

VDI

# 10th International VDI Conference Cyber Security for Vehicles

June 11-12, 2024, Munich, Germany

- Regulations, Standards, Processes & Homologation
  - Post-Development and Vehicle Operation
  - Future Cyber Security
  - Security Technologies & Further Developments
  - Security Testing
- + Panel Discussion: What Comes Next?  
+ OEM Presentations: Honda R&D Europe - Volkswagen AG - Ampere  
+ International VDI Workshop: Capture The Flag

Meet international Experts from:



An event organized by VDI Wissensforum GmbH  
[www.vdi-international.com/01K0907024](http://www.vdi-international.com/01K0907024)



09:00 Registration & Welcome coffee

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

**Mathias Dehm**, Chief Product Security Officer, Continental AG, Germany

## I. Regulations, Standards, Processes & Homologation

### 10:15 Cybersecurity from a Global Perspective - China and its Rules for Automotive Cyber Security

- International automotive cyber security regulations are evolving & more national standards adding complexity to international type approval
- China is developing a cyber security and data security standard system for ICV
- Strong references to UNECE, ISO and other international standards
- What additional effort is required if, e.g. ISO standards & UNECE regulations are already implemented in an organization

**Janine Funke**, Strategic Area Lead Cybersecurity, co-author: Sergej Weber, both: Kugler Maag Cie by UL Solutions, Germany

### 10:45 The Achilles' Heel of AI-Based Systems in the Automotive Domain: Security Aspects and Challenges

- New challenges in terms of cyber security
- AI specific vulnerabilities and risks
- Threats and attacks along the life-cycle

**Vasilios Danos**, Artificial Intelligence, Head of AI Security & Trustworthiness, co-author: Thora Market, both: TÜVIT (TÜV NORD GROUP), Germany

### 11:15 Cyber Security beyond Cars: Compliance Challenges for OEMs and their Supply Chain

- Small OEMs and the need for CSMS/SUMS compliance
- Small OEMs depend on bigger suppliers and OTS components
- Big OEMs' business models vs. small manufacturers and special vehicle builders
- Secure communication: Changing configurations of trucks & trailers during operation

**Jan-Peter von Hunnius**, Associate Partner and Head of CYRES Consulting, Austria

### 11:45 Strategic Use of Intellectual Property Rights for the Automotive Sector: Creating and Capturing Value

- Use of exclusive rights to derive value out of data sets, architecture, AI solutions and software
- Contracting for security by design in the multi-tiered automotive supply chain
- Organizing security compliance in light of the new and upcoming European legislation

**Maurits Westerik**, Attorney-at-law, co-author: Lot Waemakers, Attorney-at-law, both: Coupry, The Netherlands

12:15  Lunch

## II. Post-Development/ Vehicle Operation

### 13:45 Utilizing Simulated AUTOSAR Security Events for the Detection of Cyber Attacks on Vehicles

- Investigates a realization of the interplay of an in-vehicle IDS system with a monitoring backend system according to UNECE R155
- Digital traces of a real-world cyber attack are mapped to AUTOSAR security events which are integrated into fleet simulations of AUTOSAR events
- The generated data is transferred to a backend system where it is analyzed and different approaches for detecting the attack among a multitude of noise events are evaluated

**Thomas Bitterlich**, Senior Automotive Security Consultant, co-authors: Dr.Grit Pientka, both: T-Systems, Max Engelsberger, Vector all: Germany

### 14:15 Secure Decommissioning: Automotive Security at the End of the Life Cycle

- Security risks at end of life cycle
- Challenges regarding secure decommissioning
- Best practices

**Mathias Löbl**, Security Manager, Bosch Engineering GmbH, Austria

14:45  Networking & Coffee Break

## III. Future Cyber Security

### 15:30 Car Forensic in Protecting Future Cars from Experiences in the Field

Volkswagen AG, Speaker to be announced


### 16:00 Post-Quantum Cryptography on Embedded ECUs

- Post-quantum cryptography
- Embedded Security
- AUTOSAR classic platform

**Claude-Pascal Stöber-Schmidt**, Project Manager Security Engineering; co-authors: Philipp Jungklass & Marco Siebert, all: TT-E1, Embedded Security, IAV GmbH, Germany

### 16:30 Panel Discussion: What comes next?

17:15 End of Conference Day 1

17:45  **Get-together**

At the end of the first conference day, we kindly invite you to use the relaxed and informal atmosphere at our conference dinner for in-depth conversations with other participants and speakers.

09:25 Chair's Welcome

#### IV. Security Technologies & Further Developments

##### 09:30 Cyber Security Considerations for Time-Sensitive Networks in Next-Gen E/E-Architectures

- Introduction – Deterministic and reliable automotive ethernet requires the toolset of time-sensitive networks
- Security analysis of selected TSN protocols (IEEE 802.1AS gPTP and IEEE 802.1Qav CBS)
- Analysis of a sample attack in a testbed environment

**Utku Bal**, Project Engineer, Energy and Digital Systems Research, Honda R&D Europe (Deutschland) GmbH, Germany

##### 10:00 Cyber Security: the HW Challenges of SW-Defined Vehicles

- SDV architectures tend to merge HW, which tends to weaken the cyber security resilience level
- Several solutions and strategies exist in the market to adopt fusion architecture in the same system-on-chip
- The presentation will explore the strategies, missing components or certifications in the existing product roadmaps
- Summarization of the pros/cons of SDV fusion architectures.

**Frederic Ameye**, Cybersecurity Lead, Ampere Software Technology, France

##### 10:30 V2X Security, Mutual Trust, and Data Sharing - Challenges When Introducing a Trust Model for External Data in V2X

- V2X Security ensures the integrity, authenticity, and confidentiality of communications and anonymity of participants
- Misbehavior detection provides measures to identify malfunctioning devices and malicious actors
- Future use cases require the determination of the trustworthiness of external data
- Various techniques support the evaluation of the trustworthiness of data and entities

**Stephan Rein**, Consultant - Software Defined Vehicle, msg systems ag, Germany

11:00  Networking & Coffee Break

##### 11:45 Challenges and Strategies for Enhancing Firmware Security in Automotive Systems

- Common automotive firmware attack vectors
- Firmware reverse engineering for IP theft and competitor analysis
- Technical countermeasures: exploit mitigations and software protection
- Overcoming implementation challenges for diverse automotive environments
- Future directions in firmware security and industry-academia collaboration

**Tim Blazytko**, Chief Scientist, Head of Engineering, emproof, Germany

##### 12:15 Resource Efficient Hybrid Automotive Ethernet Firewall for Smart Switches

- Tool based creation of allow list firewall policies
- Multilevel optimization of filter conditions
- Efficient utilization of switch resources

**Alexander Zeeb**, Senior Solution Manager Embedded Software, Vector Informatik GmbH, Germany

12:45  Lunch

#### V. Security Testing

##### 14:00 The Importance of a Consistent Process from TARA to Testing

- Establishing standardized cybersecurity processes in the dynamic automotive industry
- Overcoming challenges by integrating TARA seamlessly
- Standardization and automation of test procedures for faster iteration of tests and integration
- Utilizing model-based TARA for automated test case generation, improving testing efficiency
- Employing a versatile testing platform for diverse interfaces, saving time and resources in the testing lifecycle

**Harald Petschnik**, Business Innovation Manager, co-authors: Jürgen Wurzinger & Stefan Marksteiner, all: AVL List GmbH, Austria

##### 14:30 Full-Vehicle Penetration Testing - A Silver Bullet for Cyber Security Homologation?

- Current cyber security homologation/ vehicle-type-approval setup for global UN-R 155 member states
- Detailed insights into industry experience as security testing provider
- Description of effective attack vectors, techniques and specific tools to conduct full-vehicle penetration test in context of VTA
- Appreciation of full-vehicle penetration testing compared to testing on component level

**Thomas Irmscher**, Product Manager Security Testing, co-author: Abdallah Ourad, both: ETAS GmbH, Germany

##### 15:00 Protecting Vehicle Architectures: Common Security Pitfalls to Avoid

- Learn how to design more secure vehicle architectures and avoid common security pitfalls at the component (e.g., ECU) and vehicle levels
- Get insights into real-world cases of vulnerabilities found in vehicle architectures
- Practical advice for building testing requirements for Tier 1 suppliers

**Ilya Dubnov**, Security Research Team Lead, Argus Cyber Security, Israel

##### 15:30 Closing Remarks

15:45 End of Conference

# Capture the Flag (CTF): The Hands-On Introduction to Cybersecurity

## Date and Venue:

June 10, 2024

Munich, Germany

## Time

10:00 – 16:00

## Workshop Chair

Abdallah Ourad, Security Tester, ETAS GmbH

## Content

This hands-on workshop offers you a close-to-reality experience to test and exercise your security skills. You will simulate an offensive security engagement from an attacker's point of view and gain insights into hacking methodologies and strategies. You will be solving challenges based on real-life applications and scenarios. The goal is to shape a better understanding of securing your products and services.

## Agenda

### Setup

- Introduction to tools and system under test
- Introduction to the challenges

### Solving challenges, finding flags

- Many diverse challenges to crack
- Varying complexity and difficulty
- Differing ways to solving them
- Employ hacking techniques and use hacking tools
- Experienced supervision and guidance

### Reflection

- Difficulties encountered in solving the challenges
- Unique and creative solutions devised
- Implications for implementing and developing systems

### Target Group

- Security managers, product managers or project managers
- System engineers, software engineers, hardware engineers
- Developers
- Technical understanding on engineering level is required

### Prerequisites

- Bring your own laptop with your preferred operating system and hacking tools. Recommended: Kali Linux and its tools
- If you are new to this: You can install a Kali Linux instance in a virtual machine software. Virtual Box is recommended.

Source: © iStock-technoir



## Sponsoring Partner

**MICRONOVA**  
Software and Systems

## Exhibitors

Argus Cyber Security Ltd.  
CarByte GmbH  
Emproof B.V.  
MicroNova AG  
UL International Germany GmbH

## Supporting Experts

Dr. Mathias Dehm, Chief Product Security Officer, 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

## About us

---



The Association of German Engineers (VDI) is one of the largest technical-scientific associations in Europe. Throughout the years, the VDI has successfully expanded its activities nationally and internationally to foster and impart knowledge about technology-related issues. As a financially independent, politically unaffiliated and non-profit organization the VDI is recognized as the key representative of engineers both within the profession and in public.



## 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: Software Defined Vehicle, Automated Driving 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

Holiday Inn Munich - Westpark  
Albert-Rosshaupter-Strasse 45  
81369 Munich, Germany  
Phone: +49 89 411 113-0  
Email: info.wp@himuc.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 Holiday Inn Munich - Westpark. 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 June 11, 2024.

**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.

## 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:

**Jasmin Habel**

Project Consultant

Exhibitions & Sponsoring

Phone: + 49 211 6214-213

Email: [jasmin.habel@vdi.de](mailto:jasmin.habel@vdi.de)

10th International VDI Conference

# Cyber Security for Vehicles



**Register online!**

[www.vdi-international.com/01K0907024](http://www.vdi-international.com/01K0907024)



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/01K0907024](http://www.vdi-international.com/01K0907024)

VDI Wissensforum GmbH | VDI-Platz 1 | 40468 Düsseldorf | Germany

Yes, I will participate as follows:

**Participation Fee + VAT**

**VDI Conference 11.-12.06.2024**  
(01K0907024) € 1990

and/or

**Workshop Capture the Flag 10.06.2024**  
(01ST945024) € 990

and/or

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

(Conference + 1 Workshop) € 2830

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.