

VDI

## 8th International VDI Conference Cyber Security for Vehicles

July 06-07, 2022, Dusseldorf

- The Future Trends of Cyber Security
- Regulations, Standards & Processes
- Security for Automated Vehicles
- Connected Vehicle Security & Privacy Challenges
- Security of E-Mobility/ E-Vehicles

+ International Best Practices

+ Newest Research & Projects

+ OEM Presentation: Volkswagen AG

Meet international Experts from:



An event organized by VDI Wissensforum GmbH  
[www.vdi-international.com/01K0907022](http://www.vdi-international.com/01K0907022)



08:45 Registration & Welcome Coffee

### 10:00 Chair's Welcome & Opening Address

Dr. Mathias Dehm, Security & Privacy Expert, Continental AG, Germany

## I. Regulations, Standards & Processes

### 10:15 ISO/SAE 21434 in Practice – A Semiconductor Supplier's Perspective

- Application in day-to-day activities
- Interactions with supply chain partners
- Practical insights and recommendations

Timo van Roermund, Director Automotive Security, NXP Semiconductors, Germany

### 10:45 Case Study: CSMS Audit of a Supplier. What does it mean? Experiences made!

- CSMS audit according the ISO CD 5112: What is a CSMS and what is the purpose of audit standard ISO CS 5112?
- Relationships between UNECE reg. and interpretation Nbr. [155], ISO/SAE 21434, VDA ACSMS, ISO CS 5112, ISO 19011
- Conducting of the audit: How was it done? Which points were most discussed?
- Lessons learned

Dr. Thomas Liedtke, Principal Consultant, KUGLER MAAG CIE GmbH, co-author: Antonio Almeida, Senior Process & Quality Management Expert - Cybersecurity, VECTOR Informatik, both: Germany

11:15 ☕ Networking & coffee Break

### 11:45 Auto-ISAC Europe - Need for Collaboration

- Mission of Automotive Information Sharing and Analysis Center (Auto-ISAC) Europe
- Update on Auto-ISAC Europe activities
- Highlights of Auto-ISAC Annual report
- Auto-ISAC threat assessment

Dr. Martin Emele, European Director, Auto-ISAC Europe, Germany

### 12:15 Long-Term Software Updates – A Challenge for the Automotive Industry

- Cybersecurity as a gamechanger for post-SOP software updates
- Specific challenges in the automotive domain
- Software maintenance in the context of cybersecurity operations

Dr. David Förster, Cybersecurity Portfolio Management, Robert Bosch GmbH, Germany

12:45 🍴 Lunch

## II. Security for Automated Vehicles

### 14:15 Security Challenges in Autonomous Vehicles Market Entry Services

- Robotaxi and hub-to-hub commercial truck operations are the first use cases in autonomous driving
- Service management and dispatching processes are suddenly having real world safety implications
- Challenges and solutions for securing a market entry autonomous service in the public domain
- Best Practices for Building Security Protocols

Cristian Ion, Head of Risk Analysis and Secure Engineering, CYMOTIVE Technologies, Germany

### 14:45 The CAMEL project and beyond- AI based cybersecurity

- Results from the concluding H2020 project caramel
- Aftermarket solutions and collaborative CCAM scenarios - The missing link
- Introduction in the subsequent workshop on July 8

Dr. Daniel Fulger, Head of R&D Autonomous & Connected Mobility, Capgemini Engineering, Germany

### 15:15 Domain Separation for Vehicle Networks

- Challenges of integrating online capabilities and safety-critical systems
- Attacker model to consider differences between online and offline attacks
- Effective separation of online and offline domains within the vehicle

Alexander Tschache, Vehicle Security Architect, Volkswagen AG, Germany

15:45 ☕ Networking & coffee Break

## III. Future Cybersecurity

### 16:15 Post Quantum Security Quantum – A Quantum of Crypto?

- Current status of NIST PQC competition and impact on automotive industry
- Impact of crypto agility on the product life cycle process
- Operational security aspects for long-term crypto and security solutions

Prof. Dr. Marc Stöttinger, Professor, Hochschule RheinMain, Germany

### 16:45 Open-Source Hardware Security Module - Opportunities & Challenges

- Open-Source Hardware
- Digital Sovereignty
- RISC-V
- Cryptography

Prof. Dr. Steffen Reith, FB DCSM, Hochschule RheinMain, Germany

17:15 End of Conference Day 1

17:30 👥 Get-together

Relaxed and informal atmosphere for in-depth conversations

09:25 Chair's Opening Address

### III. Future Cyber Security (2)

#### 09:30 Automotive Security: Learning from critical Infrastructures, Industry 4.0, Social Media & eHealth

- Automotive has strong safety traditions that Automotive Security tries to uphold in a cyber world, but modern cars are much more than metal boxes taking us safely from A to B
- They are Critical Infrastructure, networked media hubs, social tools, big data sources, and a projection surface for much more
- For holistic Automotive Security it is therefore crucial to look at how other sectors have „solved“ „cybersecurity“
- Obvious and not so obvious links, analogies, and lessons to be learned

David Fuhr, Head of Research & Innovation, HiSolutions AG, Germany

### IV. Security Testing

#### 10:00 Security Testing – Hands-on Experiences and innovative Methods

- Cybersecurity testing: overview on methods
- Combining different test methods: Static analysis, unit test, fuzzing, pen-test
- Test-Driven Requirements Engineering (TDRE) for cybersecurity
- KPI for effectiveness and efficiency
- Case study with some examples

Dr. Christof Ebert, Managing Director, Vector Consulting, Germany

#### 10:30 How to avoid common Mistakes in Cybersecurity Projects in the automotive Industry

- „Strategic“ mistakes, examples and easy-to-use impulses to overcome such mistakes will be described
- „Technical“ mistakes, examples and applicable proposals to avoid these mistakes will be described
- „Cultural“ mistakes, examples and inputs related to the organizational culture will be provided
- Summary and actionable real-world tips for systematic implementation of automotive cybersecurity

Manuel Sandler, Associate Partner, Cyres Consulting Services GmbH, and, Orhun Suezter, Independent Consultant, both: Germany

11:00 ☕ Networking & coffee Break

#### 11:30 Backdooring of Real Time Automotive OS Devices

- Exploitation techniques in a bare-metal environment
- Bypassing common security mitigations in automotive ECUs
- Case study of a critical security vulnerability in the CAN interface of an ECU
- Lessons learned from crafting an end-to-end exploit of an automotive ECU

David Lazar, Security Researcher, Shaked Delarea, Security Researcher and Ariel Kadyshevitch, Security Research Team Leader, all: Argus Cyber Security, Israel

#### 12:00 Model-based Security-Testing: Yet another Pentest?

- Functional security testing based on given requirements
- Re-Use of threat and risk analysis in V&V activities
- Towards an automation of security tests

Prof. Dr.-Ing. Reiner Kriesten, University of Applied Sciences Karlsruhe/Speaker Institute of Energy Efficient Mobility, and co-author: Florian Sommer, Research Assistant, University of Applied Sciences Karlsruhe, both: Germany

12:30 🍴 Lunch

### V. Connected Vehicles Security & Privacy

#### 13:45 Public Key Infrastructure (PKI) for Cooperative Intelligent Transport Systems (C-ITS)

- The attack surface for the vehicles and the infrastructure rises. The need for secure data exchange between vehicles and with the surrounding infrastructure becomes more and more important
- Cooperative Intelligent Transport Systems (C-ITS) addressed these topics. Cryptographic security mechanisms are needed to establish confidentiality and integrity data exchange. A Public Key Infrastructure (PKI) is needed to provide trusted digital key material
- The specific requirements are defined by ETSI TS 102 941. We talk about the impact for OEMs and Tier 1s and about „Technical Guideline BSI TR-03164“

Harry Knechtel, Head of Development and Production, Division Industry, secunet Security Networks AG, Germany

#### 14:15 Paradigm change now: Overview of Vehicle Cybersecurity

- Back-end infrastructure: Regulations and requirements to change how vehicle parts are manufactured and updated
- Endpoints: Protecting vehicle software system network from attacks and unnecessary traffic
- Communications: Establishing safety and trust for communications between endpoints, as well as back-end infrastructure

Jaeson Yoo, CSO, Autocrypt, South Korea

#### 14:45 Automotive Privacy: Challenges & Opportunities

- (Almost) all data from connected vehicles is likely to be personal data
- Privacy is rarely a design principle of modern cars
- How to address privacy concerns from an engineering perspective

Sarah Syed-Winkler, Specialist Security & Privacy, Continental, Germany

15:15 ☕ Networking & Coffee Break

## VI. Security of E-Mobility / E-Vehicles

### 15:45 E-Mobility Security: The 3 Level Concept

- Three pillars of charging infrastructure: Physical security, user security, and software security
- "Software First" and "Security by Design" – Meaning full compliance with cybersecurity standards from the very first components right through to the finished product
- All other actors have to be involved. Only a jointly coordinated and agreed strategy can ensure capable defence against future cyber threats to electric vehicles, charging stations and the power grid

**Christoph Erni**, Founder and CEO, Juice Technology AG, Switzerland

### 16:15 Secure EV Charging: Plug and Charge

- Future of EV charging: Plug and charge and various stakeholders involved in Plug and Charge ecosystem
- Vehicle to Grid (V2G) use cases and need for cybersecurity
- Public Key Infrastructure (PKI): Technology needed to enable secure authentication and authorization via Plug and Charge
- Regulations & standards for Vehicle to Grid (V2G) communication interface

**Juha Hytönen**, Director of Embedded Security Business Line for Connected Transport, Irdeco, Netherlands

### 16:45 Conference Chair's Closing Remarks

17:00 End of Conference

## Supporting Experts

**Dr. Mathias Dehm**, Security & Privacy Expert, Continental AG, Germany

**Prof. Dr. Christoph Krauß**, Head of Automotive Security Research, INCYDE GmbH and Head of Research Group Applied Cyber Security Darmstadt, Darmstadt University of Applied Sciences, Germany

**Prof. Dr. Jörn Eichler**, Head of Security Engineering, Electric/Electronic Engineering, Volkswagen AG, Germany

**Dr. Christian Köbel**, Senior Project Engineer Cyber Security, Honda R&D Europe GmbH, Germany

## International VDI Workshop

# Lower the hurdle: Implement a cross-stakeholder Nucleus Ecosystem for Automotive Cybersecurity in CCAM – Call for Action

### Date and Venue

July 08, 2022, Dusseldorf

### Time

10:00 - 16:00

### Workshop Chairs

**Dr. Johannes Springer**, Deutsche Telekom / T-Systems International GmbH, Lead 5G@Automotive Program

**Dr. Daniel Fulger**, Head of R&D Automotive & Connected Mobility, Capgemini Engineering

**Wael Yahyaoui**, Senior Technology & Innovation Management Consultant, Capgemini Engineering

### Target Group

Representatives and decision makers of Auto-OEMs, infrastructure, and transportation willing to actively collaborate in a multi-stakeholder cyber security scenario.

### Objectives of the workshop

- Bring together representatives of the stakeholders around Mobility Cybersecurity
- Identify distinguished partners/stakeholders that share the interest in the deployment of a nucleus Cyber Security "Framework" with low entry hurdles, driven by information exchange
- Create a high-level roadmap for the above implementation, simple governance, regulatory, and business processes in a non-safety critical transportation setup, and to continue the action beyond this workshop. The Chairs are willing to organize a follow-up.

### Background

Industry faces a bottleneck in implementing a first Cyber Security Framework across stakeholders with a working business process model beyond the hermetic OEM or infrastructure operator. We propose to put together a group of early adopters designed to move fast towards implementation. The resulting scenario – low-cost, simple ecosystem, lean governance, business processes, and non-critical data content – should be embedded in business with low level of technological innovation to allow roll-out and operationally realistic processes.

Attendees are invited to present their view of the matter and what they perceive as potential directions upgrading their business.

## Exhibitors

EnCo Software GmbH

## Exhibition / Sponsoring

If you want to meet with and reach out to the first-rate experts attending this VDI conference and to powerfully present your products and services to the well-informed community of conference participants, please contact:

**Sandra Schreiner**  
Project Consultant  
Exhibitions & Sponsoring  
Phone: + 49 211 6214-188  
Email: Schreiner@vdi.de



## Become a speaker

Become a speaker at our international VDI Automotive Conferences. Make yourself known in the industry and discuss best practice examples with other international experts. We are looking for speakers on: Automotive Sensor Systems, Smart Construction Equipment, Future of Buses and Connected Off-Highway Machines.

Please submit your topic to:

**Annick Cathrin Pauwels**  
Product Manager International Business  
Phone: +49 211 6214-8646  
Email: Pauwels@vdi.de

## Registration

## Terms and Conditions

**Registrations:** Registrations for conference attendance must be made in writing. Confirmation of your registration and the associated invoice will be mailed to you. Please do not pay your conference attendance fee until you have received our invoice and its invoice number to be stated for transfer. German VAT directives apply. Please state your VAT-ID with your registration.

### Conference venue

Leonardo Royal Hotel Düsseldorf Königsallee  
Graf-Adolf-Platz 8-10  
40213 Düsseldorf, Germany  
Phone: +49 211/38480  
Email: info.royalduesseldorf@leonardo-hotels.com



You will find more hotels  
close to the venue at  
[www.vdi-wissensforum.de/hrs](http://www.vdi-wissensforum.de/hrs)

**Hotel room reservation:** A limited number of rooms has been reserved for the benefit of the conference participants at the Leonardo Royal Hotel Düsseldorf-Königsallee. Please refer to "VDI Conference". For more hotels: [www.vdi-wissensforum.de/hrs](http://www.vdi-wissensforum.de/hrs)

**VDI Wissensforum service package:** The conference package includes the conference documents (online), beverages during breaks, lunch and the get-together on July 6, 2022.

**Conference attendance conditions and terms** can be found on our website:  
[www.vdi-wissensforum.de/en/terms-and-conditions/](http://www.vdi-wissensforum.de/en/terms-and-conditions/)

**Data protection:** VDI Wissensforum GmbH captures and processes the address data of conference participants for their own corporate advertising purposes, enabling renowned companies and institutes to reach out to participants by way of information and offers within their own marketing activities. We have outsourced in part the technical implementation of data processing to external service providers. If you do not want to receive any information and offers in the future, you may contradict the use of your personal data by us or any third parties for advertising purposes. In that case, kindly notify us of your contradiction by using the email [wissensforum@vdi.de](mailto:wissensforum@vdi.de) or any other of the contact options mentioned.

8th International VDI Conference

# Cyber Security for Vehicles



**Register online!**

[www.vdi-international.com/01K0907022](http://www.vdi-international.com/01K0907022)



VDI Wissensforum GmbH  
P.O. Box 10 11 39  
40002 Düsseldorf, Germany  
Phone: +49 211 6214-201  
Fax: +49 211 6214-154  
Email: [wissensforum@vdi.de](mailto:wissensforum@vdi.de)  
[www.vdi-international.com/01K0907022](http://www.vdi-international.com/01K0907022)

VDI Wissensforum GmbH | VDI-Platz 1 | 40468 Düsseldorf | Germany  
[www](http://www.vdi-international.com)

Yes, I will participate as follows:

**Participation Fee + VAT**

**VDI Conference 06.-07.07.2022**  
(01K0907022) € 1890

and/or

**Workshop 08.07.2022**  
(015T945022) € 1320

and/or

**Package Price** (Please tick the boxes)

(Conference + 1 Workshop) € 3060

I am interested in sponsoring and/or exhibition

Participation Fee VDI-Members\* Save 50 € for each Conference Day.

\* For the price category 2, please state your VDI membership number

VDI membership no.

Title

First Name

Last Name (Family Name)

Company/Institute

VAT-ID

Department

Street

ZIP Code, City, Country

Phone

Fax

Email

Please state your invoice address if this differs from the address given

Participants with an invoice address outside of Austria, Germany and Switzerland are kindly requested to pay by credit card.  
Please register at [www.vdi-international.com](http://www.vdi-international.com). Your credit card information will be transmitted encrypted to guarantee the security of your data.