

# Requirements for a Cybersecurity Case Approach for the Assurance of Future Connected and Automated Vehicles

Luis-Pedro Cobos<sup>1,2</sup><sup>a</sup>, Alastair R. Ruddle<sup>1</sup><sup>b</sup> and Giedre Sabaliauskaite<sup>2</sup><sup>c</sup>

<sup>1</sup>*HORIBA MIRA Limited, Watling Street, Nuneaton, U.K.*

<sup>2</sup>*Institute for Future Transport and Systems, Coventry University, Coventry, U.K.*


**Keywords:** Assurance, Automotive, Connected and Automated Vehicles, Cybersecurity Case, Vehicle Cybersecurity.


**Abstract:** Cybersecurity is an issue of increasing concern for emerging connected vehicles. Ensuring public trust in future connected and automated vehicles will require very high levels of confidence in their dependability, which will include cybersecurity assurance. In functional safety engineering, the safety case has become a widely used approach to describing and documenting safety assurance arguments and their supporting evidence. The use of a similar security case can also be considered in cybersecurity engineering, but there are significant differences between safety and cybersecurity. Cybersecurity impacts include, but are not limited to, possible safety issues. Furthermore, the cybersecurity threats arise from the ingenuity of human attackers, and available technology, with the result that they are constantly evolving. This paper proposes the use of an assurance case approach for cybersecurity and outlines the particular requirements that are considered to be necessary for the development of such a cybersecurity case.


## 1 INTRODUCTION

The connected car is not a thing of the future. Commercially, the industry is already rolling out connected vehicles with highly capable electronics and software to match. Furthermore, the driving functions are becoming increasingly automated, with the desired end-game being fully automated driving. These connected and automated cars are not simply computers on wheels as they must also be aware of obstacles (including other vehicles) and vulnerable road users (cyclists, pedestrians, etc.) in their environment. Software is increasingly key to enabling these technologies and offers the potential for through-life upgrades that will lead to future vehicles being in a state of evolution, rather than a static product. However, being close to a computer and being part of the Internet-of-Things introduces the potential for cybersecurity threats. As vehicles are also providing increasingly automated driving functions, some cybersecurity threats could result in adverse safety impacts.

Ensuring the public acceptability of connected and automated vehicles will require considerable confidence to be established in their cybersecurity and safety characteristics, as well as their basic functionality. Traditional methods of assuring key performance characteristics such as safety involve demonstrating compliance with a very specific and set of criteria using standardised methods before product launch. However, current trends such as the increasingly rapid pace of technological change, increasing system complexity, adoption of non-deterministic machine learning technologies, and through-life system modifications are making the traditional assurance model untenable. Moreover, cybersecurity is subject to the additional difficulty that the “operating environment” involves the ingenuity of human adversaries in seeking out vulnerabilities to exploit in order to attack normal vehicle operation. This, together with the interest in through-life software updates, leads to the conclusion that future vehicle assurance must become an ongoing process throughout the vehicle lifecycle, rather than a more limited procedure prior to product launch.

<sup>a</sup> <https://orcid.org/0000-0002-1333-7767>

<sup>b</sup> <https://orcid.org/0000-0003-4425-0979>

<sup>c</sup> <https://orcid.org/0000-0003-1183-7001>

Based on past experience from safety engineering, it is argued here that the best way to demonstrate this would be through the development of an assurance case for cybersecurity. Like a legal case, a safety case presents a justified and reasoned argument that the safety risks associated with using the vehicle are considered to be acceptable at product launch. A cybersecurity case would similarly argue that the cybersecurity risks associated with using the vehicle are deemed to be acceptable at product launch, and that appropriate measures are in place to ensure that any emerging threats can subsequently be identified, assessed and, where necessary, mitigated in a timely fashion.

This paper provides an overview of relevant technological trends within the automotive industry, primarily the expansion of wireless connectivity and the emergence of ongoing software updates for modifying vehicle functionality, as well as the merits and limitations of existing safety case techniques, in order to identify requirements for an analogous cybersecurity case to demonstrate cybersecurity assurance for future vehicles.

## 2 RELEVANT DEVELOPMENTS

This section outlines industry developments that are relevant to the requirements for a cybersecurity case.

### 2.1 V2X Communications

A connected car is a vehicle capable of communicating bidirectionally with other systems outside of the car. Connected car protocols are known collectively as Vehicle-to-everything (V2X) or Car2X and C2X (Cui, 2019). There are two types of application of V2X:

- Single vehicle applications: this type of application concerns information obtained for the vehicle to use by itself.
- Cooperative safety and efficiency applications: these are use cases in which a vehicle learns something that it could also potentially communicate to another vehicle or entity for their benefit.

The concept of V2X encompasses a wide range of interactions, as illustrated in Figure 1. The original purpose of V2X was to increase the safety of the vehicle by expanding its field of vision to more than just what it perceives with vehicle-based sensors in the immediate surroundings, into a wider vision through connecting with other information systems (Wang, 2018). V2X will probably be a standard safety feature in the coming years (Macher, 2017).



Figure 1: Examples of V2X technologies.

Some examples of V2X applications are listed in Table 1, including description of their potential benefits and the communication channels used for these applications. This shows that, even if 5G seems like the option that has the most followers, there are also other ways to achieve communication.

Table 1: Example uses of V2X applications.

Applications	Potential Benefits	Channel Models
<b>Road Safety</b>	<ul style="list-style-type: none"> <li>• Collision avoidance (safe distance)</li> <li>• Road sign notifications (curve speed warning)</li> <li>• Incident management (emergency vehicle warning)</li> </ul>	<ul style="list-style-type: none"> <li>• DSRC</li> <li>• WAVE</li> <li>• Wi-Fi</li> <li>• Cellular Network</li> </ul>
<b>Traffic Management</b>	<ul style="list-style-type: none"> <li>• Traffic management (intelligent traffic flow control)</li> <li>• Road monitoring (vehicle tracking)</li> </ul>	<ul style="list-style-type: none"> <li>• DSRC</li> <li>• WAVE</li> <li>• Cellular Network</li> <li>• ZigBee</li> </ul>
<b>Comfort and Infotainment</b>	<ul style="list-style-type: none"> <li>• Entertainment (music-audio download)</li> <li>• Comfort (parking booking)</li> </ul>	<ul style="list-style-type: none"> <li>• DSRC</li> <li>• WAVE</li> <li>• Cellular network</li> <li>• WiMAX</li> </ul>

Current V2X implementations are summarized in Table 2 below, which also indicates some of the associated challenges.

Table 2: Current status of V2X technologies.

V2X Technologies Status	
Current Implementations	Current Challenges
<ul style="list-style-type: none"> <li>• Downloading of maps, weather data, and accident notifications</li> <li>• Health of electromechanical components through CAN</li> <li>• Emergency call system (e-call)</li> <li>• Connection between mobile phone and vehicle user interface</li> <li>• Connection between vehicles</li> <li>• Connection to traffic signal database</li> <li>• Management of electric vehicle charge/discharge to the grid</li> </ul>	<ul style="list-style-type: none"> <li>• The infrastructure (for V2I) is not been built or is not widespread</li> <li>• The cellular network connection should be independent of the e-call system</li> <li>• Availability of access in remote or relatively unpopulated areas</li> <li>• Cybersecurity issues such as future proofing, data integrity protection, access control, and detection and prevention of attacks</li> </ul>

Wireless connectivity offers great benefits in terms of improved services and functionality. However, it also opens the vehicle up to a wide range of potential cybersecurity threats.

## 2.2 Driving Automation

Vehicle systems comprise a number of Electronic Control Units (ECUs) that are tasked with controlling a specific vehicle function or a particular set of functions. These ECUs communicate with each other through a central gateway unit linked to a number of different buses (like CAN or LIN) that allow communication flows within different domains.

These electronic control capabilities are now being combined with advanced sensor technologies and information obtained from V2X communications in order to automate driving tasks. At present this is mostly in the form of advanced driver assistance systems (such as parking assistance, adaptive cruise control, lane keeping assistance etc.). However, the expected end game is full automated driving under all road conditions.

Driving automation offers significant benefits to society in removing the potential for human error, which is the main cause of road accidents. However, it also opens the vehicle up to a wide range of potential cybersecurity threats.

## 2.3 Software Updates

Nowadays, even everyday vehicles contain software that is updated, such as infotainment systems or digital cockpits. We can summarize the main reaches of software updates as:

- **Customer:** Device interaction (smart phones, tablets) or User Interface.
- **Cloud:** Connection to online servers for satellite and weather info or connecting to a 5G network for road data.
- **Service and Repair:** Fault diagnosis or the addition of new features.
- **Management:** Provision of administration data, manufacturing distribution notes, and IT security.

These updates can be more frequent, efficient and faster (due to smaller size) if they are done by connecting online and installing in the background.

An Over-The-Air (OTA) update is the wireless delivery of new software or data to a device. The conditions to achieve and perform a wireless Software (SW) update requires the Diagnostic Tester, an element possessing the current and newer software versions and all required keys to authorize the update, to connect the vehicle to the OEM using automotive diagnostic protocols such as Unified Diagnostic Services. The remaining process comprises three steps (Steger, 2018):

- i. Initialize the update process and validate and authorization for the update.
- ii. Transfer the binary to the ECU.
- iii. Override and flash the ECU.

These steps normally happen locally and remotely in an authorized garage or a service centre, using Wi-Fi (Shavit, 2007).

The greatest challenge of software updates is how to make them secure. There are two main ways to do so; namely, the blockchain and certificate-based approaches. Both approaches seem to have similar properties with respect to the added latency as well as the total number of packets exchanged (Steger, 2018). The certificate-based approach uses a certificate to check the keys and updates depends on whether the certificate is signed or unsigned. The blockchain algorithms are well known in cryptocurrency and video game matchmaking applications. They work by appending new data blocks into each existing data block, thus decentralizing the process while changing and reallocating the need of private keys.

Through-life software updates offer great benefits in terms of improved service and functionality. In addition, they allow the implementation of patches that may be needed to ensure ongoing vehicle safety and cybersecurity. This points to the need for cybersecurity assurance to become an on-going process throughout the operational life of the vehicle, rather than the conventional, largely pre-launch, activity.

## 3 VEHICLE CYBERSECURITY

A connected car becomes a target for cyber security threats, and although safety is an important consideration in relation to cybersecurity threats, cybersecurity has a much wider scope than safety alone. Deliberate attacks on vehicle data may also have other potential implications, such as:

- infringement of privacy (including Intellectual Property Rights protection);
- possible economic aspects, such as fraudulent financial transactions;
- the loss of availability for key functions that, although not safety-related, are nonetheless regarded as mission-critical for the vehicle.

Various types of security attack that could be deployed against vehicles are summarized in Table 3.

Table 3: Main types of cybersecurity attacks applied against vehicles.

Types of Cyber Security Attacks			
Authenticity	Availability	Integrity	Confidentiality
<ul style="list-style-type: none"> <li>• Sybil Attack</li> <li>• Falsified Entity Attack</li> <li>• Replication Attack</li> <li>• Injection or Spoofing Attack</li> <li>• Timing Attack</li> </ul>	<ul style="list-style-type: none"> <li>• Jamming Attack</li> <li>• Flooding Attack</li> <li>• Malware Attack</li> <li>• Spamming Attack</li> <li>• Wormhole Attack</li> </ul>	<ul style="list-style-type: none"> <li>• Masquerading Attack</li> <li>• Replay Attack</li> <li>• Data Alteration/Tampering Attack</li> <li>• Location Poisoning Attack</li> </ul>	<ul style="list-style-type: none"> <li>• Eavesdropping Attack</li> <li>• Interception Attack</li> </ul>

### 3.1 Potential Threats

The main threats of cybersecurity are authenticity, availability, data integrity, and confidentiality. Authenticity or identification means data was generated by legitimate entities and the location matches, eventually ensuring integrity. Availability means information is provided as required in real time. Data integrity or data trust means no unauthorized alteration during generation or transmission. Confidentiality means that data are never disclosed to someone unauthorized (Cui, 2018).

A further consequence of cybersecurity concerns, as well as of increasing reliance on software controls, is that the need for software updates will become increasingly common. Furthermore, the ability to modify vehicle software could also be of interest as a new business opportunity, by providing the possibility of remote vehicle upgrades and/or differentiation, resulting in a “software defined vehicle”. However, software updates are also a potential source of new safety issues, as well as providing a further entry point into vehicle systems for malicious attackers.

As the deployment of wireless connectivity and environment sensors rises in automated vehicles, they are expected to become increasingly susceptible to faults and failures due to cyber-attacks. Such attacks may be achieved by external manipulation (e.g. jamming, spoofing, replay etc.) of sensor inputs, GNSS data, and V2X communications. Access to in-vehicle networks may also enable direct control of vehicle functions.

The increasing use of artificial intelligence (AI) technologies in support of automated driving systems brings unique vulnerabilities, for both safety and cybersecurity, that have yet to be adequately resolved. For example, corruption of the training data for AI systems is a conceivable attack.

### 3.2 Standards and Regulations

Preliminary recommendations relating to vehicle cybersecurity are already available (e.g. SAE J3061,

which recommends a risk-based approach) and more comprehensive regulations and standards are currently emerging or under development.

Type approval regulations concerning cybersecurity have recently been published (UNECE Regulation 155), which include requirements for vehicle cybersecurity risk analysis and an associated cybersecurity management system, while intentionally avoiding any mandate on specific technical measures. This approach is therefore goal-based (see section 4.2), requiring the demonstration of achievement of a goal described in terms of risk using any suitable methods, rather than the traditional prescriptive assurance method (see section 4.1) of requiring compliance with particular performance criteria using specified methods.

In response to the emergence of Regulation 155, the automotive cybersecurity standard ISO/SAE 21434 is currently under development, with formal issue expected by mid-2021. Created to take in account the trend towards greater networking of vehicles and the focus on embedded platforms, the standard addresses the protection of vehicles from threats associated with the classic IT environment. This standard covers the entire development process and life cycle of a vehicle, in a similar way to the functional safety standard ISO 26262 and ISO/PAS 21448 for Safety of The Intended Functionality. The ISO/SAE 21434 standard similarly recommends a structured threat analysis and risk assessment.

In addition, it is anticipated that by 2025 consumer tests like NCAP (New Car Assessment Program) will also expect a certain level of cybersecurity to be demonstrated by manufacturers.

## 4 DEPENDABILITY AND ASSURANCE

In order for connected and automated vehicles to be successfully adopted there is a need to establish public trust in them. To be trusted they need to be dependable, and their dependability needs to be assured. In this context dependability is the ability to perform (i.e. deliver the required functionality, safely and securely), as and when required (Ruddle, 2020). Assurance is the set of justifiable grounds for confidence that the risks of using a product, process or service are acceptable to the stakeholders.

### 4.1 Prescriptive Assurance

The traditional approach (Kelly, 2005) to product assurance is highly prescriptive, based on standards

that detail not only the required performance criteria, but also specifying exactly how performance is to be demonstrated. Establishing assurance is then a simple case of demonstrating compliance with standards.

Prescriptive assurance approaches may be applied either to specific product features or to associated development processes:

- **Product Assurance Standards** generally detail specific performance criteria that are required, as well as how they are to be demonstrated, and therefore reflect specific technologies, designs or features. Achieving assurance is then based on demonstrating compliance of the products with these requirements.
- **Process Assurance Standards** describe features of the process that is to be used in producing a product, rather than specific performance criteria or design features. Assurance is then based on establishing whether the process was followed, and often on the quality of the process and its outputs.

For the automotive industry, type approval within Europe and many other territories is achieved by demonstrating compliance with UNECE regulations.

This type of approach is well-known and understood, with clear advantages in terms of simplicity and transparency. It is very well suited to relatively simple systems with few functions. However, the prescriptive approach becomes increasingly difficult as the complexity of the target system rises, resulting in a richer set of functions and such large numbers of states that comprehensive testing is no longer a practicable option. In addition, this approach can lead to an excessive focus on simply passing the test, which can lead to the exclusion of wider considerations that the spirit of the test is intended to be representative of, or even fraudulent activity, as discovered in the recent scandal concerning gaseous diesel engine emissions.

A further limitation is that the prescriptive approach is inevitably technology-centric, since it aims to specify the details of how and what are required to be done. This makes it difficult for prescriptive standards and regulations to adapt to new technology, since the acceptance criteria and validation methods are so closely related to the anticipated technology of the product. As different technological solutions emerge, the number of standards and regulations must multiply to accommodate the newer options. This rising number of standards may be further multiplied by territorial differences. As the pace of technological change is becoming increasingly rapid, the standards management burden of the prescriptive approach will

become increasingly unmanageable unless a more efficient alternative is used to limit the need for changes more effectively.

## 4.2 Goal-based Assurance

The limitations of the prescriptive approach have resulted in the emergence of an alternative assurance approach more recently, which is based on specifying more generic goals that are to be achieved (Kelly, 2005). These goals are technology-agnostic and are often specified in terms of risk. The goal-based approach is less straightforward to apply than prescriptive methods, as it requires the construction of a specific justification of compliance, the merits of which must be judged.

The goal-based assurance approach is more readily comprehended using the notion of claim-argument-evidence. Based on approaches developed in the analysis of structured argument styles (Toulmin, 1958), justification for achievement of the goal should be shaped using the following elements:

- **Claims**, assertions that are not immediately self-evident, but must be judged on the quality of the supporting argument and evidence.
- **Argument**, a coherent chain of thought that presents the claim as a logical conclusion based on the available evidence.
- **Evidence**, specific data and other established facts, assumptions or contextual information that provide the grounds for the claim.
- **Rebuttals**, possible counterarguments that result in a different conclusion to the claim.

Thus, constructing the argument can be a way of identifying the nature of specific evidence that is required to be obtained, such as performance data. Alternatively, an argument could be crafted to exploit the available evidence.

## 4.3 Safety Case

A common approach to presenting the justification for a claim of compliance with an assurance goal is to construct an *assurance case*. The purpose of the assurance case is to present a valid and convincing chain of argument to justify a claim that is based on the evidence presented in support of the claim. In many cases, typically safety-related, the certification process requires the assurance case to be subject to independent audit by an appropriately qualified and knowledgeable external party.

The safety case is a commonly employed approach in automotive functional safety (Ward, 2013) and many other sectors (e.g. rail, aircraft) that

are required to achieve risk-based goals. With the aim to justify claims that the risks associated with using a product, process or service are acceptable to the stakeholders, a safety case is a living document assuring a system's critical properties. It provides and documents a convincing and valid argument that a specified set of critical claims regarding the safety properties of a product, process or service are adequately justified for a given application in a given environment. A safety case must be clear in communicating the ideas to be convincing and acceptable; and acceptable does not mean absolutely safe, as that is theoretically impossible, but safe enough, with tolerable residual risk (Kelly, 2004).

Safety cases have been implemented in many ways, including natural language (Tanguy, 2016), structured natural language (Giannakopoulou, 2020), and graphical formats such as the Goal Structured Notation (GSN) (Kelly, 2004). Graphical approaches more naturally provide for a hierarchical presentation of the assurance case than purely natural language documents.

However, a number of concerns about the effectiveness of the safety case approach have been raised, including the tendency towards "box-ticking", potential for confirmation bias, and a lack of focus on uncertain aspects and potentially unsafe behaviour (Leveson, 2011). Nonetheless, the safety case approach is widely used, including within the automotive industry, is familiar to regulators and assessors, and fits naturally with one of the four potential impact factors for automotive cybersecurity considerations (i.e. safety). The safety case therefore provides a natural model that could be adapted and extended for cybersecurity (Armstrong, 2011).

## 5 CYBERSECURITY CASE

A goal-based approach with risk-based targets, like that used in functional safety assurance, seems inherently well suited to cybersecurity, where the threat (the equivalent of a hazard in safety) is even less readily defined.

A risk analysis approach for automotive cybersecurity was adapted from automotive functional safety concepts in the context of the EC project EVITA (Ruddle, 2016). In this scheme, the hazard severity notion of automotive functional safety was extended to encompass the wider implications of cybersecurity threats, whilst the attack potential concept of cybersecurity was exploited as a proxy for threat likelihood to allow qualitative risk rankings to be derived. This approach, as well as a

number of other cybersecurity risk assessment methods, are outlined in SAE J3061.

Cybersecurity threats depend on technology and on human ingenuity and motivation to interfere with the correct functioning of that technology. Some threats will be foreseeable, so can (and should) be addressed before product launch, but unforeseeable threats are highly likely. The unforeseeable threats can only be responded to reactively, so cybersecurity assurance inevitably needs to become an ongoing process, throughout the operational life of the vehicle.

### 5.1 Cybersecurity Case Requirements

Based on emerging technological trends in the automotive industry, as well as current functional safety engineering practices (as outlined above), it is considered that an assurance case for automotive cybersecurity should ideally provide the following basic characteristics:

1. Unified approach with existing safety case techniques – since potential safety impacts are also associated cybersecurity threats and efficiency can be maximised by exploiting existing familiarity with safety case techniques, facilitating the reuse of common arguments and supporting evidence where possible.
2. Ability to address aspects beyond traditional safety – including availability of mission-critical (rather than safety-related) functions, privacy issues, fraudulent financial transactions, and indirect safety implications (such as kidnapping) that are beyond the remit of more traditional safety analysis.
3. Ability to adapt to emerging threats – to cope with the inevitability of threats emerging that were unforeseeable at design time, including those that may result from the implementation of software updates during the operational life of the vehicle.
4. Ability to integrate cybersecurity analysis – as essential sources of argument and evidence, as well as their limitations.
5. Support probabilistic risk analysis – to cope with system complexity and the significant uncertainties of cybersecurity analyses.
6. Provide explicit visibility of uncertainties – in order to provide a more balanced view of the limitations of the arguments that are presented for independent audit.
7. Hierarchical structure – to help cope with wide scope of the analysis, system complexity, and readability.
8. Graphical approach – to help cope with the wide scope of the analysis, system complexity, and readability.

9. Dynamic, living document – will need to be readily adapted throughout development and operational lifecycles to reflect the impact of software updates and security patches.
10. Modular construction – to allow the impact of system changes to be assessed efficiently and the cybersecurity case to be updated.
11. Support for emerging legislation – to provide a convenient path for demonstrating compliance with relevant standards and regulations, such as the UNECE Regulations 155–156, and ISO/SAE 21434.

## 5.2 Differences from Safety Cases

In adapting the safety case notion to cybersecurity, the main difference is that a cybersecurity case has to address a much wider scope, being concerned not just with the safety implications of deliberate attacks, but also with the availability of non-safety functions, potential for privacy infringement, and possible financial losses due to fraudulent transactions. These separate aspects could be individually treated but combined in a hierarchical assurance case. It is likely that the individual cases they would draw on common argument structures and evidence streams, resulting in an interlinked web-like structure.

Another significant difference is that, unlike safety, the operational environment is subject to ongoing change and evolution, as new threats emerge and technology progresses. This leads to a need for through-life monitoring, to detect cybersecurity breaches, assess their risks, and respond to them in a timely fashion (where the risk analysis suggests that mitigation is necessary). This will “provide lessons learned” to contribute to future cybersecurity design and risk analysis, but will also require the security case to be updated to reflect current system knowledge.

Nonetheless, in the same kind of manner any software update that the vehicle receives, even if it is upgrading a safety function already evaluated through a safety case, would require the re-evaluation of both the safety and cybersecurity cases.

A further difference to be considered is that, during development the consideration of safety and security issues should happen in parallel, yet may not do so. This can happen because of the requirements at the start of production will not necessarily align with the final builds for all the software. However, in both safety and cybersecurity it is more effective to initiate the analysis as early as possible in the vehicle development process.

## 5.3 Challenges for Assurance Cases

Significant challenges faced in developing assurance cases, for both safety and cybersecurity applications, include the following:

- Linking to evidence, while being able to identify bias.
- Handling the non-deterministic behaviour of AI systems – how can we argue the safety and cybersecurity of these technologies, and what kind of evidence would be required to support these arguments?
- How to handle evolving systems – e.g. due to SW updates or unsupervised learning by AI?
- How to provide a balanced view of the limitations of such a case, such as by including and explicitly showing the failure of possible counter-arguments, such as for “non-safety” (Leveson, 2011).
- Assurance cases need to provide a better and more explicit handling of uncertainty and the limitations of the arguments that are presented.
- There needs to be a deeper understanding of where formal methods might add value.

## 6 CONCLUSIONS

Connected and automated vehicles are expected to provide many benefits to society, but the enabling technologies are also associated with new threats, particularly in terms of cybersecurity. Ensuring public trust in future connected and automated vehicles will require very high levels of confidence in their dependability, which will include cybersecurity assurance. Traditional prescriptive assurance strategies are not practicable for establishing automotive cybersecurity performance. The anticipated constant evolution of both on-board technology and attack techniques also means that conventional pre-product launch assurance activities, while still of great importance, will not be sufficient to provide the necessary assurance. Cybersecurity performance metrics can only be expressed in terms of risk, with cybersecurity assurance aiming to both contain the known risks to tolerable levels and provide a mechanism for identifying and responding to emerging threats. This is reflected in the risk-based, goal oriented, and ongoing assurance approach now mandated in UNECE Regulation 156 for vehicle type approval.

A dynamic and modular *cybersecurity case* approach, adapted and extended from existing safety case approaches such as those used in automotive

functional safety, could provide a useful mechanism for both recording and maintaining cybersecurity assurance claims. This paper has identified a number of essential requirements for a cybersecurity case for automotive applications, and differences from safety cases, as well as a range of particular challenges that will need to be overcome in future, for both safety and cybersecurity applications.

## ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 812788 (MSCA-ETN SAS – Safer Autonomous Systems). This publication reflects only the authors' view, exempting the European Union from any liability. Project website: <http://etn-sas.eu/>.

## REFERENCES

- Armstrong, R., Hawkins, R. & Kelly, T. (2011). Security Assurance Cases: Motivation and the State of the Art. University of York Report CESG/TR/2011/1, April 2011 <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.221.456&rep=rep1&type=pdf>.
- Cui, J., Liew, L. S., Sabaliauskaite, G., & Zhou, F. (2018). A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Networks*, 90 (December 2018), 101823. <https://doi.org/10.1016/j.adhoc.2018.12.006>.
- Cui, J., Sabaliauskaite, G., Liew, L. S., Zhou, F., & Zhang, B. (2019). Collaborative Analysis Framework of Safety and Security for Autonomous Vehicles. *IEEE Access*, 7 (March 2018), 148672–148683. <https://doi.org/10.1109/ACCESS.2019.2946632>.
- Giannakopoulou, D., Pressburger, T., Mavridou, A., & Schumann, J. (2020). Generation of Formal Requirements from Structured Natural Language. In N. Madhavji, L. Pasquale, A. Ferrari, & S. Gnesi (Eds.), *Requirements Engineering: Foundation for Software Quality* (pp. 19–35). Springer International Publishing. [https://doi.org/10.1007/978-3-030-44429-7\\_2](https://doi.org/10.1007/978-3-030-44429-7_2).
- Kelly, T., & Weaver, R. (2004). The Goal Structuring Notation – A Safety Argument Notation. *Elements*. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.5597&rep=rep1&type=pdf>.
- Kelly, T. P., McDermid, J., & Weaver, R. (2005). “Goal-Based Safety Standards: Opportunities and Challenges”, *Proceedings of the 23rd International System Safety Conf.*, San Diego, California (August 2005). <https://www-users.cs.york.ac.uk/~tpk/ISSC23.pdf>.
- Leveson, N. (2011). The Use of Safety Cases in Certification and Regulation. *MIT-ESD Working Paper Series* November 2011, 1–12. <https://dspace.mit.edu/bitstream/handle/1721.1/102833/esd-wp-2011-13.pdf?sequence=1&isAllowed=y>.
- Macher, G., Messnarz, R., Armengaud, E., Riel, A., Brenner, E., & Kreiner, C. (2017). Integrated Safety and Security Development in the Automotive Domain. SAE Technical Papers, March 2017. <https://doi.org/10.4271/2017-01-1661>.
- Ruddle, A.R., et al., (2020). *Requirements and timescales for CYB-R: the UK Centre of excellence for road transport cybersecurity resilience*, ResiCAV Project Deliverable 1, 30th March 2020. <https://zenic.io/reports-and-resources/>
- Ruddle, A.R., & Ward, D.D. (2016). “Cyber Security Risk Analysis for Intelligent Transport Systems and In-vehicle Networks”, in A. Perallos, U. Hernandez-Jayo, E. Onieva and I. Garcia (Eds.) *Intelligent Transport Systems: Technologies and Applications*, Chapter 5, Wiley-Blackwell, 2016, pp. 83–106. <https://doi.org/10.1002/9781118894774.ch5>.
- Shavit, M., Gryc, A., & Miucic, R. (2007). Firmware update over the Air (FOTA) for automotive industry. SAE Technical Papers, 724. <https://doi.org/10.4271/2007-01-3523>.
- Steger, M., Dorri, A., Kanhere, S. S., Römer, K., Jurdak, R., & Karner, M. (2018). *Secure Wireless Automotive Software Updates Using Blockchains: A Proof of Concept*. 137–149. [https://doi.org/10.1007/978-3-319-66972-4\\_12](https://doi.org/10.1007/978-3-319-66972-4_12).
- Tanguy, L., Tulechki, N., Urieli, A., Hermann, E., & Raynal, C. (2016). Natural language processing for aviation safety reports: From classification to interactive analysis. *Computers in Industry*, 78, 80–95. <https://doi.org/10.1016/j.compind.2015.09.005>.
- Toulmin, S. (1958). *The Uses of Argument* Cambridge University Press. doi:10.1017/CBO9780511840005.
- Wang, P., Di, B., Zhang, H., Bian, K., & Song, L. (2018). Cellular V2X Communications in Unlicensed Spectrum: Harmonious Coexistence with VANET in 5G Systems. *IEEE Transactions on Wireless Communications*, 17(8), 5212–5224. <https://doi.org/10.1109/TWC.2018.2839183>.
- Ward, D., Ibarra, I., & Ruddle, A. (2013). Threat Analysis and Risk Assessment in Automotive Cyber Security. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, 6(2), 507–513. <https://doi.org/10.4271/2013-01-1415>.