THE | AUTONOMOUS

Chapter Event Safety & Security

co-hosted by

EXECUTIVE SUMMARY

On June 22nd, 2020, The Autonomous together with Infineon, Secunet, and Integrity Security Services hosted a virtual Chapter Event on "Safety & Security". The event featured five presentations and two panel discussions. A moderator managed the interaction between the audience and the speakers. The audience participated by submitting numerous questions that were answered by the presenters and by completing a post-event survey. The event focused on two main topics: (i) "Fundamentals and Current Activities on Security" and (ii) "Challenges and Opportunities in the Security Domain". This report summarizes the presentations, panel discussions, the Q&A, and the results of the post-event survey.

Focus I: Fundamentals and Current Activities on Security

The topic aimed to address subjects, such as the "Overview of existing and emerging cybersecurity standards and prominent gaps", as well as, "Changes in the security landscape: the shift from the car of today to the highly-connected car of the future". Three keynotes from industry and academia were presented and 17 questions were thoroughly discussed – some of which are:

- What is the right balance of implementing security requirements versus system performance?
- What is the status and focus of the UNECE WP29 Automotive Cybersecurity Regulation?
- Should there be an alignment between safety and security standards?

Furthermore, a post-event survey resulted in the following data:

- 77% of the survey participants do think that not enough emphasis on cybersecurity is given today in the automotive industry.
- The key challenges in the context of cybersecurity that need to be tackled are: bringing cybersecurity awareness and changing to security by culture, ensuring security over the whole lifecycle, harmonizing cybersecurity requirements, and strict regulations on these requirements.
- Reference solutions for update mechanisms would be necessary to guarantee identical procedures and layout for updates in different cars.

Focus II: Challenges and Opportunities in the Security Domain

Challenges raised from the increased attack surface of automated vehicles as well as zero-day attacks, secure over-the-air updates, and IP protection were the main subjects addressed in this session. Two high-quality keynotes were presented, and 11 technical questions were passionately discussed – a portion of which are:

- How to guarantee the detection of unknown security violations?
- Are there any publicly available standard security events databases?
- Should the lack of diversity in hardware and software in the automotive domain be considered as an opportunity or threat to cybersecurity?

The post-event survey resulted in the following data:

- 92% of the participants think that runtime monitoring is an important complementary measure for detecting unsafe vehicle operation resulting from a cybersecurity attack.
- When asked, "Do you think the automotive industry should take an example of other domains when it comes to cybersecurity?", 85% of the participants answered with "Yes". Participants recommended looking into good practices from the railway, avionics, IT, telecommunication, government, public agencies, defense, finance, and banking domains.
- The automotive sector often sees their products through the customer's eyes and argues that cybersecurity does not offer clear customer benefits. Nevertheless, insecure cars will lead to high risks of loss of brand reputation and of costs for OEMs and Tiers.

"Cybersecurity is not an integral part of the development process, as it is the case with functional safety. It is less regulated and still has to be argued."

--A quote from a participant

BACKGROUND AND EVENT DETAILS

The Initiative

For all actors involved in the development of autonomous mobility solutions, who position safety as a fundamental value of their products - The Autonomous is a knowledge ecosystem - that generates new knowledge and technological solutions to tackle key safety challenges that shape the future of safe autonomous mobility. Complementary to standardization organizations that establish uniform engineering or technical criteria, methods, and processes, The Autonomous will develop Global Reference Solutions for autonomous mobility that conform to relevant standards and facilitate the adoption of these solutions on a grand scale. The benefits The Autonomous will provide to the partners of the ecosystem are:

- Development of safe and best-in-class AD solutions thanks to the wisdom of the crowd;
- Reduction of potential product liability risk by (i) tightly working with government and regulatory institutions and (ii) developing common basis for regulatory bodies;
- Reduction of development costs by (i) developing modular and reusable Global Reference Solutions and (ii) sharing the development efforts;
- Reduction of risk of wrong development by joint definition of state-of-the-art and state-of-practice;
- Accelerating the learning curve by collectively learning from individual failures and field observations.

Towards this vision, in 2020, The Autonomous is hosting a series of workshops - "The Autonomous Chapter Events" - to facilitate discussions among experts and take the first steps towards the targeted Global Reference Solutions. The third Chapter Event titled "Safety & Security" was hosted by The Autonomous, together with Infineon, Secunet, and Integrity Security Services.

Event Details

Presentations

Focus I: Fundamentals and Current Activities on Security

- Best Practice in Cybersecurity | Harry Knechtel | Secunet
- A Streetview on Automotive Cybersecurity | Christoph Schmittner | AIT
- Automotive Cybersecurity Under Construction | Markus Tschersich | Continental

Focus II: Challenges and Opportunities in the Security Domain

- Combining VSOC and Onboard IDS Technologies to Understand Cyberattacks on Vehicles | Shiran Ezra | Argus
- Challenges and Solutions for Automotive Onboard Intrusion Detection | Eduard Metzker | Vector

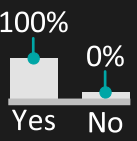
Event Statistics

Facts

- 207 event registrations
- 113 different companies attended
- Livestream:
  - 125 unique views
  - 93 concurrent viewers
- 28 questions thoroughly discussed

Feedback

- 21 participants provided feedback
- Did the event meet your expectations?



- How would you rate the event? ★★★★★½

Technical Report

Chapter Event Safety & Security

Edited by
Harry Knechtel, Jochen Schönweiß, Ayhan Mehmed

The Autonomous
November, 2020

Contents

1 | The Initiative

As autonomous mobility is moving closer to becoming a reality, safety and trust concerns prove to be the main hurdle in the way of reaching broad acceptance. OEMs and technology suppliers (Tier 1, 2 & 3, and others) cannot overcome the safety challenge and the necessary investment costs with a "go it alone" approach. Therefore, the autonomous mobility industry and other relevant institutions need to come together and show significant efforts in prioritizing and ensuring safety on all technological levels, as well as set common technical and legal standards. Towards this, TTTech Auto initiated The Autonomous - an open platform that brings together actors from the autonomous mobility ecosystem to align on relevant safety subjects.

1.1 Vision

> *Create a safer, more livable,*
> *and more sustainable future.*
>
> — The Autonomous

For all actors involved in the development of autonomous mobility solutions, who position safety as a fundamental value of their products - **The Autonomous is a knowledge ecosystem** - that generates new knowledge and technological solutions to **tackle key safety challenges** that shape the future of safe autonomous mobility. Complementary to standardization organizations that establish uniform engineering or technical criteria, methods, and processes, The Autonomous will develop **Global Reference Solutions** for autonomous mobility that conform to relevant standards and facilitate the adoption of these solutions on a grand scale. The benefits The Autonomous will provide to the partners of the ecosystem are:

- Developing safe and best-in-class solutions for Automated Driving (AD) challenges thanks to the wisdom of the crowd;
- Reduction of potential product liability risk by (i) tightly working with government and regulatory institutions and (ii) developing a common basis for regulatory bodies;
- Reduction of development costs by (i) developing modular and reusable Global Reference Solutions and (ii) sharing the development efforts;
- Reduction of risk of wrong development by joint definition of state-of-the-art and state-of-practice;
- Accelerating the learning curve by collectively learning from individual failures and field observations;

Furthermore, the work products of The Autonomous are expected to serve as further input to existing standardization activities and may also result in new standardization projects.

1.2 Mission

Towards the above-defined vision statement, The Autonomous will:

- Provide a diverse and balanced knowledge ecosystem for autonomous mobility;
- Set the stage for open discussions on main technical and architectural questions where controversial approaches can be freely discussed;
- Act as an interface between industry requirements, standardization, regulation bodies, and academic research in safe autonomous mobility. Collectively identify important gaps in the field and focus the efforts;
- Build consensus on major safety solutions within the automotive industry;
- Generate high-quality know-how and Global Reference Solutions compliant to relevant standards in autonomous mobility;
- Facilitate the adoption of the Global Reference Solutions on a grand scale by placing them into relevant standards as solutions compliant to their requirements.

1.3 Approach

Current Approach

The development approach of automotive systems has remained unchanged over many years. Generally speaking, a car manufacturer (OEM) and its suppliers (Tier 1, 2 & 3, and others) cooperate and then compete with other manufacturers in providing better solutions and products (see Figure 1). This approach has worked well for developing standard, well constrained, and deterministic automotive embedded systems like Anti-Lock Braking System (ABS), Engine Control Units (ECU), and others.

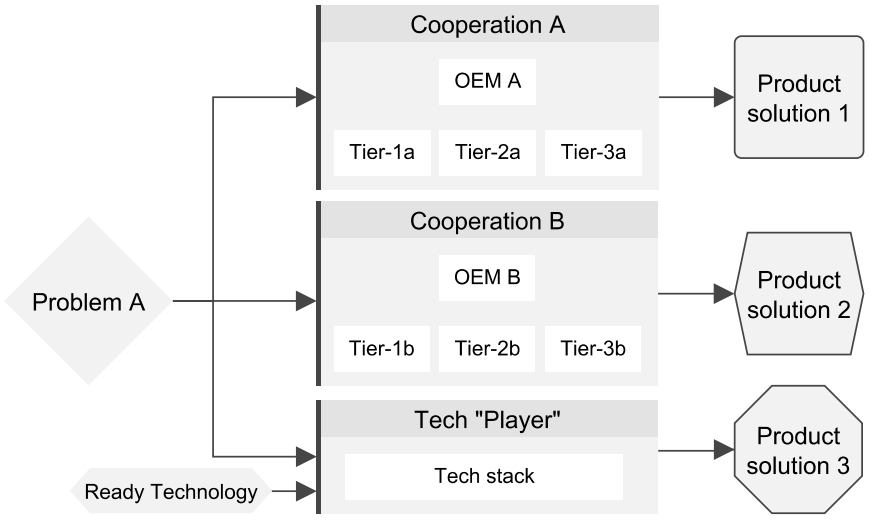


Figure 1: Current development approach of automotive systems.

However, the approach is sub-optimal when it comes to the development of upcoming SAE Level 3 - Level 5 Automated Driving Systems (ADS). The rationale for this is (i) the novelty and high complexity of the AD systems, (ii) unprecedented high development costs, and (iii) different technical solutions will likely not align in a common state of the art.

Proposed Approach

To reduce the development cost, a shift from many interdependent cooperation groups (where cooperation groups compete with each other on providing a better solution for a given problem) to a single, larger, and more diverse knowledge ecosystem where partners collaborate towards a single shared goal is necessary (see Figure 2). Such an approach will enable (i) the development of safe and best-in-class products, (ii) ecological and sustainable development, and (iii) faster development autonomy. Furthermore, in addition to car manufacturers and technology suppliers, The Autonomous also invites stakeholders from governmental, academic, regulatory, and standardization institutions in order to ensure an integrated view.

In “STEP 1” of the proposed approach, the partners of the knowledge ecosystem, will work together on Global Reference Solutions that conform to relevant standards. The notion of the Global Reference Solutions is to cover all relevant problems in the development of future AD systems. Hence, more than one reference solution will be available, i.e., ranging from Fail-Operational/Fail-Degraded (FO/FD) architectures to verification and validation (V&V), runtime verification approaches, sensor and sensor fusion configuration, and others. In “STEP 2” of the proposed approach, the partners of the ecosystem will be able to individualize the Global Reference Solution to their needs and therefore keep the competition “alive".

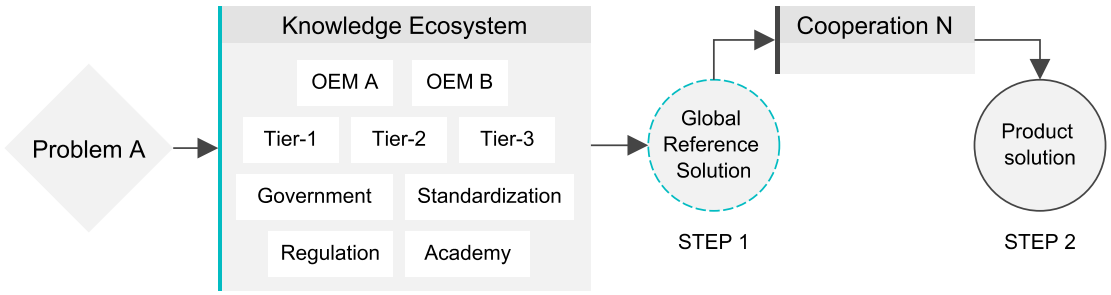


Figure 2: Proposed approach for development of future AD systems.

1.4 Roadmap

In 2020, The Autonomous is organizing a series of *virtual* technical workshops, also known as "The Autonomous Chapter Events", to facilitate discussions among experts and work towards the target Global Reference Solutions. Figure 3 presents a summary of the Chapter Events planned for 2020. While the scope of the Chapter Events will be further broadened by adding other relevant topics, the list below summarizes the current status:

- Chapter Event Safety & Architecture: April 2nd, 2020 with co-host TTTech Auto.
- Chapter Event Safety & Artificial Intelligence (AI): June 5th, 2020 with co-host Five.
- Chapter Event Safety & Security: June 22nd, 2020 with co-hosts Infineon, Secunet, and Integrity Security Services.
- Chapter Event Safety & Regulation: July 9th, 2020 co-hosted with Posser Spieth Wolfers & Partners (PSWP).
- Chapter Event Safety & Sensor Fusion: November 5th, 2020 with co-host BASELABS.
- The main The Autonomous event: March 10th, 2021 co-hosted with TTTech Auto in Vienna, Austria as well as virtually.

The target outcome of each Chapter Event is a high-quality content summarized in reports. The current report is a summary of Chapter Event Safety & Security. The outcomes of the reports will be outlined in The Autonomous Main Event on March 10th, 2021.

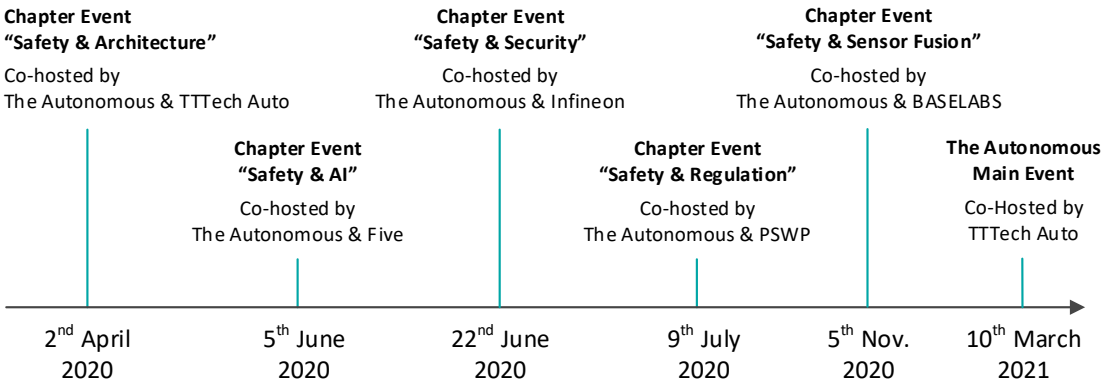


Figure 3: Summary of events planned for 2020-2021.

2 | Chapter Event Safety & Security

2.1 Scope and Topics

This Chapter Event covered the following topics related to security in autonomous vehicles:

- **Focus I: Fundamentals and current activities on Security**
  - The change in the security landscape: the shift from the car of today (i.e., the traditional "connected" car) to the car of the future (i.e., autonomous car).
  - Overview of existing and emerging cybersecurity standards relevant for Autonomous Driving, e.g. ISO 21434, ISO 14229, ISO 15118, AUTOSAR CAL/CSM, and others).
  - Prominent gaps in today's standards and existing products.
  - Security relevant systems for autonomous driving (e.g., vehicle, mobile devices, roadside units, backend, and others),
  - Overview of best practices in the security domain.
- **Focus II: Challenges and Opportunities in the Security Domain**
  - Cross-domain view: from carmakers and suppliers to insurers, regulatory bodies, and customers.
  - Widening of the attack surface.
  - SAE L3+ Automated Driving: the lack of a fallback-ready driver.
  - Ensuring secure autonomous vehicles over the whole lifecycle.
  - And other relevant challenges: zero-day attacks, secure over-the-air updates, IP protection, performance requirements, and others.

2.2 Event Statistics

Figure 4 summarizes the facts about the event and the feedback given by the participants. In particular, 207 registrations were made for the virtual event. The participants were from 113 different companies/institutions. The live stream had in total 125 unique views. Throughout the four-hour event, there were 93 concurrent viewers. Last but not least, 47 questions were asked by the audience, of which 28 were addressed (see Section 3 and Section 4 for the summary of answers). Twenty-one participants provided feedback after the event, where 100% of them said *"yes"* when asked whether the event met their expectations. The participants also rated the event with an average of 5.1 stars out of six.

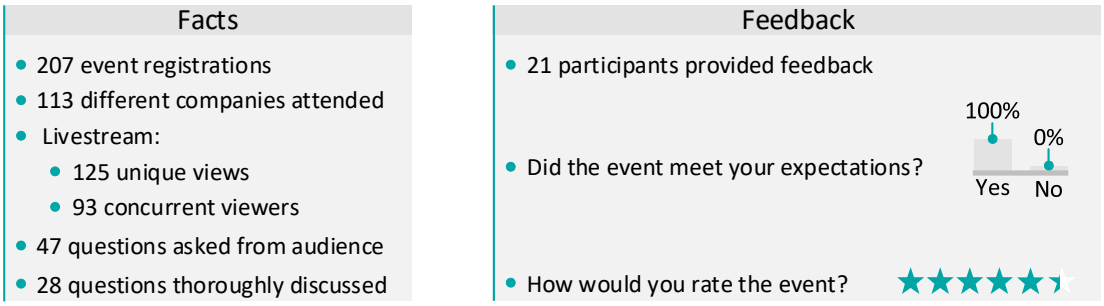


Figure 4: Facts about the event and feedback from participants.

3 | Focus I: Fundamentals and Current Activities on Security

3.1 Talk 1: Best Practice in Cybersecurity

Harry Knechtel
Head of Production - Industry Division, Secunet

Summary

The future of mobility will be driven by the idea of autonomous, connected, electrified cars, which are shared between parties. This will lead to new challenges up on the road, even though electronics have been in the car for several decades. First of all, the network technologies, from 2G to 5G massively increased the reachable bandwidth, resulting in more interactions between car, customer and environment and thus increasing the number of possible attack vectors. Secondly, higher levels of autonomous driving trigger less manual control by the driver, and therefore more responsibility is handed over to the car and infrastructure. Thirdly the time of car attacks, where the attacker needs to have physical access to the car is over. This results in a higher scalability of attack scenarios and, thus, in higher potential damage as more systems can be controlled simultaneously. This means security measures need to be established to prevent high damage to passengers, brand value, and the environment.

There are already several "best practice" IT-security measures used in the automotive branch, like security access, secure onboard communication, secure boot, and hardware security. In the future, we see the additional demand for autonomous driving, like secure Car2x-communication, crypto-agility, certified security tests. But those technical security controls cannot stand alone, independent from an overall security strategy. Therefore a cybersecurity management systems are needed, covering the complete product lifecycle.

To sum it up: "Security is a process, not a product"(Bruce Schneier), meaning secure processes, organizations, and infrastructure are as relevant as the security solution within your products. In the end, everything starts with the definition of requirements. Secunet is convinced that best practices from the past can be adjusted for the future and a common understanding can be generated, still leaving room for OEMs and Tiers to establish their own specifications. "The Autonomous" can help to define the mentioned requirements.

Addressed questions

Q1 It is evident that additional security measures will add overhead when it comes to system performance. In your opinion, how can we balance security & performance when it comes to implementing security measures in V2X communication?

> **Answer by Harry Knechtel**
> Security measures do have an impact on the performance demand of a system. Especially for communicating devices, which are needed for V2X communication. Therefore the security needs a holistic approach, which starts during the design phase of the solution. In this phase, security requirements are defined as well as threat analysis and risk assessments (TARAs) are executed to verify critical messages to the system and to get a view of the possible attack paths. In the end, more and less critical components of the system are determined. In order to be able to implement security in a way that does not conflict with performance requirements by safety – you may have to invest in sufficient hardware that will have an impact on costs.

Q2 When referring to "monitoring" under secure field operation, do you mean monitoring at runtime, the safe operation for the system, or if not, could you elaborate?

> **Answer by Harry Knechtel**
> With autonomous vehicles, different types of monitoring will be necessary. Monitoring of the individual device and vehicle will be standard, as well as the monitoring of the backend and the overall fleet. The backend includes both OEMs/Tier-X backend and infrastructure like roads, traffic lights, etc. The main goal of monitoring is to detect malfunction, incidents, and attacks.

3.2 Talk 2: A Streetview on Automotive Cybersecurity

Christoph Schmittner
Scientist, Austrian Institute of Technology - AIT

Summary

Security has always been an issue for vehicles. Around 1900, cars started to have keys, initially to lock the ignition, later on also for the doors. A few years later, electronic elements began to play a role. A resistor with a secret value was integrated onto a key. With the rising communication and interaction of vehicles with external systems, there was a transition towards automotive cybersecurity. With this, the focus of security moved from preventing car theft to focusing on a more holistic view of cybersecurity and security properties. All of this makes it relevant to define the scope of automotive cybersecurity. Structuring the system, we have the vehicles, the road and traffic infrastructure under the control of the road operators, and telecommunication infrastructure. Service operators and manufacturers control the backend, and we see here classical IT security standards from the ISO 27000 series. The challenge is harmonization and coordination. Therefore there is a need to develop a clear picture of automotive cybersecurity,

the scope, and the interactions with other domains. The main point is the interaction between an automated vehicle and intelligent road infrastructure. These systems are controlled and maintained by different parties, and the establishment of trust will be a challenge. Already for simple use cases, we see different approaches. We need to ensure security, trust, cooperation, and safety in all cases, considering the involved elements. This talk provides a comprehensive view of today's highly-connected vehicles and supporting infrastructure and addresses the difficulty of defining the scope of cybersecurity.

Addressed questions

Q3 Is it possible that Security mechanisms interfere with safety mechanisms? If yes, what is the solution?

> **Answer by Christoph Schmittner**
> Yes, security and safety mechanisms can interfere. There have been proven incidents in the past where functional security requirements led to security incidents. Also, the other way around can happen. This leads to the necessity of defining processes like in the ISO-26262 – but for security. Meanwhile, it is and will be a continuous challenge to look at all the different domains.

Q4 Suppose you have to weigh the criticality of a successful security attack. How would you order the following: attack on the vehicle, attack on a road infrastructure item (e.g., a traffic light), attack on a cloud-based system, etc.?

> **Answer by Christoph Schmittner**
> There is a difference between safety and security. The safety perspective examines the random effects on one vehicle. From the security perspective, the scale of the attack needs to be considered, so the number of affected elements. This means – if the consequences of an attack are the same – the weight and order of criticality are defined by the affected vehicles. For example, it could be a single attack on one specific vehicle, an attack on a traffic light affecting all the vehicles in the vicinity or an attack on a cloud system affecting all the connected vehicles.

3.3 Talk 3: Automotive Cybersecurity Under Construction

Markus Tschersich
Manager Security, Privacy Standardization and Regulatory Affairs, Continental

Summary

The automotive industry is under construction also with respect to cybersecurity. The upcoming UN regulation on cybersecurity in the vehicle type approval demands the industry to ensure cybersecurity along the value chain on both organizational and technological level. The regulation is also seeing cybersecurity as a prerequisite for type approval of autonomous functions.

This presentation gives a brief summary of the upcoming regulation and shows organizations can prepare with the help of the ISO/SAE 21434 Standard on Automotive Cybersecurity Engineering.

Addressed questions

Q5 When you refer to the "Proposed work products for documentation", do you asume that they will be required from all suppliers in the chain: e.g., system suppliers, subsuppliers, and others? If so, when deciding on the "Work products for documentation" do you include all the suppliers?

> **Answer by Markus Tschersich**
> At the current state, it is not clear how deep within the supply chain the requirements from ISO / UNECE dealing with the "Proposed Work Products for documentation" have to be fulfilled.

Q6 When is the UNECE Interpretation Document going to be available?

> **Answer by Markus Tschersich**
> The interpretation document of the UN regulation both for software and cybersecurity is still under draft. The expected release is by the end of 2020. The yellow book (Gelbband) is in the review phase and can be found online. The red book (Rotband) is planned to be published by the end of the year.

3.4 Panel Discussion on Fundamentals and Current Activities on Security

Addressed questions

Q7 Is there another standard available or under development that addresses the additional requirements that are not covered in the ISO/SAE-21434?

> **Answer by Markus Tschersich**
> The technical level is not in the scope of the ISO/SAE-21434, meaning it does define requirements for processes and methods. When it comes to specific technical aspects, more standards will be published. For example, there are initiatives in the ITU (international telecommunication union) domain and the car2car consortium. Also, Harry Knechtel mentioned upcoming certifications of technical parts resulting in more standardization for technical specifications as well as guidance to certain product categories and security parts.

Q8 It seems that there is a high number of upcoming standards to cover the gaps in the automated driving domain. How do you assure the alignment of all these standards?

Answer by Markus Tschersich 1/2
This more or less explains my activities that I do in the name of my company by attending UNECE and different standardization groups. We are working on a national level like VDA. On the horizontal level with all the activities also with the European associations like ACEA/CLEPA, but also with some industry delegations on the UN level. But of course, as they are distributed on different levels, there is not one organization taking care of combining all the elements. So it is up to the responsibilities of the different organizations in the industry to build those bridges. There are several colleagues that I can luckily see in different groups. So we try to do this job.

Answer by Harry Knechtel 2/2
We do see different standards being defined, resulting in major challenges: On the one hand, we might have the standards in the future on the security goals to be implemented, but on the other hand, there will be a lot of problems due to the quality of implemented security. So even with a good recommendation of minimum requirements, faults in the implementation are still possible, resulting in the question, whether the quality of security in heterogeneous systems is achievable. Different cars from different vendors, different infrastructures, different traffic lights, and others could result in a state in which some kind of certification or qualification of the security level is necessary as well as its implementation.

Q9 Is there a standardized way of performing quality checks? Or every company is following their own quality procedures.

Answer by Harry Knechtel
At the moment, we do not see a broad approach between different vendors regarding the quality of implemented security. We do see testing on a functional level, like interoperability tests to examine how systems are working with one another. But these tests are executed from a technical perspective, not from a security perspective. In the future, we expect more regulation and standardization regarding the quality of security implementation, which is, for example, important for embedded devices.

Q10 Are there any upcoming initiatives that aim at filling the gaps in the current standards?

Answer by Markus Tschersich (1/2)
The current standardization can be seen as a baseline addressing processes and methods. If talking about the functionality of a new vehicle, environmental aspects for this product have to be considered as well as issues that can be standardized from a technical point of view. The cybersecurity environment is changing fast, while standards need time to be revised. This means scientific publications might be a better tool than standards in order to achieve really secure products from a technological point of view.

Answer by Christoph Schmittner (2/2)
There is a large amount of work already on publications like intrusion detection systems (IDS) or cryptography suited for the automotive domain. The challenge regarding standardization is always that the standard takes time so that it is valid for a longer time like 3, 4, 5 years. This is possible with cybersecurity processes, but regarding the cybersecurity technology, no one is able to claim that he or she knows this cryptographic algorithm will be secure for the next five years.

Q11 Is there a need for an alignment between safety (e.g., ISO 26262) and security standards? If so, how do you ensure that?

Answer by Christoph Schmittner (1/2)
Definitely, this is something similar to the alignment between the standards themselves (ETSI, UNECE, ISO/SAE). In the definition of the standard experts are participating, who were already involved in the safety standardization of ISO-26262 and gave their input, how both domains (security and safety) can be harmonized. For example, using the same set of vocabulary and sharing core concepts lead to easier development of safety and security standards and alignment.

Answer by Markus Tschersich (2/2)
I fully support the description of harmonizing standards, as Christoph said. Sometimes though, there is the need to see the difference and deviations between the standards.

Q12 Are there guidelines on essential security algorithms that systems need to implement? Or guidelines for the timeframe in which a security algorithm needs to be updated to ensure protection against the latest security threats?

Answer by Harry Knechtel (1/2)
This is one of the major problems of the automotive industry when it comes to security. Of course, there are sources about the state of the art algorithm and length standards that can be looked up on the internet (e.g., BSI, NIST). Most of the recommended algorithms, which currently can be implemented, are only valid for the next 5-7 years. The major challenge is connected vehicles with a long lifetime, while the automotive industry has a big focus on cost reduction. This leads to microcontrollers in the vehicle not having the hardware power to process longer keys and other algorithms, which might be needed in 5 years. Thus a software update might not solve this issue. Therefore we assume new concepts on how to modularize security and cryptographic functions within your system to update to future algorithms, which will be secure, are needed.

Answer by Jörg Schepers (2/2)
This is exactly the challenge we are facing now when defining our next generation of MCUs. It's not only the long time in the field we have to anticipate, but also the development of such MCUs, and the qualification takes a couple of years. So we are now already looking forward to a time span up to 2040 where those products will be in the field. And yes, that's a challenge, but I think it is also something you can prepare for. So in our new architecture, for example, we will have a fundamentally different concept for all the use cases coming up now with secure communication and stuff like that. We will define the hardware architecture in a way that it becomes more flexible. We are even looking to cross quantum algorithms already right now. There are many people not taking it seriously because it might be a couple of years ahead of us, but in 2040, I am 100% sure we will see it in the field, so we have now to define a hardware architecture with sufficient memory space for higher key-length with more power for computational units; that is something we are doing. So we have to build in this agility for adaptations in the hardware itself, and then we can take it from there. Because nobody can predict what kind of algorithms will then be used in the field ten years from now.

Q13 In the context of connected vehicles, security algorithms are a necessity. However, they may require significant hardware resources. What should be the strategy for ensuring that a system will have sufficient hardware resources for implementing critical security algorithms in the long term (e.g., 20-30 years)? Should we design ECUs with extra resources, or should we simply design with modularity in mind: e.g., a hardware security module that can be later added to the ECU?

Answer by Jörg Schepers
This cannot be answered in general, as today, a vehicle can have 100 ECUs with differing security requirements. A telematics unit is one of the preferred attack targets, but a different gateway might need a differing security concept in comparison to a body controller for interior light or a transmission unit. I think the hardware architecture we are defining now is scalable, but we are also optimistic that high-end hardware will have sufficient resources for the units of the upcoming 15 years or so. Furthermore, there should be a balance between the how-much security features are implemented and the price of the hardware. Built-in security is sometimes not shocking for the developers but for the purchasers because of the price tag. Nobody is yet willing to pay for a security or at least reluctant to pay for security in 10 years from now on. If you built in more powerful hardware, there would be a cost, and we have to work together to clarify that the security features are worth their costs. In the end, it is a little bit like an insurance policy as you have to pay for something now in order not to let it happen in 10 years from now on.

Q14 How to ensure overall safety when updating an autonomous vehicle?

Answer by Christoph Schmittner (1/2)
One question here is also related to the update itself, as shown in a study of AIT (Australian Institute of Technology) about safe and secure updating. We used a mockup car to show the willingness of the user to update by sending an update message like: “It will add some new security issues, besides, it will add, e.g., automated parking”. The behavior of the participants was similar to a desktop or normal IT domain – most of the participants, who were asked to update, decided to update the new security feature last as they wanted to drive. The new automated driving function was updated with a much higher likeliness.

Answer by Markus Tschersich (2/2)
Field regulation or penalties will also be an additional motivator. In UN task force discussions, it was seen as common sense that the supply chain is responsible for providing an update in a respective timeframe, but it is not responsible for ensuring that the update will be installed. In China, there was recently a case where a forced over-the-air update resulted in a car stopping on the highway and blocking it for 2 hours. This is also not a nice situation for passengers. In the end, there will likely be some replacables – type approval replacables – and at the inspection, it will be identified whether the latest update is installed within the respective timeframe. Then it will be the responsibility and the penalty of the owner or the driver of the vehicle for not having done this.

Q15 Do you see over-the-air updates coming to Europe soon? If yes, do you have a timeframe in mind?

Answer by Markus Tschersich (1/2)
When it comes to regulation, the question is twofold. Talking about updates, by January 2021, if WP29 decides so, in Europe, you will be allowed to type approve ALKS (automated lane-keeping systems), so autonomous driving level 3. A prerequisite besides the cybersecurity regulations to be considered is also the software update regulation. It is necessary to make sure that all autonomous driving systems 3+ have software update regulations in place with respective processes resulting from some technical requirements. So far, for Europe, there is no plan to apply software updates to all kinds of vehicles. But as the cybersecurity regulation requires to react "in a reasonable timeframe", it will be more or less necessary that all the vehicles have an over the air interface. Otherwise, it will end up at a high cost if you have to call vehicles in every time you want to update the software.

Answer by Harry Knechtel (2/2)
I think we will see over the air updates in the future as diagnostics over the air and remote management of cars are already done today. In the end, it will also be about the convenience of the customer as, on the one hand, the customer is responsible for having a safe and secure environment for the car to update (e.g., updates are not possible while driving on the highway). On the other hand, the customer needs to get used to new processes. This leads to necessary discussions on both the technical side and from the perspective of the customer's expectation.

Q16 How can one make customers better understand the process and reasoning behind the over-the-air updates?

Answer by Christoph Schmittner
It is important to show the customer clearly why he/she should update the vehicle. If the message is rather "press here to update and do not move your car for half an hour" almost none of the participants will decide to initiate the update. If there are a clear message and reason regarding the added feature, the customer's willingness to update is increased. From a technical perspective, I think updates are not that challenging, as we can already see successful implementations (e.g., for some domains with embedded systems). But there are many questions for society and regulation. Once this issue is addressed, updates will be established quite fast.

Q17 Do you think that in the future, we will see cars put out of service if a critical update needs to be installed? Do you think we will have a classification of software updates to allow scenarios in which you are only allowed to drive your car if it was updated?

Answer by Christoph Schmittner (1/3)
It is a challenge if the car was legal to be driven first, and later on, you remove the legal driving permission. I am not sure if this will happen, even though it would increase security. It will be interesting to see – with our experience in other domains of most operations system, browser updates, and so on – how the update process and the user interaction will take place from technical, regulation, and societal point of view.

Answer by Christoph Schmittner (2/3)
Currently, the UN regulations leave it to authorities to shut down a fleet or a specific vehicle type when there are no security updates available. The regulation states a support time during which the supply chain has to provide updates. It does not specify the time as this is subject to national regulation. It might be 10, 15, or 20 years. This will also be a discussion in society when it comes to end consumer protection rights and how long these rights should last. But after the end of support, when there are no software updates to be expected, the car can drive. Nevertheless, if there is a serious incident that cannot be solved and there is no one to solve it for the vehicle, the authority will call back the type approval, and you are not allowed to drive the vehicle anymore. This is comparable to a situation with replaceable goods – if you are not able to repurchase some specific goods that are mandatory, you are also not allowed to drive further with your vehicle.

Answer by Jörg Schepers (3/3)
I think this is the legal point of them, and legislation is one of the topics, but as Christoph said, also for me, this is a topic of user experience, if an update lasts 20 or 30 minutes and the car is not usable during that timeframe. At least I can understand the reluctance of a user to install it. But from today's point of view, I think the technical solution is available that an update can be done within a minute or even within seconds, so our next MCU generation, which is now in a ramp up, the AURIX second generation has all the features that you can build up an update system that has minimized downtimes for the user experience. If this is being used more widely in the field, also the user acceptance will significantly rise.

4 | Focus II: Challenges and Opportunities in the Security Domain

4.1 Talk 4: - Combining VSOC and Onboard IDS Technologies to Understand Cyberattacks on Vehicles

Shiran Ezra
Product Director, Argus

Summary

Detecting and understanding the complete attack story while proposing an appropriate mitigation plan remains a key challenge in today's cybersecurity landscape, and particularly in the automotive world. This is also one of the fundamental pillars for managing the cybersecurity lifecycle of vehicles.

This talk addresses recent approaches to facilitating the analysis of attacks on vehicles. A common approach is based on end-to-end detection and analysis, which includes off-board analysis with an ASOC system based on different data sources. Such sources include telematics data (available today), as well as onboard IDS events that will become much more prevalent in the near future. Using a case study, the talk covers the process of such an analysis and demonstrates how valuable insights on the attack are created based on an example Ethernet IDS alert. In this case, an Ethernet IDS alert (with contextual information) on a specific unexpected connection is received, but there's a lot more to learn in order to derive further information on the attack. Using Automotive SOC techniques, we are able to understand the indication of a potential attack campaign using a Bluetooth CVE on an IVI. This is the process of shifting from the "WHAT" to the "HOW and WHY", which is crucial in mitigating an attack.

The most obvious mitigation may have been to block the specific communication pattern (for example, via OTA), but instead, we are able to understand that an update to the IVI is even more crucial. These insights are possible when the ASOC is designed using deep automotive knowledge of the makeup of an IDS event, i.e., what types of events will it log, how they can be more widely interpreted, and what their limitations are. In addition, the ASOC's dedicated automotive-specific logic enables analysts to gain a deeper understanding of those events so that they can respond more effectively and efficiently.

It is also critical for the IDS provider to provide relevant contextual information and alerts so that an ASOC will be able to draw deep insights. This requires IDS providers to understand how their events are analyzed in an ASOC. The combined knowledge of how IDS solutions are built and ASOC analysis methods is becoming increasingly important and will play a pivotal role in the automotive industry in order to perform effective and efficient cybersecurity monitoring.

Addressed questions

Q18 When you mention detection of known and unknown violations, how do you guarantee the detection of unknown security violations?

Answer by Shiran Ezra
First of all, in the cybersecurity world, no one will guarantee the detection of unknown attacks. Nevertheless, there are some methods coming from the IT domain to the automotive domain. These are usually based on specific rules for something unexpected, suspicious, or a combination of both. For example, let us assume there are known attacks (could be something violating via invalid packet structure). That's okay. On the other hand, if an increase of CPU in combination with unexpected commands or unexpected packets can be seen, we are able to get a better understanding that something is going on. Together with contextual information and information regarding the network host, our understanding is often increased. This is also the usual practice for trying to detect potential zero-days or unknown attacks in the IT domain, which can also be applied here.

Q19 Can you give an example of a response when the ASOC/VSOC detects an attack on a fleet of vehicles?

Answer by Shiran Ezra
The standard way, given the latency between the vehicle and the ASOC itself, is a passive role of the ASOC. This means it is controlled only with no real-time tracking. Once an issue has been detected, possible responses could be to trigger an over-the-air-update campaign or update some specific security features. There is a lot of ongoing discussion about security controls in the vehicles allowing an update of the configuration in real-time, e.g., issuing a small update to a configuration of a specific filter. There are more potential reactions, which are not necessarily at the vehicle specific level. Responses can be on an organizational, marketing, or regulation level and etc. Looking into the future generation of architectures with ASOC logic being integrated into the vehicle itself leads to very interesting discussions.

4.2 Talk 5: Challenges and Solutions for Automotive Onboard Intrusion Detection Systems

Eduard Metzker
Manager Automotive Cyber Security Solution, Vector

Summary

Megatrends such as the comprehensive connectivity of vehicles and autonomous driving continue to accelerate. The industry largely agrees that cybersecurity is a vital enabler for these megatrends. In recent years massive efforts have been made to equip E/E-architectures with security controls. Signed SW updates, secure boot, and authentic communication are becoming mainstream solutions. Currently, an additional security control receives growing attention from OEMs and Suppliers: So-called Intrusion Detection and Prevention Systems (IDS). While IDS are well established in the classic IT-security landscape, they are not widely applied in the automotive sector. This presentation outlines the specific challenges and requirements for automotive IDS. Additionally, I give insights into promising standardization activities that are moving forward right now.

Addressed questions

Q20 Are the onboard "security event sensors" actual physical sensors or rather software mechanisms that detect the attack?

> **Answer by Eduard Metzker**
> The onboard security event sensors can be both hardware or software sensors. Currently, AUTOSAR is introducing a number of software-based security sensors. However, if there are hardware capabilities on a lower level, the provided interfaces are capable of supporting security events reported from lower-level software components like drivers. We have been in talks with hardware vendors about the capabilities of their devices, which can be used for this purpose.

Q21 What are the criteria the IDSM uses for qualifying an event as a true security event?

> **Answer by Eduard Metzker**
> We do not have proposed hardware rules for specific security events which we standardized, but rather provided a set of configurable filter sets which can be basically configured according to the needs of the OEM and for the specific security event. So this is something that can be fully customized and depends on the specific use case and also on the EE-architecture. Rarely occurring security events (e.g., update of a certificate) do not need a very complex ruleset, while often occurring security events need a more comprehensive set of rules. This is configurable.

4.3 Panel Discussion on Challenges and Opportunities in the Security Domain

Addressed questions

Q22 Regarding the MITRE ATT&CK method that was presented by Shiran, that proposes to ask three questions regarding an attack: *"WHY did it happen?"*, *"HOW did it happen?"* and *"WHAT really happened?"* Is the *"WHY"* is detected based on selection between option or is deduced? If so, what if there is a new *"WHY"*? A new reason for the attack.

Answer by Shiran Ezra
The TTP mutual attack frame describes a set of points to look for. That means there is a baseline, which can be used. This baseline is never enough. That is why, if you look into ASCO or analysis of events, it is developing into the direction of several tiers of analysis. There is basic monitoring and looking into events, but there will also be advanced tiers of inspections, which have cybersecurity expertise. This leveling is what we can expect in the future for events in the backend.

Q23 How do you react to unknown so far attacks?

Answer by Eduard Metzker
The approach is not to recognize actual attacks but rather security events. In the backend, the event will be analyzed and compared to all related security events to see whether it was a security incident or an attack. However, if some security sensor that is important for the attack is missing, the security event will also be missed out and cannot be analyzed in the backend. The question of completion is an ongoing race in security.

Q24 Are there existing methods for detecting unknown attacks?

Answer by Shiran Ezra
Let us talk about a real-world example: In 2017, a critical vulnerability was published about the ability to exploit an airbag ECU with a really unknown method attack, so companies were not ready for that attack. Nevertheless, it was severe and classified. But tracking back showed how the detection of the path could have worked – looking into an unexpected rate of diagnostic commands, for example. There are different methods, and based on specific rules – rate, patterns – you can really identify some things you did not know before.

Q25 Is the standard security event catalog publicly available?

Answer by Eduard Metzker
Shiran and I are colleagues in a working group, so we have adopted some of his ideas regarding the categorization of attack. The group has developed quite a comprehensive catalog covering communication, diagnostics, operation systems, canvas, Ethernet, and so on. We are currently working on pushing this into the upcoming standards. So if you have some access to this standardization group – as many automotive companies have – you have access to the catalog.
The catalog, as well as the whole concept group, does not only focus on the classical type of ECU but also on newer, POSIX-based ECUs, which are more powerful. There is no specific security event yet, which directly relates to autonomous driving, but with respect to the technology, it is applicable. Maybe this is something for the future.

Q26 Do you consider the lack of diversity for hardware and software in the automotive domain an opportunity or threat to cybersecurity?

Answer by Darryl Parisien (1/2)
I do not know which diversity you are referring to, but of course, there are a lot of different silicon and software providers in the automotive sector. In terms of AUTOSAR, in terms of standard solutions, there are not so many. Security though in the automotive sector has only really been moving over the past three years. But there is a challenge for OEMs, Tier1s, and the other solution providers, which are solving these kinds of security issues for automotive and autonomous driving vehicles. It is the challenge of the proper choice of hardware in the underlying security systems. For example, real-time operation systems like vehicles are safety-critical environments, and they need to have full real-time deterministic behaviour. That means you have to do things, and you need to choose your software environment and the tools that you use quite diligently. The more time you spend learning all the different issues, the better opportunity you have to build a much better security posture for whatever automotive solution you are trying to put in place, whether it is autonomous vehicles or whether it is something simpler and it's just a basic classic ECU.

Answer by Shiran Ezra (2/2)
Yes, I fully agree with this realization of Darryl, that some things are more diverse and some things are more similar. Today we see that a lot of software is implemented again not only in similar characteristics but for many different projects. So here we have the same capability, but there are a lot of different components implemented a bit differently in each project. This may increase the risk and vulnerabilities, and then again, it very much relates to what Darryl said before. The standardization and the facts that a lot of things can be statically configured and we know what is going on really helps us. It is a very big base to build much more secure environments where everybody can just install with software. Generally, I think you can look at some advantages and disadvantages at the same time.

Q27 An attacker would prefer as less diversity as possible because if millions of cars implement the same system, an attacker would have access to the entire fleet of cars. Is this correct?

Answer by Darryl Parisien (1/2)
All of this has to be included in designs. If you look at the connected vehicle standards like V2X and C2X, that is how cars are going to communicate. But in the design of that system, you have the ability to recognize misbehavior and address that misbehavior. So once again, you got to look at all the different interfaces and the different things you are doing. If it is just over-the-air-update, this is going to be very proprietary to each OEM. This is not technology that is going to be shared, so it is going to be very difficult to try one OEM implementing it the same way as another.

Answer by Shiran Ezra (2/2)
The topic you raised about similarities and differences is a key question right now. If you have specific software, which I know how to research and analyze, this can lead to a very big scale of an attack. On the one hand, it does have high complexity, and by sharing it among people, it will be much more secure. On the other hand, the scale of an attack is also a big risk if there is a security issue. We need to balance this in the crypto world. The approach was to go away from security through obscurity - to have many things that are proprietary based – but to rather have a thing that is shared. I am not sure it will be the same in the automotive, but it is very interesting to see.

Q28 What is your take when it comes to over-the-air updates and cybersecurity? When they come to Europe, what is going to be the biggest challenge around that?

Answer by Eduard Metzker (1/2)
Over-the-air-updates are coming really fast. For us - as an embedded software vendor - we see a lot of efforts to make over-the-air-updates work. Currently, we are not only working on over-the-air-updates for the actual functional software but also for over-the-air-update for the hardware security modules, which are embedded in the ECUs to provide some crypto agility for the future. We are already addressing not only updates of telematics units or increasing some functions for your navigation, but also topics like updating the HSM software stack, which does the heavy lifting with regards to crypto material and crypto algorithms. So it is on the roadmap.

Answer by Darryl Parisien (2/2)
You also have to look at the scale. So, for example, Tesla is doing a remarkable job with all their new capabilities within their products. But you also have to compare their tens of thousands of vehicles on the road with, for example, VW, which builds 10 million cars per year. So if Tesla has 1% incident rate, it might result in a couple of hundred cars to be addressed in the service environment. For VW, we are talking about 10000s of vehicles, a much bigger issue. Just the volume of all the updates is a pure scale point for those OEMs leading to a much more difficult problem.

5 | Survey Results

5.1 Contributors

In total, 13 contributions were made to the post-event survey. A summary of the contributors' workplace, their role, company/institution, and experience is summarized in Figure 5, under Survey Question (SQ1-SQ4). Contributors' workplace was from 5 different countries. Concerning their current role in the company, the distribution is as follows: 46% have managing roles, 15% research and teaching-oriented (e.g., Ph.D. student, Professor), 15% general technical/engineering (e.g., system architect, project engineer), 15% are consultants and 8% work as experts in the regulatory field. Furthermore, 31% are working in a Tier 1 company, 23% for a semiconductor company, 23% for a company from the security domain, 8% for in a research institution or university, and 15% for other. Finally, 23% of the contributors are involved in the development or research of SAE L3 AD systems, whereas 15% in SAE L5 AD, and 8% in SAE L4 AD. 8% are involved in the development of automotive networking solutions, which is highly relevant for AD, and 31% not involved in AD-related projects.

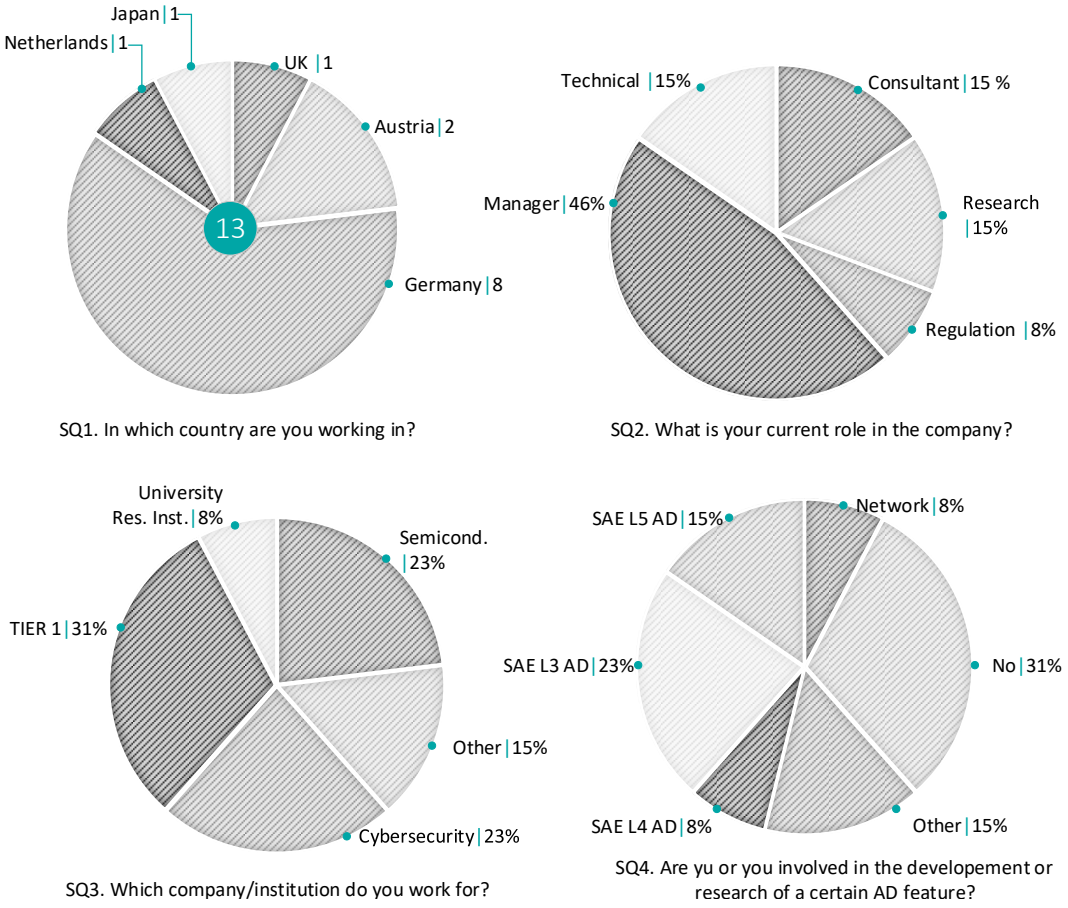


Figure 5: Information about the contributors of the survey.

5.2 Subject: General AD

The topics discussed during the Chapter Event often focused on challenges that are faced during the development of future SAE L4 ADS[1]. Therefore it is important to have a common understanding of when SAE L4 ADS are expected to be on public roads and which ODD SAE L4 AD is bringing the most value. The results of the questions are summarized in survey questions SQ5-SQ6.

SQ5 When do you expect SAE L4 AD features to be available in the Highway operational design domain?

Results
The majority expect SAE L4 AD to be on public highway roads between 2023-2025 (54%). Others expect them to be available in 2026-2028 (38%) or later than 2028 (8%).

SQ6 When do you expect SAE L4 AD features to be available in the Urban operational design domain?

Results
Most contributors (62%) expect SAE L4 AD to be available on public urban roads between 2026-2028. Others expect them to be available later than 2028 (31%). Only 8% expect this to happen in the time between 2023-2025.

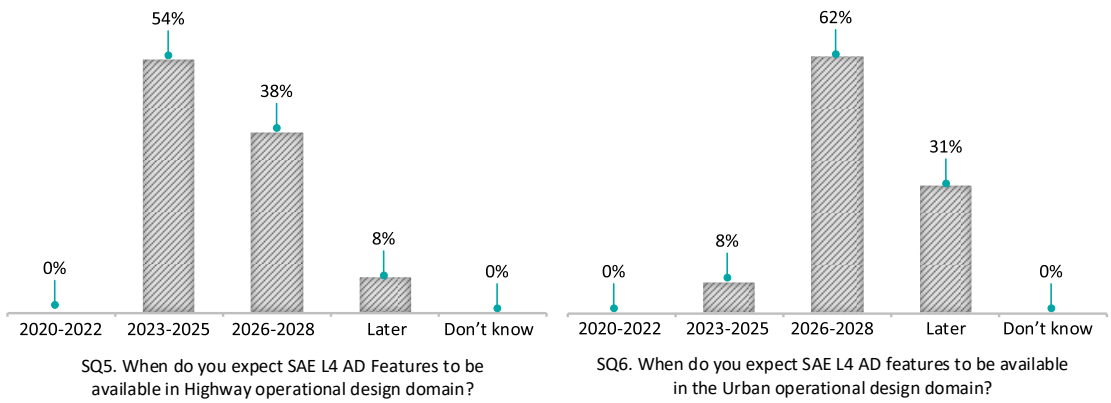


Figure 6: General AD questions - part 1.

[1]SAE L4 ADS performs the complete dynamic driving tasks (DDT) and DDT Fallback (i.e., no fallback-ready driver needed) within a limited ODD.

5.3 Subject: The Autonomous

It is essential for an initiative to continuously receive feedback from contributors on the selected approaches and vision. Hence, we asked the following questions SQ7 and SQ8.

SQ7 Do you think the approach proposed by The Autonomous is feasible?

Results
Figure 7 depicts the results. A greater part (92%) of the participants believe that The Autonomous approach is feasible, whereas 8% do not.

For the sake of transparency, opinions (positive and negative) from the survey contributors are summarized below.[2]

Participants - justifying their answers

Yes: I think Autonomous is a good platfrom for raising awareness and information exchanged, but should be backed up by international specification - and maybe regulation.

Yes: It will be very challenging to make many players in the field who are by nature competitors to work together in a harmonized and standardized way. Still, any attempt taken to establish such collaboration is appreciable.

Yes: Many challenges we are facing today in this area can only be tackled efficiently with a joint approach.

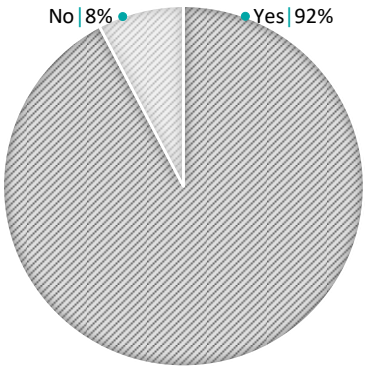


Figure 7: Results from survey question SQ7.

[2]Only spelling and grammar changes have been made. The out-of-context text has been removed.

SQ8 In your opinion, what do you think the main challenges will be for building and maintaining The Autonomous ecosystem?

Results

The list below summarizes the main challenges indicated by the participants.

- To change the *"non-share"* to *"share"* mindset.
- Establish trust amongst stakeholders and common ground on the approach to be taken.
- Bringing the opinions from all stakeholders together and provide this ecosystem within a small time period. Also, the way of sharing the parts of this ecosystem would be an important aspect.
- Define future mobility: privately owned vehicles that stand around for >95% of the time and need to be very flexible on the application level or move to robo-taxies? If we do not decide on one, the energy is at least doubled and may lead to both failing.
- Interoperability and consistent level of security over a wide range of devices (partly unmanaged yet) with long life cycles and various update concepts and different technical restrictions.
- Bringing together the uncoordinated research and development taking place at a diverse range of locations, both academia, and industry.
- Crypto-agility, as the automotive branch, has long lifecycles.

5.4 Subject: Automated Driving and Cybersecurity

SQ9 In your opinion, do you think automotive cybersecurity is given enough emphasis/awareness today?

Results

Figure 8 depicts the results. To a large extent (77%) the participants have answered with *"No"*, whereas 23% with *"Yes"*.

Participants - justifying their answers

No: Cost per item is the main driver for privately owned vehicles. Security measures are very expensive to implement and do not give immediate benefits to end users.

No: Many OEMs and suppliers do not really take security aspects and actual known vulnerabilities into account at the development of new products. Furthermore, car-owners do not see the high possibility of attacks on their cars.

No: Because of a cost-driven decision-making management mindset, the topic has been put aside for a long time, unfortunately also today. The UNECE WP29 will be strongly attacked, like when and how it should be used. I hope the proposed timeline will stay largely unchanged.

No: There is a lack of awareness, experts, and holistic approach for security.

No: Cybersecurity is not an integral part of the development process as, for example, functional safety. It is less regulated and still has to be argued.

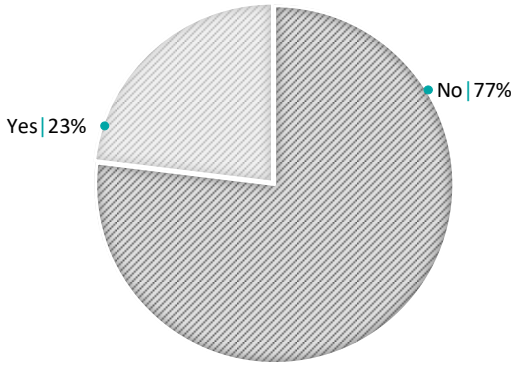


Figure 8: Results from survey question SQ9

Participants - justifying their answers

No: Yet no strict regulation of what level of security has to be implemented for single components/entities. Cybersecurity is still no *"default"* requirement. Security controls often only implemented if required by the customer or has to be argued by cybersecurity teams against functional owners.

No: Coming to research recently after working within the industry for several years, my observations on the emphasis given to cybersecurity within OEMs and tier 1s tend to be inadequate.

No: The automotive sector often sees their products through the customer's eyes and argues that cybersecurity does not offer clear customer benefits. Nevertheless, insecure cars and functions lead to high risks of loss of brand reputation and of costs for OEMs and Tiers.

SQ10 In your opinion, what is the key challenge to be tackled in the context of automotive cybersecurity?

Results

The list below summarizes the main challenges indicated by the participants.

- Bringing cybersecurity awareness to all stakeholders would get very hard.
- Changing the mindset of each company level - from higher management to each key developer, then changing to security by culture.
- Foresee which hardware and software are necessary to guarantee a secure product for more than 15 years in the field.
- Cost, integration, interoperability.
- Harmonization of security requirements. Proof/classification of the level of security and quality of implementation of security controls on the system as well as in the backend and development process.
- Collaborate research and standardization of approaches and processes for implementation.
- Strict regulations and security requirements should be defined and implemented. Continuous IT-security tests have to be mandatory as proof of implemented security along the whole development process.
- Strong connection of security and safety

SQ11 Considering The Autonomous approach for Global Reference Solutions – In your opinion, where is the need for a Global Reference Solution in the automotive cybersecurity context?

Results
The list below summarizes the answers of the participants.

- A reference solution for an update mechanism would be necessary to guarantee an identical procedure and layout for updates in different cars.
- A regulation of the implementation of IT-security is necessary as well as standard-/reference for secure automotive architecture. Key management systems need to be standardized as well as CSMS-implementations.
- Regulation of Cyber Security Implementation, Global Reference PKI / KMS for the handling of cryptographic keys and cryptographic operations, Reference Design for Automotive Architecture, Security Architecture, and CSMS.

SQ12 Do you think that monitoring the correct operation of an automated vehicle at runtime is an important complementary measure for detecting unsafe operation that has resulted due to a security attack?

Results
Figure 9 depicts the results. The majority (92%) of the survey participants believe that runtime monitoring for the correct operation of the automated vehicle is an important measure for detecting unsafe operations resulted from cybersecurity attacks. 8% do not share this view.

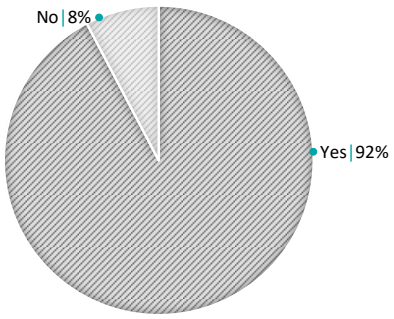


Figure 9: Results from survey question SQ12.

Participants - justifying their answers

Yes: With Monitoring functions, it would be possible to detect anomalies early, and it would be possible to ward off this attack at other cars.

Yes: If you do not monitor, you cannot detect an attack until the result has a major impact on a specific entity or reaches a huge/global scale

Yes: Monitoring is necessary so that the scalability of attacks is decreased and as an early warning system for a successful attack

SQ13 Future automated vehicles will utilize wireless communication for different V2V and V2X features. Are you aware of a wireless communication protocol that implements security measures sufficient for ensuring the secure communication of future automated vehicles?

Results

Figure 10 depicts the results. To a large extent (69%) the participants have answered with *"Yes"*, whereas 31% with *"No"*.

Participants - justifying their answers

Yes: C2C Communication as defined by Car2Car Consortium, most modern wireless protocols, TLS 1.3 for IP based communication

Opinion from a participant

- The problem is not the protocol but the cost of implementation in a privately owned vehicle.
- A constant tracing of the vulnerability of certain protocols is necessary if flaws have been found.

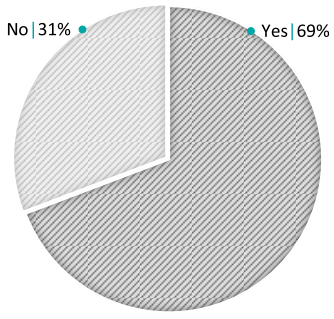


Figure 10: Results from survey question SQ13.

SQ14 Do you think the automotive industry should take an example of other domains when it comes to cybersecurity?

Results
Figure 11 depicts the results. The majority (85%) of the survey participants believe that automotive cybersecurity should take an example from other domains when it comes to cybersecurity. Whereas 15% believe the opposite.

Participants - justifying their answers
Participants that have answered "Yes" have mainly recommended looking into examples from the railway, avionics, IT, telecommunication, government, public agencies, defense, finance, and banking domains.

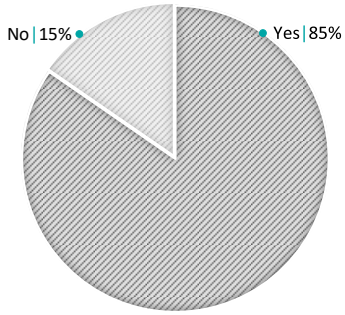


Figure 11: Results from survey question SQ14.

Appendices

A | List of Abbreviations

AD	Automated Driving
ADAS	Advanced Driving Assistance Systems
ADS	Automated Driving System
AI	Artificial Intelligence
ANSI	American National Standards Institute
ASIL	Automotive Safety Integrity Level
AUTOSAR	Automotive Open System Architecture
AV	Automated Vehicle
CD	Commission Draft
CPS	Cyber-Physical System
ECU	Electronic Control Unit
FO/FD	Fail-Operational/Fail-Degraded
FuSa	Functional Safety
ISO	International Standardization Organization
L1	SAE Level 1
L2	SAE Level 2
L3	SAE Level 3
L4	SAE Level 4
L5	SAE Level 5
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
PAS	Publicly Available Specification
SAE	Society of Automotive Engineers
SaFAD	Safety First for Automated Driving
SOTIF	Safety of The Intended Functionality
TR	Technical Report
UL	Underwriters Laboratories
V&V	Verification and Validation

B | Compliance Guidelines

Ensuring safety is the key to gaining acceptance of autonomous mobility on a broad scale. The Autonomous will start this critical discussion by gathering together the complete autonomous mobility ecosystem and facilitate a mutual exchange of ideas by offering various workshops on key topics (Safety & Security, Safety & AI, Safety & Architecture, Safety & Regulation), panel discussions, and keynote speeches.
At The Autonomous, we are committed to ensuring that all discussions take place in full compliance with the rules of competition law. In order to allow for an open exchange of ideas within the limits of the law, this Guideline sets out practicable rules for The Autonomous. Compliance with this Guideline is obligatory for all organizers and participants.

1. **Permitted topics:** Topics which may be covered in discussions, workshops and meetings organized by The Autonomous include:

    1.1. General technical and scientific developments relevant to autonomous mobility;

    1.2. Legislative proposals and/or regulatory measures and their impact on the autonomous mobility ecosystem;

    1.3. The political environment;

    1.4. Current economic developments and general developments in the industry (if publicly available);

    1.5. Exchange of freely available information e.g. economic data available online or in annual reports.

2. **Non-permitted topics:** Participants may not discuss, agree, share information on, or in any other way coordinate their behavior regarding competitively sensitive issues, including:

    2.1. Current and future prices, including selling prices, purchase prices, price components, price calculation, rebates, and intended changes in prices;

    2.2. Terms and conditions of supply and payment for contracts with third parties;

    2.3. Market sharing, including discussions on the division of sales territories or customers (e.g., by size, product type, etc.);

    2.4. Co-ordination of bidding towards third parties, including information on customers' commercial expectations and the firm's proposed response, as well as information on proposed bids (whether a bid will be submitted, for which lots, etc.);

    2.5. Boycotts against certain companies, e.g., agreements not to work with certain customers or suppliers, or to exclude specific companies from discussions on the establishment of a technical standard;

    2.6. Information about business strategies and future market conduct, such as planned investments or the commercial launch of new technologies or products (if not publicly available). In particular, agreements to delay a new technology or to fix the commercial terms of its introduction are prohibited;

2.7. Detailed information on financial performance, such as recent information on profits and profit margins on a non-aggregated basis (if not publicly available);

2.8. Information on internal research and development projects. This comprises estimations about the feasibility of specific technical solutions or the costs attached to the implementation of a specific solution.

3. **Measure to ensure compliance:** In order to ensure compliance and to contribute to an open discussion, The Autonomous will implement the following measures:

   3.1. Attendance by legal counsel: All discussions and workshops will be attended by in-house or external legal counsel. Legal counsel may break off or adjourn the discussion in case of doubts with regard to competition law compliance.

4. **No Reliance:** The purpose of this Guideline is to briefly summarize the competition rules applying to discussions at The Autonomous. It, however, cannot address the full complexity of the applicable law and does not constitute legal advice to participants and their respective firms as to their obligations under competition law. At The Autonomous, we encourage participants to familiarize themselves with the rules of competition law. Should any participant have doubts as to the legality of any discussion in the course of The Autonomous, she/he may:

   4.1. raise such doubts to the legal counsel attending the discussion. The legal counsel shall record any such request in the minutes;

   4.2. leave the meeting if the discussion continues without the participant's doubts having been resolved. The legal counsel shall record the name of the participant as well as the exact time of the participant's departure in the minutes.

C | Standard Settings Guideline

Ensuring safety is the key to gaining acceptance of autonomous mobility on a broad scale. To address security concerns in connection with autonomous driving, safety proves to be the main concern and challenge for mass adoption. These current challenges and associated investment costs cannot be mastered by a single OEM, Tier 1, or Tech company. Just like in aviation, autonomous driving needs to set common technical and ethical standards, legislation, and a process to learn from past incidents and avoid future ones.
At The Autonomous, our mission is to establish a Global Reference Solutions, created by the global community, which facilitate the adoption of autonomous mobility on a grand scale. We are committed to ensuring that this process takes place in full compliance with the rules of competition law. To this end, this Guideline supplements The Autonomous' Compliance Guideline, by setting out practicable rules for standard-setting processes at The Autonomous. Compliance with this Guideline is obligatory for all organizers and participants.

1. **Openness and transparency:** The Autonomous follows an open and transparent approach to participation in its panels, workshops, and other working groups. The establishment of Global Reference Solutions will follow the following principles:

    1.1. Unrestricted participation: involvement is open to all industry stakeholders. Active involvement may only be limited if absolutely necessary (i.e., to prevent inefficiency) and based on objective and non-discriminatory criteria;

    1.2. Transparency: all attendees of The Autonomous, as well as all other stakeholders concerned, will be informed of any announcement, progress, and outcome;

    1.3. Review and comments: Stakeholders not participating in the process will be able to review and comment on the result of the standard-setting process. Any agenda referring to activities of The Autonomous will be disseminated to participants in due course prior to the execution of the activity. Participants shall have the right to comment or to contribute to such an agenda.

2. **Non-exclusivity, free access**

    2.1. No obligation to comply: Participants are free to develop alternative standards or products that do not comply with the evolving standard;

    2.2. Free access to standards: Any developed standards will be accessible for all interested stakeholders (whether or not they participated in The Autonomous) on fair, reasonable, and non-discriminatory terms.

3. **IPR Policy**

    3.1. **Definitions:**

        3.1.1. "Affiliate": any subsidiary or holding company of a participant, any subsidiary of any of its holding companies and any partnership, company, or undertaking (whether incorporated or unincorporated) in which a participant has the majority of the voting rights or economic interest.

3.1.2. "Essential": an intellectual property right is essential where it would be technically (but not necessarily commercially)impossible, taking into account normal technical practice and state of the art generally available at the time of adoption of the standard, to implement the respective standard without making use or infringing the IPR in question.

3.1.3. "FRAND terms": fair, reasonable, and non-discriminatory terms.

3.1.4. "Implement/Implementation": (i) to make, market, sell, license, lease, otherwise dispose or make use of equipment; (ii) repair, use or operate equipment; or (iii) use methods – as specified in the respective standard.

3.1.5. "Intellectual Property Rights" or "IPR": any copyright, Patent, registered design, and any application thereof. IPR does not include trademarks, trade secrets, moral rights, right of know-how, and confidential information.

3.1.6. "Patent": any patent, utility model, or any application for such.

3.2. **Scope of Application:** Participants owning any Essential IPR shall be free to exploit such IPR outside the scope of The Autonomous at their absolute discretion and any revenues or other benefits, which the participant may receive from such exploitation of such Essential IPR, shall be for the participant's own account.

3.3. **FRAND commitment**

3.3.1. Save in the case of any Essential Patents identified in accordance with Section 3.4.4, a participant will give an undertaking that it is prepared to grant licences to anyone wishing to Implement the standard to which the Essential IPR relates:

(i) on FRAND terms;

(ii) to all its Essential IPR relevant for the respective standard;

(iii) to the extent necessary to permit the Implementation of the respective standard.

3.3.2. The undertaking pursuant to Section3.3.1 may be made subject to the condition that those who seek licenses agree to reciprocate.

3.3.3. Where a participant has elected not to declare or has failed to declare any Essential IPR for a given standard in accordance with Section 3.4.4, the participant shall be deemed to have given the undertaking in accordance with the terms of Section 3.3.1.

3.3.4. Both, the participant who has given an undertaking pursuant to Section 3.3.1 or who is deemed to have given an undertaking pursuant to Section3.3.3, and any beneficiaries of such undertaking wishing to acquire a license in accordance with Section 3.3.1, acknowledge and agree that:

(i) They will act in good faith, in order to negotiate a license agreement;

(ii) If both parties have not been able to agree on an Essential IPR license, each party has the right to pursue the matter before the national courts to resolve the matter.

3.3.5. Each participant will ensure that its Affiliates and its Affiliates' successors in title will give an undertaking pursuant to Sections 3.3.1 to 3.3.4 above. If a participant or its Affiliate transfers ownership of Essential IPR that

is subject to an undertaking 3 pursuant to Sections 3.3.1 to 3.3.4 above, such undertaking shall include appropriate provisions in the relevant transfer documents to ensure that the undertaking is binding on the transferee and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding all successors-in-interest. The undertaking shall be interpreted as binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

3.4. **Declaration of Essential IPRs**

3.4.1. Prior to any official adoption of any standard or part thereof, each participant shall provide a written declaration of the Essential IPR relevant to the subject matter. Such declaration shall list:

(i) all potentially relevant Essential IPR held by the participant or its Affiliates;

(ii) filing and registration number, application date and if published the title of the respective Essential IPR;

(iii) terms (i.e., explicitly (non-FRAND terms as opposed to clause 3.3.1, but without specifying royalty rates on any other royalty terms)) on which the participant or its Affiliate is prepared to grant licenses to other participants or any third parties; and

(iv) statement whether the declaration is made subject to the condition that those who seek licenses agree to reciprocate.

3.4.2. In the absence of a declaration of any Essential IPR, the participant will be deemed to have given the undertaking for that Essential IPR associated with the relevant standard or part thereof, in accordance with Section 3.3.3.

3.4.3. Any declaration may identify such Essential Patents, for which the participant or its Affiliate are unwilling or unable to enter into an undertaking to license on FRAND terms in accordance with Section 3.3.1. The declaration shall:

(i) identify any such any Essential Patent, by way of filing number, date, and if published, optionally its title;

(ii) describe in sufficient detail the reasons why the participant or its Affiliate are unwilling or unable to enter into an undertaking to license on FRAND terms in accordance with Section 3.3.1.

3.4.4. Where a participant, in accordance with Clause 3.4.3, has identified an Essential Patent, which the participant, or its Affiliates, is unwilling or unable to license in accordance with Clause 3.3.1, the participant will lose its right to participate and to receive undertakings pursuant to Clause 3.3.1 from other participants in relation to the respective standard or part thereof to which an Essential Patent relates, if:

(i) any other participant informs the Chairman within a reasonable period, in writing, that it does not accept that the reasons in the relevant declaration (as required in accordance with Clause 3.4.3(ii))are reasonable and justified; and

(ii) based on its duly justified non-acceptance of these reasons pursuant to Clause 3.4.4.(i), wishes that the aforesaid participant shall not be able to rely on its right to participate and to receive undertakings pursuant to Clause 3.3.1 from other participants.

3.5. **Disputes concerning ownership of Essential IPR:**If two or more participants claims ownership of the same Essential IPR, the participants claiming ownership shall:

(i) negotiate and resolve the question of ownership in good faith and

(ii) if no solution is found pursuant to section s3.5.1, have the right to pursue the matter before the national courts to resolve the dispute.

D | Acknowledgments

First and foremost, sincere thanks to all keynote speakers, namely Christoph Schmittner, Eduard Metzker, Harry Knechtel, Markus Tschersich, and Shiran Ezra. Their constant support over the past months and in-depth knowledge in the field resulted in outstanding presentations and discussions.

Furthermore, profound gratitude to all the participants at the virtual Chapter Event as well. Their questions enriched and deepened the discussions throughout the workshop.

Special thanks also go to the contributors of the post-event survey who additionally enhanced the quality of discussions and ultimately of this report. In this post-event survey, the contributors were given the option to select whether their names should be mentioned or not. The following is a list of a substantial number of contributors: Andreas Kerschl, Asha Gamage, Berthold Puchta, Borislav Nikolov, Martin Brunner, and Max Turner.

Likewise, warm thanks to all reviewers - for all your comments and ideas for enhancement you have proposed.

Sincere thanks to Infineon, Secunet, and Integrity Security Services for co-hosting this event with The Autonomous. It has been a pleasure working with you on this project.

Many thanks to Georg Kopetz, Marc Lang, Ricky Hudi, and Stefan Poledna for initiating The Autonomous and believing in this cause.

Last but not least, warmest thanks to The Autonomous team - Iulia Alina Baidac, Luisa Griesmayer, Susanne Blum, and Philip Schreiner - for your excellent work and continuous support.

E | Feedback

In our continuous effort to develop The Autonomous as an open platform and space for dialogue among different stakeholders, we welcome all feedback and interest in making safe autonomous mobility a reality. We highly value any comments, ideas, or suggestions you may have to help improve the outcome of this report or contribute to the initiative. Please do not hesitate to contact us at: [*contact@the-autonomous.com*].