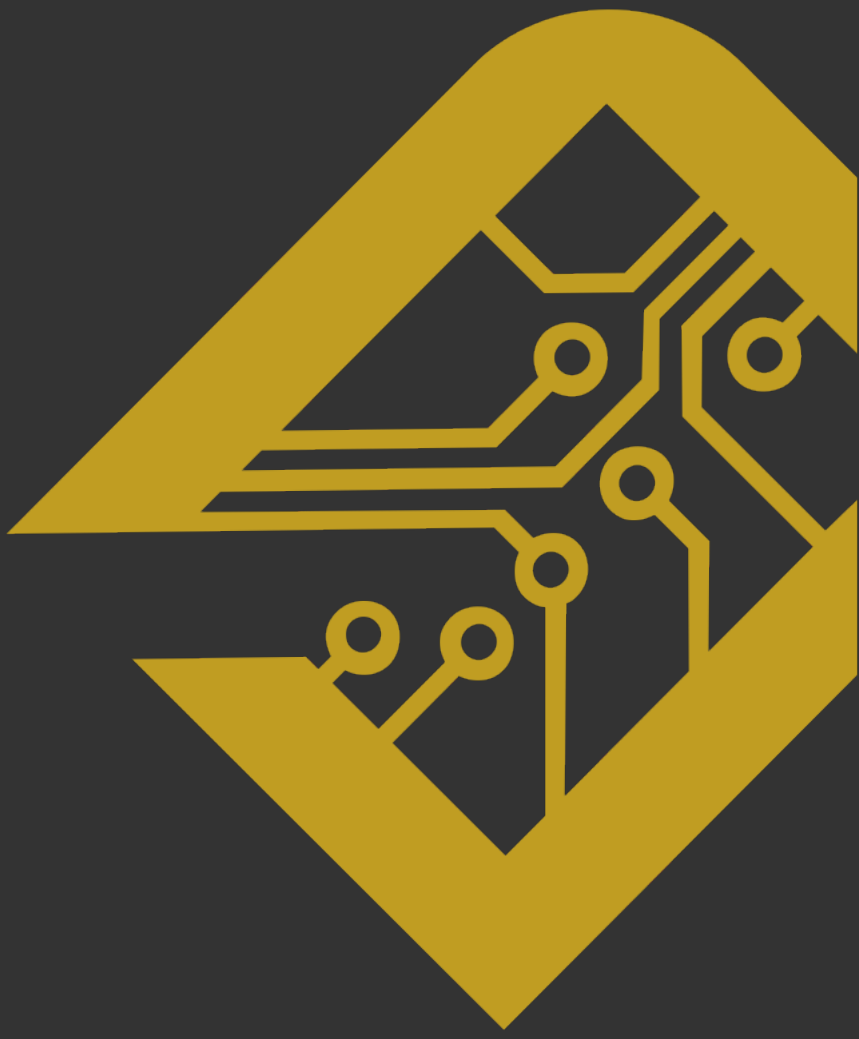
dissecto

Product Guide 2025



Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto

Overview

Building on years of extensive research and our expertise as maintainers and primary contributors to Automotive Scapy, a widely embraced packet manipulation tool, we have developed **dissecto HydraVision**, an intuitive, scalable, and cost-effective solution that simplifies cybersecurity testing of embedded systems. In the meantime, we have become the technological leader in automated security testing, offering PaaS, SaaS, and on-premise solutions to cater to diverse industry needs.

Portfolio:

- **Security Test Environment**
- **Hardware**
- **Consulting & Pentesting**
- **Training & Workshops**

HydraVision

HydraVision is a platform for automated security testing throughout the ECU lifecycle, ensuring compliance with regulations like **UNECE R155** or **GB 44495-2024**. It enables manufacturers and suppliers to perform practical cybersecurity tests on their products automatically and remotely. We offer HydraVision as both a **Platform as a Service (PaaS)** and **on-premise** solution. The platform provides full trans- parency and control, allowing users to comprehensively review, audit, and customize workflows.

Benefits:

- **Always Compliant**
  Stay compliant with industry-specific regulations.
- **Automated & Scalable**
  Reduce manual effort and focus on the right things!
- **Global Collaboration**
  Easy on- and off-boarding of parties around the globe!
- **Cost-Efficient**
  Save up to 75% of security testing & validation costs!

HydraLink

HydraLink is the worlds sleekest USB 3 Gen 1 to Automotive Ethernet Interface! Powered via USB and supporting both 100BASE-T1 and 1000BASE-T1 standards, HydraLink eliminates the need for additional media converters.

HydraLink

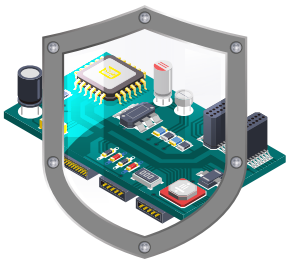
Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto HydraVision

Dissecto HydraVision is a **Platform as a Service** that enables automated security testing over the entire lifecycle of an ECU and ensures compliance with the latest industry- specific standards such as **UNECE R155**, **ISO 21434 or GB 44495**.

With our intelligent security test environment, manufacturers and suppliers can not only easily comply with the new directives and standards, but also carry out practical cybersecurity tests on their products – **automatically and remotely**. This allows attack vectors against your system to be verified and validated in a timely manner. We also offer HydraVision as **on-premise** solution!



Features:

- **Customizable User Dashboard:** Intuitive user dashboard that allows each user to tailor their interface according to their preferences and workflow
- **Full Remote Access:** Project participants can manage and monitor security tests from their location
- **Notifications & Alerts:** Receive immediate updates on the status of your safety tests and be informed of any status changes
- **Security Reports:** HydraVision enables rapid creation of tailored, client-ready PDFs through semi-automated, markdown-based reporting directly editable in VSCode.
- **Testcase Editor:** Easily create, modify and customize test cases to ensure they cover the unique requirements of your system and organization
- **User- & Group Management:** Assign roles based on responsibilities, control access to system relevant data, and optimize collaboration within the security testing environment
- **CI/CD Integration:** Seamlessly integrate HydraVision into your CI/CD pipeline and automate security testing processes to identify vulnerabilities early in the lifecycle
- **Full Control and Transparency:** Over all components of the platform in order to review and audit them and to design your work process as individually as possible.

Benefits:

Always Compliant
Stay compliant with industry-specific regulations.

Automated & Scalable
Reduce manual effort and focus on the right things!

Global Collaboration
Easy on- and off-boarding of parties around the globe!

Cost-Efficient
Save up to 75% of security testing & validation costs!

Interfaces & Protocols

- UDS
- GMLAN
- DoIP
- TCP
- OBD
- UDP
- IPv4
- IPv6
- DHCP
- DNS
- HSFZ
- SOME/IP
- UART
- XCP
- TLS
- CAN & CAN FD
- JTAG
- UART
- (Automotive) Ethernet
- GPIO

Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto HydraLink

The automotive sector is undergoing a paradigm shift from (CAN)-based systems to advance Automotive Ethernet networks like **BroadR-Reach**.

Dissecto HydraLink, a high-performance USB to Automotive Ethernet Interface, is engineered to support this transition seamlessly. With compatibility for **100BASE-T1 and 1000BASE-T1** standards, HydraLink provides a cost-effective solution for reliable diagnostics, testing, and efficient prototyping. Engineered to eliminate the need for additional media converters, HydraLink **simplifies connectivity** while meeting the demands of modern Ethernet protocols in automotive.

Features:

- **USB3 Gen 1 to Gigabit Automotive Ethernet (100/1000):** Provides high-speed data transmission, enabling real-time diagnostics, simulation applications, and fast data exchanges with minimal latency.
- **Supports 100BASE-T1/1000BASE-T1 over single twisted pair:** Fully compatible with modern Ethernet protocols in automotive applications, offering seamless integration into automotive systems with both master and slave modes.
- **Driver Support for Windows, Linux & Mac:** Offers robust compatibility with major operating systems, simplifying integration and ensuring ease of use across platforms.
- **Commercial Temperature Range:** Designed to operate reliably in a variety of conditions, maintaining performance from 0°C to 70°C, making it suitable for diverse environments.
- **2.54 mm Pin Header:** Simplifies connection to any Electronic Control Unit (ECU), making HydraLink an ideal tool for prototyping, testing, and custom automotive projects.
- **Integrated Media Converter:** Directly connects your PC to Automotive Ethernet, eliminating the need for additional conversion equipment and streamlining your setup.
- **Powered via USB:** Operates directly through a USB connection, removing the need for an external power supply and reducing hardware complexity.

Benefits:

Seamless ECU Connection
Direct PC-to-ECU connection for diagnostics / testing

No Extra Hardware
Interface and Media Converter in one small device

Reliable Vehicle Testing
Enables pen-testing and traffic interception (MITM)

Fast, Versatile Integration
Windows, Linux & Mac support for ultimate flexibility

Technical Specifications

- Ethernet Speed: 100 / 1000 Mbit/s Full Duplex
- USB Interface: 3.0 Gen 1
- Supply Voltage: 5V via USB Interface
- Extended Functionality: Master and Slave Support
- Operating Temperature Range: 0°C to +70°C
- Dimensions (LxWxH): 74 x 41 x 16 mm,
- Weight: 55g
- GTIN: 04170000209492

Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto HydraProbe

The dissecto HydraProbe is an essential component of our Hydra environment. Acting as a critical interface between HydraVision and the device under test (DUT), ensuring smooth data flow and control.

This ECU Security Test Tool supports **dual CAN FD**, advanced power management, and **data encryption** for **reliable cybersecurity testing**. With extended functionalities like High-Speed UART and JTAG, the interface is designed for high-performance applications. The HydraProbe can operate within the HydraVision environment or your on-site location.

Features:

- **Dual CAN FD Interface:** To ensure fast and efficient data transmission, dissecto HydraProbe fully supports CAN FD with a bitrate up to 5 Mbps, making it suitable for demanding applications
- **Power Monitoring:** Gain insight into the power consumption of your system and define the ECU's system state. The HydraProbe provides precise and reliable data to analyze accurate monitoring of energy-related parameters
- **Power Switching:** Control and manage the power distribution to connected devices remotely. Our interface enables seamless activation and deactivation of your systems to return to the initial state of the system in the test sequence
- **Voltage Regulation:** Test your system in the voltage limit ranges or outside defined specifications to recognize attack vectors that occur in the event of undervoltage. Increases the test depth
- **Extended Functions:** The programmable co-processor enhances HydraProbe's capabilities, enabling the implementation of advanced functions such as High-Speed UART, JTAG, SPI, Logic Analyzer, and GPIO
- **Dual Power Supply:** The HydraProbe enables up to two systems to be supplied with power. The integration of Power-over-Ethernet (PoE) allows both power supply and communication via single cable
- **Secure Communication:** Interactions between the HydraProbe and its HydraVision instance are encrypted to ensure the integrity and confidentiality of your test data

Benefits:

Fast ECU Data Interface
Supports CAN FD up to 5 Mbps for real-time testing.

Advanced Power Control
Monitors, switches, and regulates ECU power.

Encrypted & Reliable Data
Encrypted data ensures safe test operations.

Extended Functions
Includes UART, JTAG, SPI, and Logic Analyzer.

Technical Specifications

- CAN Bitrate: Up to 5 Mbps (dual CAN FD)
- Ethernet Interface: 1 Gbps
- Extended Functionality: High-Speed UART, JTAG, SPI, Logic Analyzer, GPIO
- Power: 12V to 15V DC, Power over Ethernet (PoE)
- Operating Temp. Range: -40°C to +85°C
- Dimensions (LxBxH): 165 x 105 x 40 mm
- Weight: 450 g

Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto HydraProbe Mobile

HydraProbe Mobile is a compact, **smartphone-based remote testing device** designed for today's dynamic vehicle security workflows. Executing the HydraVision Security Test Environment on a Pinephone Pro™, it connects **directly to the car's network via OBD2 interface**.

Security engineers can **configure test sequences remotely**, allowing field personnel to **execute them on-site** - without needing technical expertise. This makes HydraProbe Mobile ideal for distributed teams, forensic investigations, and production line QA.

Features:

- **Remote Testing, Anywhere:** HydraProbe Mobile enables full-vehicle tests without the tester being physically present. The mobile device acts as a secure, remote probe, executing preconfigured tasks on-site.
- **HydraVision on Pinephone Pro™:** Our complete Security Test Environment runs on the Pinephone Pro™, offering a full suite of automotive security tools in a portable, field-ready format.
- **OBD2 Interface:** HydraProbe Mobile connects directly to the full vehicle network, supporting broad ECU coverage and diagnostics via a robust OBD2 interface with CANFD support.
- **Delegated Test Execution:** Security professionals configure tests remotely. Field users - colleagues, partners, or first responders - can run them with one tap and no technical expertise or setup effort.
- **Secure Communication:** All data exchange between HydraProbe Mobile and HydraVision is encrypted to protect test integrity, sensitive diagnostics, and logs during transmission.
- **Offline Operation with Sync:** Supports offline execution. Test results are stored locally and synced later, making it ideal for remote, air-gapped, or mobile deployment environments.
- **Made for Real-World Teams:** HydraProbe Mobile separates test design from execution, enabling efficient collaboration between central security teams and field operators across industries.

Benefits:

Remote Test Execution
Run scans without being near the vehicle.

One-Tap Test Execution
No training needed to start a test, making delegation easy.

Offline Capable
Data is stored until you regain internet connection

Field-Ready
Can be easily integrated into every corporate workflow

Technical Specifications

- SoC: Rockchip RK3399S, 2x Cortex-A72 + 4x Cortex-A53 @ 1.5GHz
- RAM: 4GB LPDDR4 @ 800MHz
- Internal Storage: 128GB eMMC, expandable via microSD (up to 2TB)
- LCD Panel: 6.0" IPS, 1440×720, Gorilla Glass 4
- Modem: Quectel EG25-G, LTE Cat 4 (global band)
- WiFi & Bluetooth: Wi-Fi 802.11ac, Bluetooth 5.0
- Connectivity: USB-C, OBD2 Port w/ CANFD support
- Battery: 3000 mAh removable Li-Po, 15W
- Dimensions (LxBxH): 161 x 77 x 11 mm
- Weight: 215 g + 75 g Adapter

Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto HydraHat

The dissecto HydraHat is a powerful **Dual CAN FD to Ethernet gateway**, designed for fast, reliable, and secure data communication. Supporting CAN FD with **bitrates up to 8 Mbps** and equipped with a **100 Mbps Ethernet interface**, this device enables seamless data transfer for demanding applications.

With versatile power options, including 6V-24V and PoE support, precise 1µs timestamps, and advanced encryption, the HydraHat is **ideal for time-critical and secure industrial or automotive environments**.

Features:

- **Dual CAN FD Support:** To ensure fast and efficient data transmission, dissecto HydraHat fully supports CAN FD with a bitrate up to 8 Mbps, making it suitable for demanding applications
- **High-Speed Ethernet:** Equipped with a 100 Mbps Ethernet interface, the dissecto HydraHat allows for smooth and rapid data transfer between your CAN and Ethernet networks
- **Versatile Power Options:** dissecto HydraHat can operate within a wide supply voltage range of 6V to 24V, providing flexibility in various industrial and automotive environments. The optional support of Power-over-Ethernet (PoE) enables the operation of the gateway directly via cable
- **Precise Timestamps:** The gateway provides precise time stamps for received CAN frames with a resolution of 1 microsecond (1µs), making it suitable for time-critical applications where synchronisation is crucial
- **Reliable and Secure Data Transmission:** With a robust and reliable design, the dissecto HydraHat ensures a stable and secure data transmission between your CAN and Ethernet systems. It employs industry-standard protocols and advanced encryption to safeguard your data from unauthorized access
- **Easy Integration and Configuration:** The device is designed for straightforward integration into your existing CAN bus and Ethernet networks. The user-friendly interface allows for easy configuration, making setup a breeze, even for those unfamiliar with industrial networks

Benefits:

Fast CAN FD to Ethernet
Transfers data up to 8 Mbps for rapid communication

Flexible Power Options
Supports 6V-24V and optional PoE

Secure Data Transfer
Advanced encryption ensures data integrity

Precise Timestamps
1µs timestamps for time-critical applications

Technical Specifications

- CAN Bitrate: Up to 8 Mbps (dual CAN FD)
- Ethernet Interface: 100 Mbps
- Supply Voltage: 6V to 24V DC
- Power over Ethernet (PoE) Support: Optional
- Timestamp Resolution: 1 microsecond (1µs)
- Operating Temperature Range: -40°C to +85°C
- Dimensions (LxBxH): 85 x 55 x 25 mm
- Weight: 165 g

Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto HydraScan

Dissecto HydraScan is an **advanced plugin for dissecto HydraVision** that enables **full vehicle scans** for various purposes, including forensic analysis and security testing.

By leveraging **HydraProbe Mobile**, users can seamlessly connect to a vehicle's OBD interface and perform full-system assessments via CAN (UDS over CAN) or DoIP (UDS over IP). This allows for **in-depth analysis** of the vehicle's electronic control units (ECUs), ensuring that potential vulnerabilities are identified and security measures are thoroughly evaluated.

Features:

- **Full Vehicle Scans:** Conducts comprehensive security and forensic scans across all electronic control units (ECUs) in a vehicle.
- **HydraProbe Mobile Integration:** Connects seamlessly to a car's OBD interface, enabling plug-and-play scanning via CAN (UDS over CAN) or DoIP (UDS over IP).
- **Automated Vulnerability Detection:** Identifies security gaps, misconfigurations, and potential attack vectors across the vehicle's communication infrastructure.
- **Forensic Analysis Capabilities:** Captures detailed system logs, helping investigators analyze anomalies, unauthorized modifications, or cyberattacks.
- **Customizable Test Cases:** Supports the creation and execution of tailored security tests, ensuring flexibility for different assessment needs.
- **Real-Time Monitoring & Reporting:** Provides live status updates and generates detailed security reports within HydraVision's centralized dashboard.
- **Compliance & Standard Verification:** Ensures adherence to automotive cybersecurity standards such as UNECE R155, ISO 21434, and industry best practices.
- **Scalable & Remote Accessible:** Works as a scalable solution for both single-vehicle assessments and fleet-wide security testing, with full remote access for distributed teams.
- **Intelligent Data Correlation:** Aggregates and analyzes scan data from multiple ECUs, providing a holistic view of the vehicle's security status.
- **Seamless CI/CD Integration:** Allows integration into Continuous Integration/Continuous Deployment (CI/CD) pipelines, ensuring security is tested throughout the development lifecycle.

Benefits:

ECU Protocol Scanning
Supports ISOTP & UDS for deep system insights.

ECU State Mapping
Reveals attack surfaces through reverse engineering.

Forensic Data Analysis
Monitors ECU data flow for investigations.

Full Vehicle Scan
Scans full vehicle networks via OBD for security tests.

Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto Pentesting

We are offering pentests of embedded systems, automotive systems and hardware components. The process targets specific systems and goals, using various methods to breach security. Results inform the client of vulnerabilities and recommend mitigation strategies.

Penetration testing is integral to security audits, mandated by standards like **UNECE R155, ISO 21434 or GB 44495** and supporting risk assessments. Penetration tests can be tailored to meet your individual requirements!

Features:

- **Comprehensive Systems Testing:** We conduct thorough security tests for entire vehicles, including ECUs and embedded systems, ensuring robust protection against potential vulnerabilities.
- **Specialized Network and Interface Testing:** Our package offers in-depth testing services for vehicle control units, using reverse engineering, hardware checks, and protocol fuzzing to identify vulnerabilities and enhance vehicle security.
- **Hardware-Security Analysis:** We carefully examine hardware components like processors and microcontrollers to uncover potential security gaps and recommend measures to fortify ECUs and microcontrollers against threats
- **Proof of Concept Attacks and Showcases:** We craft practical attack demonstrations to showcase potential vulnerabilities and provide actionable insights for strengthening security measures.
- **Customized Scope of Testing:** Our testing scope includes reverse engineering, hardware security assessments, and robustness testing through fuzzing, ensuring comprehensive coverage of potential attack vectors. However, the specific scope is always agreed with the customer in advance.
- **Detailed Reporting and Results:** Clients receive detailed reports outlining findings, risk assessments, and proposed countermeasures, along with technical scripts where feasible for reproducing findings.

Work Results

Result 1: At the start of the project a test plan is created, which shows the individual steps and processes.

Result 2: dissecto GmbH delivers a results report with the following contents:
- Management summary, summary of top risks with attack paths and requirements for counter measures
- Description of scope and out-of-scope
- A description of the test procedure
- A description of the test setup (incl. SW/HW versions of all components involved)
- All findings including concrete traces that show the security problem mentioned, classification of the findings according to the specified risk metrics and proposed countermeasures

Result 3: With the help of our fully automated Platform as a Service HydraVision, the client will receive continuous detailed reports on weak points of the integrated control units (continuous re-testing)

Result 4: If technically possible, scripts are provided to reproduce the findings.

Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto Workshops

Stay ahead in the evolving automotive landscape with our cybersecurity workshops, designed to empower you with **practical, hands-on** skills and insights into embedded and vehicle security.

Explore the fundamentals of automotive protocols, ECUs, and attack surface identification. Learn cutting-edge techniques in hacking real cars, from firmware reverse engineering to OEM design philosophies. **Fully customizable**, our workshops ensure you gain the expertise to safeguard interconnected vehicles against emerging cyber threats.

Features:

- **Attack Surface Identification:** Learn to pinpoint vulnerabilities on Electronic Control Units (ECUs) for effective security assessments
- **Low-Level CAN Communication:** Understand the intricacies of CAN communication and vulnerabilities at the protocol's foundational level
- **Vehicle Architecture Overview:** Gain insights into prevalent vehicle architectures and network topologies for comprehensive understanding
- **Relevant Protocols Mastery:** Acquire knowledge about essential protocols utilized in contemporary vehicles for targeted security analyses
- **Hands-On Network Scanning:** Engage in practical automotive network scans to identify potential vulnerabilities and weaknesses
- **Diagnostic Protocol Exploitation:** Explore techniques to attack diagnostic protocols, including firmware dumping and reverse engineering for in-depth analysis
- **Security Access Breaching:** Break through security access mechanisms deployed in modern vehicles to assess system vulnerabilities effectively
- **Immobilizer Basics:** Get an overview about current immobilizer systems

Exercise Environment

Remote ECU: The remote system facilitates the handling of the ECUs by avoiding wiring efforts. Available Manufacturers: BMW, VW, Opel, Tesla, Mercedes, Audi. The following ECU types are available: Body Domain Controllers, Gateway ECUs, Telematics ECUs, Airbag ECUs, Dashboard ECUs, Immobilizer ECUs

Physical ECU: Various ECUs will be brought on-site for training in hardware reverse engineering as well as handling ECUs

Virtualized Vehicle: By simulating a vehicle and CAN messages while driving, participants can learn how to handle low-level CAN messages and how to manipulate them

Virtualized ECU: A modified digital twin of a real ECU, which includes various IT security exercises that can be performed by the participants independently

Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

Module Outline

- **Fundamentals of vehicular networks and protocols**

- **Controller and Networks**
  - Low-Level Attacks
  - Scapy CAN layer
  - DBC file format
  - MITM attacks
  - AUTOSAR SecOC
  - Fuzzing techniques

- **ISOTP**
  - Basics
  - MITM attacks
  - Network Scanning

- **UDS/GMLAN**
  - UDS and GMLAN in Scapy
  - Security Access
  - Network Scanning

- **DoIP / HSFZ**
  - Basics of protocols
  - DoIP and HSFZ in Scapy
  - Handling and tools

- **SOME/IP**
  - Basics of SOME/IP
  - Tools

- **CCP / XCP / OBD2**

- **OEM-specific knowledge**
  - Attacks on vehicles
  - Security access implementations
  - Update processes
  - Overview of OEM-specific tools
  - Electronic immobilizers

- **Hardware reverse engineering**
  - Identification of interfaces
  - Basics of JTAG
  - Ways to read out firmware

- **Reverse Engineering**
  - Ghidra basics
  - Overview of common processor architectures
  - Handling memory maps
  - Reverse engineering of peripheral components
  - Handling of interrupt vector tables
  - Identification of automotive protocols e.g. UDS
  - Reverse engineering of security access algorithms
  - Intercommunication of bootloader and flashloader
  - Reverse engineering of state machines and AUTOSAR

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com

dissecto

Security Testing, Simplified.

dissecto GmbH,
Franz-Mayer-Str. 1, 93053 Regensburg,
GERMANY
www.dissecto.com
contact-us@dissecto.com
+ 49 941 4629 7370