

AUTOMOTIVE CYBER SECURITY CONNECTIVITY & SDV WEEK

Europe 2025

18th - 20th November, 2025 • Berlin, Germany

Share New Ideas, Challenge Existing Perspectives
& Take Actionable Intelligence Back To Your Organisations

HEAR FROM 50+ MAJOR AUTOMOTIVE BRANDS & KEY STAKEHOLDERS, INCLUDING:



Felipe Fernandez
Vehicle Cyber Security Head
JLR



Cosimo Magnani
Global Product Cyber Security Manager
Stellantis



Dr. Christian Zimmermann
Bosch Mobility Cybersecurity
Officer for Products
Bosch GmbH



Johannes Krieg
Manager Software Defined Car
Mercedes-Benz Tech Innovation
GmbH



Pankaj Seerapu
Senior Cyber Security Engineer
McLaren Automotive



Jean-Baptiste Mange
Automotive Cybersecurity Expert
Ampere

WATCH THE 2024 HIGHLIGHT REEL



2025 Event Partners



CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

WELCOME


If you attended last year, welcome back! But if you didn't attend in 2024, I'm glad to see you've got your hands on this year's programme. You will be interested to know that **last year's automotive cyber security, connected vehicles and SDV conferences were described as 'first-class', with the largest number of OEM attendees that delegates had seen at any conference that year.** We're once again committed to pulling out all the stops to give the industry an event experience like never before, and one you won't find anywhere else.


This year however, Automotive IQ's Cyber Security, Software-Defined & Connected Vehicles conferences are coming together under one brand.

I'm thrilled to present the **Automotive Cyber Security, Connectivity & SDV Week 2025**. The brand might be new, but we're staying true to our ethos of delivering strategic intelligence and the highest-quality technical case studies on only the most pressing challenges facing the industry, today and in the near future.

Automotive IQ will welcome over 200 vehicle manufacturers, suppliers, thought-leaders, technology companies, insurance providers

and other stakeholders to Berlin, Germany in November 2025, with the objective of giving attendees the opportunity to **share new ideas, challenge existing perspectives & take actionable intelligence back to their organisations to implement it immediately.**

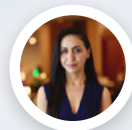
 **18th to 20th November 2025**

 **Berlin, Germany**

I encourage you to view this year's themes, focusing on solving actual technical challenges, discussion on strategic topics previously unexplored plus breakout sessions & workstreams designed to promote collaboration and idea-sharing.

Take a pause from daily activities; come and look at what the industry and your counterparts are doing. Go into 2026 feeling more informed & more prepared than when you arrive at **Automotive Cyber Security, Connectivity & SDV Week 2025.**

Sincerely,



Alishba Jan

Divisional Director
Automotive IQ

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV



**AUTOMOTIVE CYBER SECURITY
CONNECTIVITY & SDV WEEK**
Europe 2025

TWO RAZOR-FOCUSED CONFERENCE TRACKS TAKING PLACE SIMULTANEOUSLY:
1) AUTOMOTIVE CYBER SECURITY TRACK
2) SDV & VEHICLE CONNECTIVITY TRACK

OPPORTUNITY TO ATTEND ONE FOCUSED EVENT OR TO ROAM FREELY BETWEEN BOTH TRACKS AND MIX-AND-MATCH AGENDA SESSIONS

3 DAYS PACKED WITH CONTENT, DELIVERED BY **40+ SPEAKERS**, AND THE OPPORTUNITY TO NETWORK WITH **200+ ATTENDEES**

ABOUT THE AUTOMOTIVE CYBER SECURITY CONFERENCE TRACK

2024 was described by many as the year of compliance with UN ECE R155. However, achieving Type Approval was just one part of the actual **cyber security journey**. **Since then, not only have cyber security needs increased, with devices becoming more accessible and vehicles becoming more connected and software-defined**, vehicles are now much more vulnerable to attacks.

While **artificial intelligence is presenting new opportunities to enhance cyber security frameworks**, AI tools are also generating new information on how to attack vehicles, **weaponizing hackers in never-before-seen ways**. Automotive companies need to **prepare to react and respond** to these new threats.

On a macro-level, automotive companies must think about how they need to **(re)position from a cyber security perspective to gain competitiveness as the industry faces new/difficult market situations**. There is widespread recognition that customers will not pay for a feature called cyber security. This year's conference will dig deep into questions rarely asked, including 'Has the industry gone too far and are we doing too much?' and 'Are activities that the industry has pushed for the last few years justified by the value they are creating?'. Hear executive level **perspectives on ways to reduce cost, make efficiency gains and keep vehicles safe & secure**.

Attend the **Automotive Cyber Security conference track**, to hear complete coverage on these areas among others, with technical case studies focusing on solving actual technical challenges, hands-on discussions and idea-sharing on strategic topics previously unexplored and breakout sessions + workstreams designed to promote collaboration and idea-sharing.

ABOUT THE SDV & CONNECTED VEHICLES CONFERENCE TRACK

Since November 2024, many automotive companies have combined the connected car and SDV units into one department, with the view that having better alignment between on-board software teams and cloud/connectivity teams is imperative to making software-defined vehicles a reality. With all the technologies involved in building software-defined vehicles, the automotive industry is valuing the SDV market at approximately \$146 billion today. Market valuation is expected to rise to 1 trillion dollars by 2030.

Software-defined vehicles and intelligent connectivity is presenting the **largest shift in the automotive industry** and are a stepping-stone towards fully autonomous vehicles. There is a strong desire across the automotive industry to make SDVs a reality. **OEMs are moving past the theory of SDVs and towards the future re-architecture** of their systems, features, and user experiences. Creating **enhanced in-vehicle software and customers experience are vital**, and the most crucial factors for SDV development moving forward.

However, **the overall cost of SDV development continues to be a major concern**, with OEMs under increasing pressure to reduce costs while ensuring vehicles are kept up-to-date. While some OEMs are delaying SDV adoption, Chinese vehicle manufacturers are leading the way in SDV development and rollout. It is more important than ever before that manufacturers and developers continue their investments, with robust approaches in place to meet strict objectives for developing software and products in **shorter timeframes, delivering high-quality products at lower costs**.

Attend the **SDV & Connected Vehicles conference track**, to hear the latest updates on SDV architecture, OEM lessons learned from SDV rollouts, and insight into the customer perspective of SDVs and how the automotive ecosystem can collaborate to produce a vehicle based on these expectations that will last for the next 10 years.

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

PREVIEW THOUGHT-LEADERS AT THE 2025 CONFERENCE



Felipe Fernandez
Vehicle Cyber Security Head
JLR



Cosimo Magnani
Global Product
Cyber Security Manager
Stellantis



Tomasz Werocy
Product Cyber Security
Compliance Officer
Volvo Buses



Malgorzata Kurowska
Head of Information
& Data Governance
Hyundai Europe



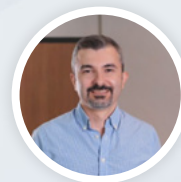
Changhyeok Bae
Principal Software Engineer
**MBition, a Division of
Mercedes-Benz**



Vishal Mishra
Development Engineer
Daimler Truck AG



Safa Caliskan
Cyber Security Technical Lead
Ford Otosan



Utku Karakaya
Automotive SW
Development Manager
TOFAS



Martin Lorenz
Head of Security,
Data & Digitalization
**Verband der Automobilindustrie
/German Association of the
Automotive Industry (VDA)**



Dr. Sheikh Mahbub Habib
Head of Cybersecurity
& Privacy Innovation
Continental



Dr. Markus Tschersich
Head of Security & Privacy
Research and Governance
Continental



Maurice Heymann
Senior Security &
Privacy Research
Continental



Dr. Christian Zimmermann
Bosch Mobility Cybersecurity
Officer for Products
Bosch GmbH



Joachim Fox
Director, Produkt-Governance/
Product Governance (DIQS)
ZF Group



Sergio Scabar
Manager, Cyber Security
Engineering Service
ZF Group

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

PREVIEW THOUGHT-LEADERS AT THE 2025 CONFERENCE



Zeeshan Naeem

Thought Leader | AI &
Cybersecurity for Autonomous
and Connected Mobility
Tier-1 Company
(note: views shared are his own)



Prasanth Gowravajhala

Senior Manager - Software
Defined Vehicles
MHP - A Porsche Company



Augustin Friedel

Mobility
Expert & Advisor
MHP - A Porsche Company



Marc Stottinger

Professor
**RheinMain University
of Applied Science**



William Dalton

Vice President &
Managing Director, North
America & Europe
VicOne



Ioan Tarnovan

Cyber Security Specialist
CyberLifeHacks



Dr. Paul Sanderson

Lead Security Architect
JLR



Pankaj Seerapu

Senior Cyber Security Engineer
McLaren Automotive



Johannes Krieg

Manager Software Defined Car
**Mercedes-Benz Tech
Innovation GmbH**



Felix Maag

Vehicle, Cyber
Security Architect
**Daimler Truck AG & Creator
and Maintainer of "CROWSI"**



Amira Barki

Cybersecurity Architect
Ampere



Jean-Baptiste Mange

Automotive
Cybersecurity Expert
Ampere



Pierpaolo Cincilla

Cybersecurity Expert - Process
& Compliance
Ampere



Prof. Dr. Christoph Krauß

Professor
**Darmstadt University
of Applied Sciences**

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

FOCUS DAY - TUESDAY, 18TH NOVEMBER 2025

Focused on Leveraging Artificial Intelligence (AI) for Automotive Cyber Security & SDV Development

Presentation & Discussion Themes:

- **Real-world threat intelligence:** Gain insight into emerging threat patterns focusing on actual vehicle ECU
- Learn how automotive companies are **integrating artificial intelligence & machine learning in cyber security activities** to make programmes more robust
- Understand the **use of AI in SDV product development for today's vehicles, future platform and E/E architectures** to ensure product are both safe and secure
- Idea-sharing on ways to **leverage AI in daily product development to further enhance & advance cyber security frameworks** and programmes
- Use **AI to speed up software development and testing processes** & decrease cost in both areas
- **Use of AI models in autonomous cars:** How does it impact security?
- **Security for AI:** Idea sharing on **how AI models are protected against cyber-attacks** & prevent cyber security vulnerabilities from being exploited in AI algorithms
- **AI from 'Cloud-to-Car' concept**
- **Cyber Security Roundtable: Training Cyber Security Specialists for Embedded Systems: From Zero to Hero**
- **Intelligent Connectivity VIP Roundtable**

7:30	REGISTRATION & REFRESHMENTS
8:45	AUTOMOTIVE IQ WELCOMES YOU TO AUTOMOTIVE CYBERSECURITY, CONNECTIVITY & SDV WEEK 2025 Alishba Jan , Divisional Director, Automotive IQ
8:50	CHAIRPERSONS' OPENING REMARKS
9:00	PRESENTATION: REAL-WORLD THREAT INTELLIGENCE: GAIN INSIGHT INTO EMERGING THREAT PATTERNS FOCUSING ON ACTUAL VEHICLE ECU Question & Answer Session
9:30	PRESENTATION: LEARN HOW AUTOMOTIVE COMPANIES ARE INTEGRATING ARTIFICIAL INTELLIGENCE & MACHINE LEARNING IN CYBER SECURITY ACTIVITIES TO MAKE PROGRAMMES MORE ROBUST Dr. Sheikh Mahbub Habib , Head of Cybersecurity & Privacy Innovation, Continental Question & Answer Session

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

10:00	PRESENTATION: UNDERSTAND THE USE OF AI IN SDV PRODUCT DEVELOPMENT FOR TODAY'S VEHICLES, FUTURE PLATFORM AND E/E ARCHITECTURES TO ENSURE PRODUCTS ARE BOTH SAFE AND SECURE Question & Answer Session
10:30	MAIN-STAGE PRESENTATION LED BY EVENT PARTNER To reserve this slot, email partner@automotive-iq.com
11:00	MORNING NETWORKING BREAK
11:30	MAIN-STAGE PRESENTATION LED BY EVENT PARTNER To reserve this slot, email partner@automotive-iq.com
12:00	HANDS-ON DISCUSSION: IDEAS-SHARING ON WAYS TO LEVERAGE AI IN DAILY PRODUCT DEVELOPMENT TO FURTHER ENHANCE & ADVANCE CYBER SECURITY FRAMEWORKS AND PROGRAMMES Question & Answer Session
12:45	LUNCH BREAK
1:45	PRESENTATION: USE AI TO SPEED UP SOFTWARE DEVELOPMENT & TESTING PROCESSES, AND DECREASE COST IN BOTH AREAS Question & Answer Session
2:15	PRESENTATION: AI UNDER ATTACK: SECURING AUTONOMOUS CARS FROM INVISIBLE THREATS This session will delve into the critical intersection of artificial intelligence and automotive cybersecurity, addressing both opportunities and challenges in securing AI-driven autonomous vehicles. Zeeshan Naeem , Thought Leader AI & Cybersecurity for Autonomous and Connected Mobility, Tier-1 Company (note: views shared are his own) Question & Answer Session
2:45	'SECURITY FOR AI' BREAKOUT DISCUSSION GROUPS: IDEA SHARING ON HOW AI MODELS ARE PROTECTED AGAINST CYBER ATTACKS & PREVENT CYBER SECURITY VULNERABILITIES FROM BEING EXPLOITED IN AI ALGORITHMS <ul style="list-style-type: none"> Examine the extent to which AI is being used in modelling. Assess how use of AI models in autonomous cars will impact security. Learn how to protect AI models against cyberattacks so that you cannot manipulate the nodes of the AI model. Zeeshan Naeem , Thought Leader AI & Cybersecurity for Autonomous and Connected Mobility, Tier-1 Company (note: views shared are his own) Question & Answer Session

4:00

AFTERNOON BREAK

4:30

TRAINING CYBER SECURITY SPECIALISTS FOR EMBEDDED SYSTEMS: FROM ZERO TO HERO AUTOMOTIVE CYBER SECURITY ROUNDTABLE DISCUSSION LED BY CYBERLIFEHACKS

What will be covered:

- ➔ Hear first-hand experience reports from training and onboarding students, and onboarding.
- ➔ Hear details on actual projects that have been delivered.
- ➔ Continuity and philosophy of training methods and perspectives for the future.
- ➔ Timelines, expectations, and results.

Tudor Tarnovan, Founder & CEO, **CyberLifeHacks**
Ioan Tarnovan, Cyber Security Specialist, **CyberLifeHacks**

INTELLIGENT CONNECTIVITY ROUNDTABLE DISCUSSION LED BY AN EVENT COMMERCIAL PARTNER

To secure this workshop/roundtable, email partner@automotive-iq.com

5:30

NETWORKING DRINKS RECEPTION



CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

MAIN DAY ONE – WEDNESDAY, 19TH NOVEMBER 2025

→ After a series of main-stage plenary presentations and discussions, two conference tracks will run in parallel

→ One track dedicated to **Automotive Cyber Security topics** and the second dedicated to **SDV and Connected Vehicles topics**.

* Attend one track or move between both tracks

JOINT MAIN-STAGE THEMES

- Executive-level views on how automotive companies must position themselves from a cyber security perspective to **gain competitiveness as the industry faces new/difficult market situations**.
- Hear new viewpoints on how to **reduce cost of cyber security while increasing efficiency and keeping vehicles safe & secure**.
- **What do cyber security engineers fear as the industry moves to software-defined vehicles** and vehicles that are connected all the time?
- **Managing automotive software complexity: effective integration strategies in HPC environments**.
- Assessing **new security features for new software-defined vehicle architectures**.

AUTOMOTIVE CYBER SECURITY TRACK THEMES

- **OEM strategies to tackle real-world vehicle security incidents**.
- Cyber security driven-by-design for vehicles that are future-ready – **learn how to plan early to win the market & stay competitive**.
- Learn how to **achieve cyber security in high-performance computing** plus hear updates on future chips.
- New technologies & solutions to **secure and enhance the safety of automated driving technologies & advanced driver assistance systems**.
- Latest **advanced TARA tools** to implement & perform threat analysis & risk assessment.
- & more.

SOFTWARE-DEFINED & CONNECTED VEHICLES TRACK THEMES

- **Year-end roundup of the SDV landscape** and roadmap for 2026 & beyond.
- **Transition from domain-centric to zonal-centric architecture**: Understand how automotive companies are adapting to this change.
- Addressing actual **challenges in zonal-based design** for software-defined vehicles.
- **Customer perception of SDVs**: Are customers willing to pay for software-defined vehicles?
- **How are automotive OEMs going to monetise software-defined vehicles?**
- & more.

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

7:30	REGISTRATION & REFRESHMENTS
8:00	WHAT DO CYBER SECURITY ENGINEERS FEAR AS THE INDUSTRY MOVES TO SOFTWARE-DEFINED VEHICLES AND VEHICLES THAT ARE CONNECTED ALL THE TIME? BREAKFAST DISCUSSION & OPEN DIALOGUE
8:45	AUTOMOTIVE IQ WELCOMES YOU TO AUTOMOTIVE CYBERSECURITY, CONNECTIVITY & SDV WEEK 2026 Alishba Jan , Divisional Director, Automotive IQ
8:50	CHAIRPERSONS' OPENING REMARKS
9:00	EXECUTIVE-LEVEL VIEWS ON HOW AUTOMOTIVE COMPANIES MUST POSITION THEMSELVES FROM A CYBER SECURITY PERSPECTIVE TO GAIN COMPETITIVENESS AS THE INDUSTRY FACES NEW/DIFFICULT MARKET SITUATIONS KEYNOTE PANEL DISCUSSION <p>Automotive companies recognise that no customer pays for a feature called cyber security, and that they will never really create business value for these products and vehicles. Taking a few steps back and taking an eagle-eye view, the industry is asking these questions among others:</p> <ul style="list-style-type: none"> ➔ What is the real status of compliance and cyber security implementation – what is the gap between reality and compliance? ➔ Has the industry gone too far and are we doing too much? ➔ Are the activities that the industry has pushed for the last few years justified by the value they are creating? ➔ What are consequences of having too much cyber security in a vehicle have when companies are operating in what is a difficult market situation? <p>Hear this panel of senior-level experts take a retrospective look at cyber security activities previously undertaken, with the view to determining steps the industry needs to take to position/reposition themselves and gain competitiveness.</p> <p>Felipe Fernandez, Vehicle Cyber Security Head, JLR Dr. Markus Tschersich, Head of Security & Privacy Research and Governance, Continental Joachim Fox, Director, Produkt-Governance/Product Governance (DIQS), ZF Group Sergio Scabar, Manager, Cyber Security Engineering Service, ZF Group Martin Lorenz, Head of Security, Data & Digitalization, Verband der Automobilindustrie/German Association of the Automotive Industry (VDA)</p> Question & Answer Session
9:45	HEAR AN OEM VIEWPOINT ON HOW PRODUCT/VEHICLE CYBER SECURITY HAS EVOLVED IN THE LAST FEW YEARS KEYNOTE PRESENTATION Cosimo Magnani , Global Product Cyber Security Manager, Stellantis Question & Answer Session
10:15	MAIN-STAGE PRESENTATION LED BY A LEAD EVENT PARTNER <p>To reserve this slot, email partner@automotive-iq.com</p>

10:45

MORNING NETWORKING BREAK

➔ AUTOMOTIVE CYBER SECURITY TRACK

11:30

PRESENTATION LED BY VICONE – TITLE TBC

William Dalton, Vice President & Managing Director, North America & Europe, **VicOne**



12:00

CYBER SECURITY DRIVEN-BY-DESIGN FOR VEHICLES THAT ARE FUTURE-READY – LEARN HOW TO PLAN EARLY TO WIN THE MARKET & STAY COMPETITIVE PRESENTATION

Major Chinese automotive companies are using advanced cybersecurity as a way to get customer attention and increase confidence to buy their vehicles. Security is being viewed as a luxury feature, with vehicles becoming more and more connected and the widespread recognition that a compromised vehicle is not only a financial problem, but more importantly a safety and privacy problem.

- ➔ In a first for the event, hear a leading expert share insight on how to think well, plan well and ensure that your cybersecurity programmes are driven by design for vehicles that are ready for the future and win the market.

Tomasz Werocy, Product Cyber Security Compliance Officer, **Volvo Buses**

Question & Answer Session

➔ SOFTWARE-DEFINED & CONNECTED VEHICLES TRACK

YEAR-END ROUNDUP OF THE SDV LANDSCAPE & ROADMAP FOR 2026 & BEYOND STRATEGIC PRESENTATION & PANEL DISCUSSION

- ➔ Explore the SDV architecture landscape and hear lessons learned from OEM SDV rollouts.
- ➔ Gain insight into commonalities and differences between OEM developments in SDVs.
- ➔ Understand the different architectures, where OEMs see developments going, and what challenges they perceive ahead.
- ➔ Discuss how OEMs are looking at the transition to SDVs in the next 2-3 years.
- ➔ Assess challenges faced by global OEMs when developing SDVs, and lessons that can be learnt from Chinese manufacturers.

Augustin Friedel, Mobility Expert & Advisor, **MHP - A Porsche Company**
Johannes Krieg, Manager Software Defined Car, **Mercedes-Benz Tech Innovation GmbH**

Question & Answer Session

TRANSITION FROM DOMAIN-CENTRIC TO ZONAL-CENTRIC ARCHITECTURE: UNDERSTAND HOW AUTOMOTIVE COMPANIES ARE ADAPTING TO THIS CHANGE PRESENTATION

The automotive industry is at a turning point as it transitions from traditional domain-centric architectures to emerging zonal-centric models. This shift is driven by the need to overcome growing complexities in vehicle systems and prepare for a more software-defined future. In this presentation, we'll explore the limitations of current domain-based designs, the challenges companies face during this transition, and the opportunities and complexities introduced by zonal architectures. The goal is to understand not just where the industry is heading, but what it takes to get there.

Prasanth Gowravajhala, Senior Manager - Software Defined Vehicles, **MHP - A Porsche Company**

Question & Answer Session

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

12:30	<p>LEARN HOW TO ACHIEVE CYBER SECURITY IN HIGH-PERFORMANCE COMPUTING PLUS HEAR UPDATES ON FUTURE CHIPS PRESENTATION LED BY A LEADING SEMICONDUCTOR COMPANY</p> <ul style="list-style-type: none"> ➔ Find out plans about the release and capabilities of upcoming security chips. ➔ Examine measures to achieve cyber security on high-performance computing. ➔ Learn how to secure high-performance computers in next-generation vehicles. <p>Question & Answer Session</p>	<p>ADDRESSING ACTUAL CHALLENGES IN ZONAL-BASED DESIGN FOR SOFTWARE-DEFINED VEHICLES PANEL DISCUSSION</p> <ul style="list-style-type: none"> ➔ Discover solutions for inherently distributed zonal design to reduce unnecessary drain on power. ➔ Understand where high-level and low-level control can be used to balance decision-making of zonal computers. ➔ A look at next-generation developments for zonal architecture, and to ingest the ADAS stack into zonal computers. <p>Vishal Mishra, Development Engineer, Daimler Truck AG Prasanth Gowravajhala, Senior Manager - Software Defined Vehicles, MHP – a Porsche Company Question & Answer Session</p>
1:00	NETWORKING LUNCH BREAK	
2:00	<p>PRESENTATION LED BY CYBER SECURITY SOLUTION PROVIDER To reserve this slot, email partner@automotive-iq.com</p>	<p>PRESENTATION LED BY SDV / CONNECTIVITY SOLUTION PROVIDER To reserve this slot, email partner@automotive-iq.com</p>
2:40	<p>NEW TECHNOLOGIES & SOLUTIONS TO SECURE AND ENHANCE THE SAFETY OF AUTOMATED DRIVING TECHNOLOGIES & ADVANCED DRIVER ASSISTANCE SYSTEMS AD/ADAS SECURITY PRESENTATION Question & Answer Session</p>	<p>CUSTOMER PERCEPTION OF SDV: ARE CUSTOMERS WILLING TO PAY FOR SOFTWARE-DEFINED VEHICLES? CUSTOMER-FOCUSED PRESENTATION Utku Karakaya, Automotive SW Development Manager, TOFAS Question & Answer Session</p>
3:10	<p>LATEST ADVANCED TARA TOOLS TO IMPLEMENT & PERFORM THREAT ANALYSIS & RISK ASSESSMENT TARA PRESENTATION</p> <ul style="list-style-type: none"> ➔ Examine cost and capabilities of the different TARA tools. ➔ Learn how to use AI in the TARA and hear real-world experience reports on efficiency and accuracy gains. <p>Question & Answer Session</p>	<p>HOW ARE AUTOMOTIVE OEMs GOING TO MONETISE SOFTWARE-DEFINED VEHICLES? PANEL DISCUSSION Question & Answer Session</p>
3:50	AFTERNOON NETWORKING BREAK	

4:30	MAIN-STAGE PRESENTATION LED BY A LEAD EVENT PARTNER To reserve this slot, email partner@automotive-iq.com
5:00	MANAGING AUTOMOTIVE SOFTWARE COMPLEXITY: EFFECTIVE INTEGRATION STRATEGIES IN HPC ENVIRONMENTS PRESENTATION <ul style="list-style-type: none"> How increasing software complexity in HPC systems introduces integration challenges across diverse components. Strategies for managing and simplifying software integration in HPC (e.g., modular architectures, containerization, environment management). Practical tips and real-world examples. Changhyeok Bae , Principal Software Engineer, MBition Question & Answer Session
5:30	ASSESSING NEW SECURITY FEATURES FOR NEW SOFTWARE-DEFINED VEHICLE ARCHITECTURES CLOSING PANEL DISCUSSION <ul style="list-style-type: none"> Sharing new ways in which cyber security features need to update/adapt as vehicle architectures and designs become more and more advanced, connected and software-defined. Find out which new security tools are available, how they are work and what benefit do they bring to secure new vehicle architectures. Establishing recommendations on the best way to organise vehicle architecture to limit the risks of threat interfaces and attack vectors. Priyankkumar Bidya , Senior Cyber Security Engineer, Scania Group Question & Answer Session
6:00	CHAIRPERSON'S CLOSING REMARKS
6:05	NETWORKING DRINKS RECEPTION



CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

MAIN DAY TWO - THURSDAY, 20TH NOVEMBER 2025

→ After a series of main-stage plenary presentations and discussions, two conference tracks will run in parallel.

→ One track dedicated to **Automotive Cyber Security** topics and the second dedicated to **SDV and Connected Vehicles** topics.

* Attend one track or move between both tracks

JOINT MAIN-STAGE THEMES

- Discuss ways to **meet customer demand for fast vehicle delivery without compromising product security**.
- **ISO/SAE 21434-based automotive risks assessment revisited**.
- Holistic strategies to **update cyber security programmes & future-proof vehicles for the next 10 years**.
- How is the **interaction between product, manufacturing & IT/OT security** influencing overall automotive cyber security?
- Recommendations on ways to **handle cyber security threats & vulnerabilities exposed from software tools** used during vehicle development.

AUTOMOTIVE CYBER SECURITY TRACK THEMES

- GB 44495: China's New Vehicle Cyber Security Standard
- Understand the **Cyber Resilience Act (CRA)** & what automotive OEMs need to do to comply with CRA.
- **European Product Liability Act**: Understand what is in scope, what is out of scope and what the reworked version will mean for automotive cyber security.
- **Post-quantum cryptography** to future-proof vehicles without compromising performance or efficiency.
- Assess the latest tools and tactics for **penetration & fuzz testing** and the ability to automate testing & reporting.
- Best practices for **detecting & reporting vulnerabilities** throughout the development lifecycle.
- Discuss where we are with **intrusion detection systems** from a security capacity & architecture POV.
- & more.

SOFTWARE-DEFINED & CONNECTED VEHICLES TRACK THEMES

- **What will the EU Data Act mean for automotive companies**, and how to manage data accessibility, security & compliance issues.
- Addressing challenges in **managing the transition towards open source**.
- Discuss **last-mile connectivity issues** and solutions to overcome them as much as possible.
- **Multi-access connectivity & security** to enable always-connected, always-secure products.
- Explore how to **bring connectivity in early & build a connected product from the start of the value chain**.
- & more.

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

7:30	REGISTRATION & REFRESHMENTS
8:00	DISCUSS WAYS TO MEET CUSTOMER DEMAND FOR FAST VEHICLE DELIVERY WITHOUT COMPROMISING PRODUCT SECURITY BREAKFAST DISCUSSION & OPEN DIALOGUE
8:40	CHAIRPERSONS' RECAP OF PREVIOUS DAY
8:45	HOLISTIC STRATEGIES ON TO UPDATE CYBER SECURITY PROGRAMMES & FUTURE-PROOF VEHICLES FOR THE NEXT 10 YEARS KEYNOTE PANEL DISCUSSION FOCUSING ON BUILDING RESILIENCE WHILST SECURING VEHICLE ECOSYSTEMS Dr. Christian Zimmermann , Bosch Mobility Cybersecurity Officer for Products, Bosch GmbH Paul Sanderson , Cyber Security Senior Manager/Group Product Owner Vehicle Second Line of Defence, JLR Question & Answer Session
9:30	ISO/SAE 21434-BASED AUTOMOTIVE RISKS ASSESSMENT REVISITED KEYNOTE PRESENTATION The ISO/SAE 21434 standard is the reference for the Automotive on-board Cybersecurity. The standard has been published in August 2021 and the discussions for a second release are starting at ISO/SAE Working Group. This talk will address some limitations of ISO/SAE 21434-based risks assessment and propose improvements related to attack feasibility rating. We will also show how relevant automotive threat agents' capability and motivation levels can be taken into account to enable a focus on relevant attack paths and determine risk values that better reflect the probability of real attacks, thus facilitating risk treatment decisions. Pierpaolo Cincilla , Cybersecurity Expert - Process & Compliance, Ampere Amira Barki , Cybersecurity Architect, Ampere Jean-Baptiste Mange , Automotive Cybersecurity Expert, Renault Group Question & Answer Session
10:15	MAIN-STAGE PRESENTATION LED BY A LEAD EVENT PARTNER To reserve this slot, email partner@automotive-iq.com
10:45	MORNING NETWORKING BREAK

	➔ AUTOMOTIVE CYBER SECURITY TRACK	➔ SOFTWARE-DEFINED & CONNECTED VEHICLES TRACK
11:30	PRESENTATION LED BY CYBER SECURITY SOLUTION PROVIDER To reserve this slot, email partner@automotive-iq.com	PRESENTATION LED BY SDV / CONNECTIVITY PROVIDER To reserve this slot, email partner@automotive-iq.com
12:00	UNDERSTAND THE CYBER RESILIENCE ACT (CRA) & WHAT AUTOMOTIVE OEMs NEED TO DO TO COMPLY WITH CRA CRA PRESENTATION CRA applies to any product with a digital element in the European market. This presentation highlights the importance of CRA in ensuring cyber resilience and implications for the automotive industry. <ul style="list-style-type: none"> ➔ Which vehicle categories does CRA apply to? ➔ What is the overlap between the CRA and ISO 21434 and UN ECE R155? ➔ If you are already complying with R155, find out what else you need to do to comply with CRA. Question & Answer Session	WHAT WILL THE EU DATA ACT MEAN FOR AUTOMOTIVE COMPANIES AND HOW TO MANAGE DATA ACCESSIBILITY, SECURITY & COMPLIANCE ISSUES EU DATA ACT PRESENTATION In September 2025, the EU Data Act will become applicable to all cars, introducing new obligations for automakers around data access, user rights, and transparency. The EU Data Act mandates a shift in how automakers design, manufacture, and manage data generated by their vehicles, and gives customers access to their data. <ul style="list-style-type: none"> ➔ Understand what the EU Data Act will mean in real terms, understand challenges that come with balancing data accessibility, security and compliance and how to manage them. Malgorzata Kurowska , Head of Information & Data Governance, Hyundai Europe Question & Answer Session
12:20	EUROPEAN PRODUCT LIABILITY ACT: UNDERSTAND WHAT IS IN SCOPE, WHAT IS OUT OF SCOPE AND WHAT THE REWORKED VERSION WILL MEAN FOR AUTOMOTIVE CYBER SECURITY EUROPEAN PRODUCT LIABILITY ACT PRESENTATION Question & Answer Session	ADDRESSING CHALLENGES IN MANAGING THE TRANSITION TOWARDS OPEN SOURCE PANEL DISCUSSION <ul style="list-style-type: none"> ➔ Understand why open source is really needed and what the main challenges the industry will face in the transition towards open source. ➔ Explore how open-source solutions can speed up development and delivery of features to improve speed to market. ➔ With Linux adoption increasing in the automotive industry, find out what impact this will have on open-source software adoption. Felix Maag , Vehicle Cyber Security Architect, Daimler Truck AG & Creator and Maintainer of "CROWSI" Question & Answer Session
12:45	NETWORKING LUNCH BREAK	

1:45	<p>POST-QUANTUM CRYPTOGRAPHY TO FUTURE-PROOF VEHICLES WITHOUT COMPROMISING PERFORMANCE OR EFFICIENCY PQC PRESENTATION & PANEL DISCUSSION</p> <p>Maurice Heymann, Senior Security & Privacy Research, Continental Marc Stottinger, Professor, RheinMain University of Applied Science Prof. Dr. Christoph Krauß, Professor, Darmstadt University of Applied Sciences Question & Answer Session</p>	<p>MULTI-ACCESS CONNECTIVITY & SECURITY TO ENABLE ALWAYS-CONNECTED, ALWAYS-SECURE PRODUCTS PRESENTATION</p> <p>Question & Answer Session</p>
	<p>→ CYBER SECURITY INTERACTIVE WORKSTREAMS</p>	<p>→ SDV & CONNECTIVITY INTERACTIVE WORKSTREAMS</p>
2:30	<p>PENETRATION & FUZZ TESTING WORKSTREAM 1</p> <p>Assess the latest tools & tactics for penetration & fuzz testing and the ability to automate testing & reporting.</p> <p>VULNERABILITY MANAGEMENT WORKSTREAM 2</p> <p>Best practices for detecting & reporting vulnerabilities throughout the development lifecycle.</p> <p>INTRUSION DETECTION SYSTEMS WORKSTREAM 3</p> <p>Discuss where we are with intrusion detection systems from a security capacity & architecture POV.</p>	<p>LAST-MILE CONNECTIVITY WORKSTREAM 1</p> <p>Discuss last-mile connectivity issues and solutions to overcome them as much as possible.</p> <p>MULTI-ACCESS CONNECTIVITY WORKSTREAM 2</p> <p>Explore multi-access connectivity & security to enable always-connected, always-secure products.</p> <p>'CONNECTIVITY IN MANUFACTURING' WORKSTREAM 3</p> <p>Explore how to bring connectivity in early & build a connected product from the start of the value chain.</p>
3:30	AFTERNOON NETWORKING BREAK	
4:00	<p>HOW IS THE INTERACTION BETWEEN PRODUCT, MANUFACTURING & IT/OT SECURITY INFLUENCING OVERALL AUTOMOTIVE CYBER SECURITY? PANEL DISCUSSION</p> <p>Safa Caliskan, Cyber Security Technical Lead, Ford Otosan Question & Answer Session</p>	
4:30	<p>RECOMMENDATIONS ON WAYS TO HANDLE CYBER SECURITY THREATS & VULNERABILITIES EXPOSED FROM SOFTWARE TOOLS USED DURING VEHICLE DEVELOPMENT CLOSING PANEL DISCUSSION</p> <p>Vishal Mishra, Development Engineer, Daimler Truck AG Question & Answer Session</p>	
5:00	CHAIRPERSON'S CLOSING REMARKS & END OF AUTOMOTIVE CYBER SECURITY, CONNECTIVITY & SDV WEEK 2025	

2025 EVENT PARTNERS



2025 KNOWLEDGE
& MEDIA PARTNERS



CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

PARTNERSHIP OPPORTUNITIES AT AUTOMOTIVE CYBER SECURITY, CONNECTIVITY & SDV WEEK 2025

Partnering with Automotive IQ provides the most effective opportunity to showcase your company's expertise, innovations and solutions, and target industry professionals in charge of decision making and implementing cybersecurity strategies. With an optimum ratio of attendees to vendors, the **Automotive Cyber Security, Connectivity & SDV Week 2025** conference will provide you with the ideal platform to meet with, and hear directly from leading OEMs, and find out what they expect and require from their suppliers.

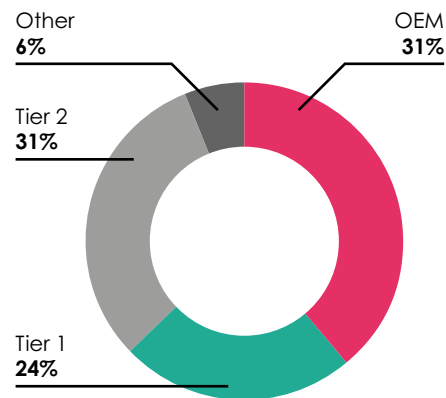
Share your company's best practices in an environment designed to expose new ideas & concepts to solve emerging cybersecurity challenges, and ensure you are front of mind with your target customers.

WHO COULD YOU MEET AT AUTOMOTIVE CYBER SECURITY, CONNECTIVITY & SDV WEEK 2025

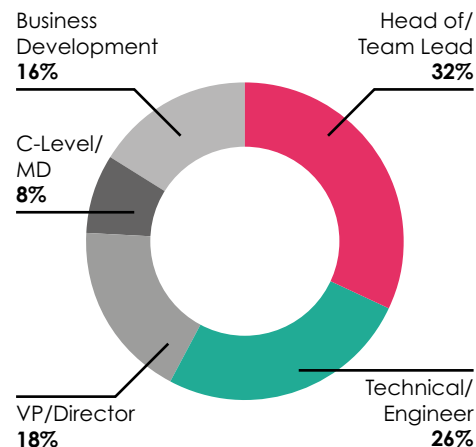
Job Functions

- Cybersecurity
- Product Security
- IT Security
- Data Privacy
- Compliance
- Software
- Autonomous Vehicle/ADAS Security
- EE/Vehicle Electronics
- Manufacturing Security
- Business Development

Market Profile



Job Title Profile



OEM & TIER-1 BRANDS REPRESENTED AT AUTOMOTIVE CYBERSECURITY, CONNECTIVITY & SDV 2024

BMW Group • Volta Trucks
Volkswagen AG • Volvo Buses
Volvo Cars • VinFast Deutschland
Tofas • Stellantis • **Scania Group** • Nissan Technical Centre Europe • **Mercedes-AMG** • Lotus Cars Europe • **JLR** • Hyundai Motor Europe Technical Center
Hyundai Mobis • Maruti Suzuki India • **Daimler Trucks Innovation Center India** • DAF Trucks • **Automobili Pininfarina** NIO • **Iveco Group** • Groupe Renault • **Ford-Werke** • Ford Trucks International • **Ferrari** Robert Bosch GmbH • **ZF Group** Mahle International GmbH • **Marquardt GmbH** • Knorr-Bremse
Valeo • Toyota Boshoku Europe
Forvia • Continental • **CARIAD** Ampere & more

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV

PRICING

Main Conference Days: 19th & 20th November 2025 • Focus Day: 18th November 2025 • **Berlin, Germany**

STANDARD RATE	Lowest Rates	Summer Rate	Super Early Bird Rate	Early Bird Rate	Full Rates
	End 11th July 2025	Ends 15th August 2025	Ends 5th September 2025	Ends 3rd October 2025	from 4th October 2025
2 Day Pass (any two consecutive days – access on 18th & 19th Nov or 19th & 20th Nov)	2795 Save 400 EUR	2895 Save 300 EUR	2995 Save 200 EUR	3095 Save 100 EUR	3195
3 Day Pass (access on 18th, 19th & 20th Nov)	3295 Save 400 EUR	3395 Save 300 EUR	3495 Save 200 EUR	3595 Save 100 EUR	3695

VEHICLE MANUFACTURER RATE	Lowest Rates	Summer Rate	Super Early Bird Rate	Early Bird Rate	Full Rates
	End 11th July 2025	Ends 15th August 2025	Ends 5th September 2025	Ends 3rd October 2025	from 4th October 2025
2 Day Pass (any two consecutive days – access on 18th & 19th Nov or 19th & 20th Nov)	1495 Save 400 EUR	1595 Save 300 EUR	1695 Save 200 EUR	1795 Save 100 EUR	1895
3 Day Pass (access on 18th, 19th & 20th Nov)	1995 Save 400 EUR	2095 Save 300 EUR	2195 Save 200 EUR	2295 Save 100 EUR	2395

BOLT-ON

Access All Areas

(Gain access to both Cyber Security and SDV & Connected Vehicles tracks and receive presentation material from both conferences)

500 EUR

Please note: All 'Early Bird' discounts require payment at time of registration and before the cut-off date in order to receive any discount. Any discounts offered (including team discounts) must also require payment at the time of registration. All discount offers cannot be combined with any other offer. Deadlines for payment can be found on the event website.

Hotel Details: Van der Valk Hotel Berlin Brandenburg • Address: Eschenweg 18, 15827 Blankenfelde-Mahlow, Germany • Phone: +49 33708 580

TERMS AND CONDITIONS

Please read the information listed below as each booking is subject to IQPC Ltd standard terms and conditions.

Payment Terms: Upon completion and return of the registration form full payment is required no later than 5 business days from the date of invoice. Payment of invoices by means other than by credit card, or purchase order (UK Plc and UK government bodies only) will be subject to a \$99 (plus VAT) per delegate processing fee. Payment must be received prior to the conference date. We reserve the right to refuse admission to the conference if payment has not been received.

IQPC Cancellation, Postponement and Substitution Policy:

You may substitute delegates at any time by providing reasonable advance notice to IQPC. For any cancellations received in writing not less than eight (8) days prior to the conference, you will receive a 90% credit to be used at another IQPC conference which must occur within one year from the date of issuance of such credit. An administration fee of 10% of the contract fee will be retained by IQPC for all permitted cancellations. No credit will be issued for any

cancellations occurring within seven (7) days (inclusive) of the conference.

In the event that IQPC cancels an event for any reason, you will receive a credit for 100% of the contract fee paid. You may use this credit for another IQPC event to be mutually agreed with IQPC, which must occur within one year from the date of cancellation.

In the event that IQPC postpones an event for any reason and the delegate is unable or unwilling to attend in on the rescheduled date, you will receive a credit for 100% of the contract fee paid. You may use this credit for another IQPC event to be mutually agreed with IQPC, which must occur within one year from the date of postponement.

Except as specified above, no credits will be issued for cancellations. There are no refunds given under any circumstances.

IQPC is not responsible for any loss or damage as a result of a substitution, alteration or cancellation/postponement of an event. IQPC shall assume no liability whatsoever in the event this conference is cancelled, rescheduled

or postponed due to a fortuitous event, Act of God, unforeseen occurrence or any other event that renders performance of this conference impracticable, illegal or impossible. For purposes of this clause, a fortuitous event shall include, but not be limited to: war, fire, labor strike, extreme weather or other emergency.

Please note that while speakers and topics were confirmed at the time of publishing, circumstances beyond the control of the organizers may necessitate substitutions, alterations or cancellations of the speakers and/or topics. As such, IQPC reserves the right to alter or modify the advertised speakers and/or topics if necessary without any liability to you whatsoever. Any substitutions or alterations will be updated on our web page as soon as possible.

Discounts: All 'Early Bird' Discounts must require payment at time of registration and before the cut-off date in order to receive any discount. Any discounts offered whether by IQPC (including team discounts) must also require payment at the time of registration. All discount offers cannot be combined with any other offer.

Jan Laskowski
enquire@automotive-iq.com
+1 212-973-1042

Illia Grodzynskyi
enquire@automotive-iq.com
+1 212-973-1042

CONTACT OUR DEDICATED EVENT TEAM

EMAIL

+49 3016 639 340

WEBSITE

#CYBERCVSDV