would definitely be used as evidence in court.”

(Participant 23)

In the current situation, the company has not had any legal case for security related issues, but there have been functional-safety related cases claiming that feature malfunctioning have caused accidents. Current evidence used in court for these kinds of legal cases are of two types: (i) usage of technology according to an acceptable standard; (ii) implementations of the used standards and technologies are correctly done (this should be certified by a third party assessor). Hence, if the ISO 21434 [5] becomes an industry standard, then it can be used as an evidence in court. However, it is very important to assure the quality of the case when it comes to completeness in the argumentation and evidence. The SAC used as an evidence will be available to the opponents, and it could be exploited to find holes and error to be used against the company.

The granularity needed for the SAC depends pretty much on the legal case according to the interviewee. However, there is a need to create SACs for complete vehicles, and views that could be broken down. This is to avoid cases where a legal case against the company involves a composition of systems (end-to-end function), and SACs are created for a subset of these systems.

The creation of SACs should, from a company perspective, be during development to assure security, according to the interviewee. However, from a legal perspective, SACs can be created once a legal case is filed, but that would increase the risk of having insufficient evidence, as it would be harder to locate and assign them. Moreover, from a liability perspective, it is much better to create the SAC proactively.

As per the interviewee, if SACs are to be used as evidence, the relevant stakeholders in the company will be reached out and asked to provide the SACs when needed. Then the legal responsible will have meetings with the stakeholders to understand it. This means that the ownership of the SACs would not be the responsibility of the legal responsible, even if it is created specially for a legal case. The legal responsible would be a user of the SAC.

At the end, the interviewee stressed that introducing a structured way of security assurance “can lead to creating better systems which can protect the company from issues from regulators and third parties.” However, there has to be a buy-in on different levels in the company in order to do this in a correct way.

5 THREATS TO VALIDITY

In terms of external validity, we are aware that the general validity of our results could be limited to the companies involved in the study, and the results might not directly translate to companies with a different culture. However, the involved companies are of high profile, quite large and compete at the international level. Therefore, they are able to provide a quite broad perspective on the entire automotive industry.

In terms of internal validity, the selection of the standards and regulations investigated in RQ1 could have been incomplete. However, we are confident we are addressing the most important documents, especially for the mentioned markets. Further, in the prioritization of the scenarios of RQ2, there is a risk that the selection of the top scenarios was biased by present market pressure towards compliance to the upcoming standards. Finally, elements of bias could be have been introduced via the selection of the participants.

6 CONCLUSION

In this study, we have analyzed the requirements around the use of security cases in the automotive domain. In particular, we have listed the constraints coming from standards & regulations and have identified the internal needs of OEMs. In future work, we are addressing the requirements identified in this paper by means of a systematic methodology to create security cases for the automotive industry. We are also interested in extending this work with a survey including a larger group of automotive companies and automotive security experts.

ACKNOWLEDGEMENT

This work is partially supported by the CASUS research project funded by VINNOVA, a Swedish funding agency.

REFERENCES

[1] Chinese Ministry of Industry and Information Technology (MIIT) and the Standardization Administration of China. 2018. Intelligent and Connected Vehicles.
[2] Mike Cohn. 2004. *User stories applied: For agile software development.* Addison-Wesley Professional.
[3] European Union. 2016. General Data Protection Regulation (GDPR) 2016/679.
[4] John Goodenough, Howard Lipson, and Chuck Weinstock. 2007. *Arguing Security: Creating Security Assurance Cases.* Technical Report. SEI CMU.
[5] International Organization for Standardization and Society of Automotive Engineers. 2019. ISO / SAE 21434 Road vehicles – Cybersecurity engineering, DIS Draft.
[6] National Highway Traffic Safety Administration (NHTSA). U.S. Government. 2017. DOT HS 812 442 - ADS 2.0 (Automated Driving Systems).
[7] National Highway Traffic Safety Administration (NHTSA). U.S. Government. 2017. HR R 3388 - SELF DRIVE Act (Safety Ensuring Lives Future Deployment and Research In Vehicle Evolution Act).
[8] National Highway Traffic Safety Administration (NHTSA). U.S. Government. 2017. S. 680 - SPY Car Act of 2017 (Security and Privacy in Your Car Act of 2017).
[9] National People’s Congress (NPC) of the People’s Republic of China. 2016. The Cyber Security Law.
[10] Society of Automotive Engineers. 2016. J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.
[11] Standardization Administration of China. 2017. GB/T 35273-2017 Information security technology - Personal Information Security Specification.
[12] State of California. 2018. CCPA - Assembly Bill No. 375 - “California Consumer Privacy Act” - AB-375 Privacy: personal information: businesses”.
[13] UN Economic Commission for Europe (UNECE) WP.29 GRVA. 2020. Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of cybersecurity management systems.
[14] United Nations Economic Commission for Europe (UNECE) WP.29 GRVA. March 2020. Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to software update processes and of software update management systems.
[15] U.S. Government. 2018. DOT 2018-21840 - Preparing for the Future of Transportation Automated Vehicles 3.0. National Highway Traffic Safety Administration (NHTSA).