
SBA
Research

You wouldn't HACK a CAR?

A Pentester's approach to embedded security on automotive ECUs

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

FFG
Forschung wirkt.

wirtschafts
agentur
wien
Ein Fonds der
Stadt Wien

European
Commission

FWF
Der Wissenschaftsfonds.

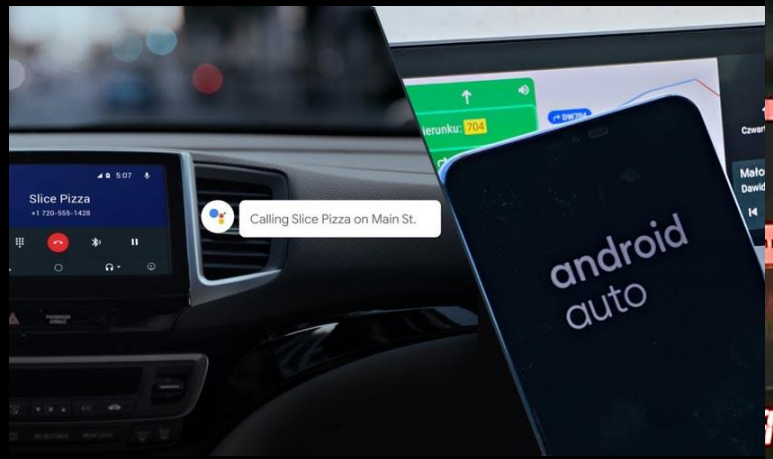
netidee
OPEN INNOVATIONS

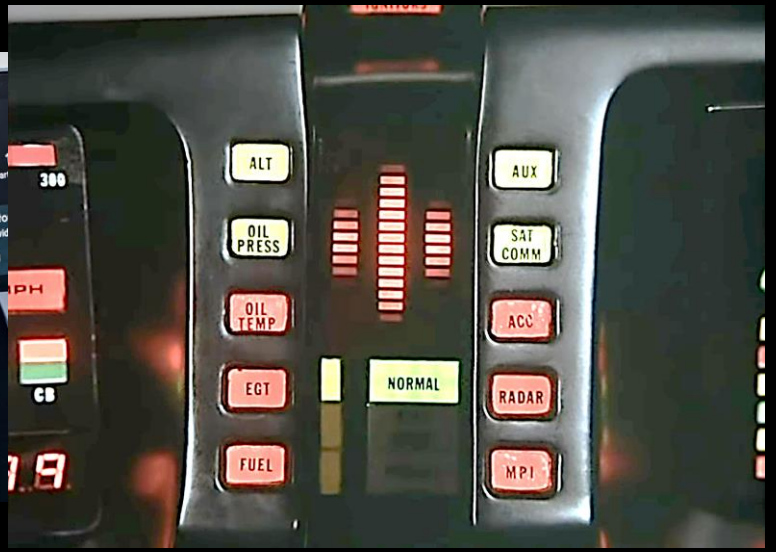
Autonomous driving

Image: https://bernardmarr.com/how-tesla-is-using-artificial-intelligence-to-create-the-autonomous-cars-of-the-future/

Images: Knight Rider, Universal Television

Voice Control





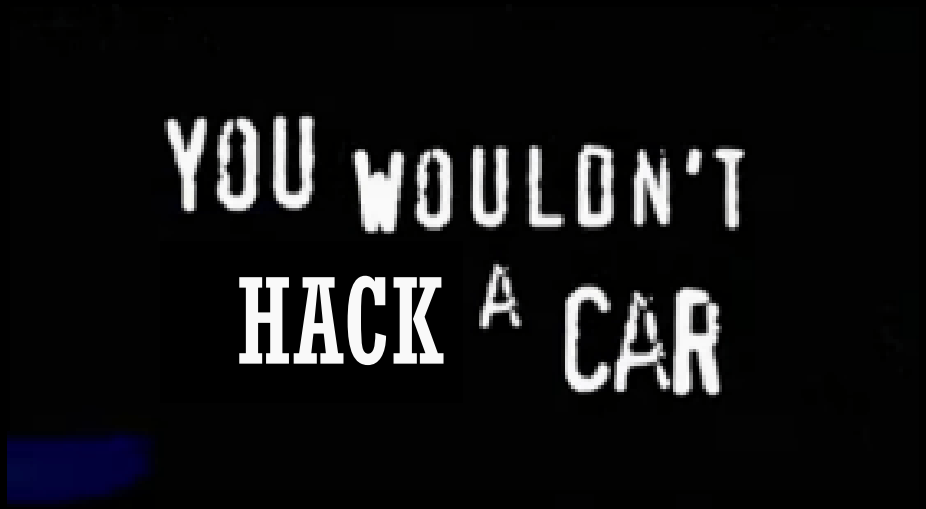
https://www.ciobulletin.com/mobile/google-assistant-android-auto-ai

Images: Knight Rider, Universal Television

Infotainment

Image: https://www.global-infotainment-system.com/

Images: Knight Rider, Universal Television



https://torrentfreak.com/sorry-the-you-wouldnt-steal-a-car-anti-piracy-ad-wasnt-pirated-170625/

Car Architecture

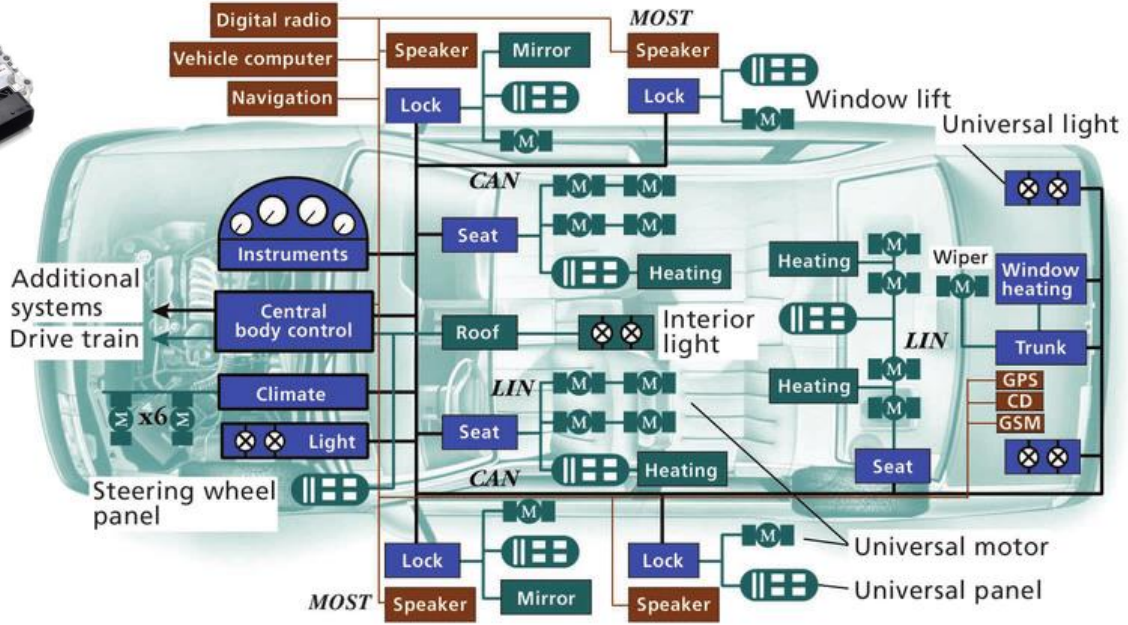
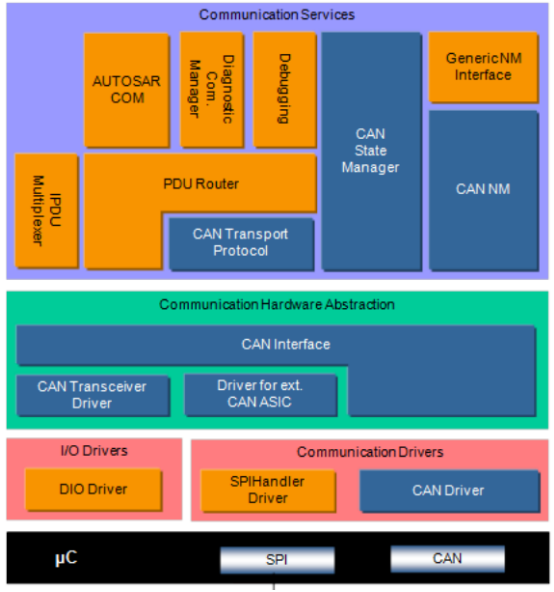


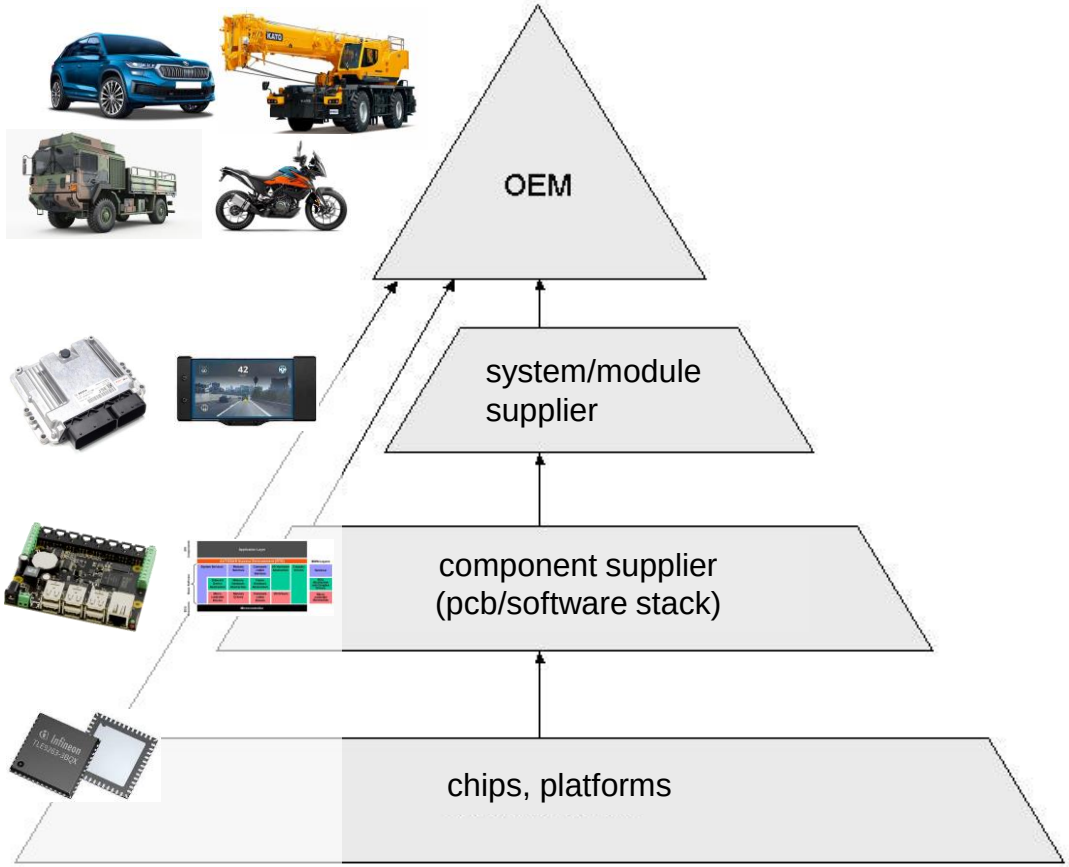
Image: https://www.researchgate.net/figure/One-subset-of-a-modern-vehicles-network-architecture-showing-the-trend-toward_fig1_2955571

Example: AutoSAR, Platform, Chip, Software



between 70 and 100 ECUs being installed in every modern vehicle

Image: Specification of CAN Interface AUTOSAR CP Release 4.3.1, p11


OEM
system/module
supplier
component supplier
(pcb/software stack)
chips, platforms

Jeep Hack (2015)

- vulnerability in the UConnect infotainment system
- cars exposed port 6667 via the Sprint 3G network
- initially 2695 vehicles were found
  - Dodge Viper, RAM, Jeep Cherokee, Chrysler, …

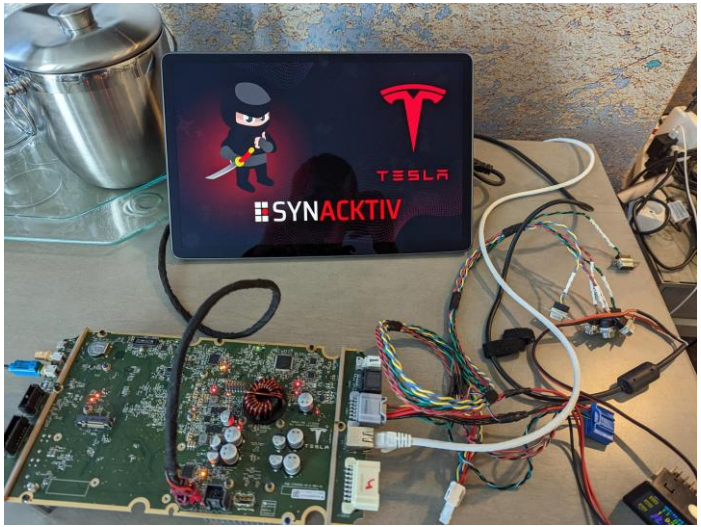
- later estimates of vulnerable vehicles to be somewhere between 292,000 and 471,000
- **lead to recall of 1.4 million cars by Chrysler**

Miller, Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. DEF CON 23 Hacking Conference. Las Vegas, NV: DEF CON. Aug. 2015
https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

Images: blackhat.com, wired.com

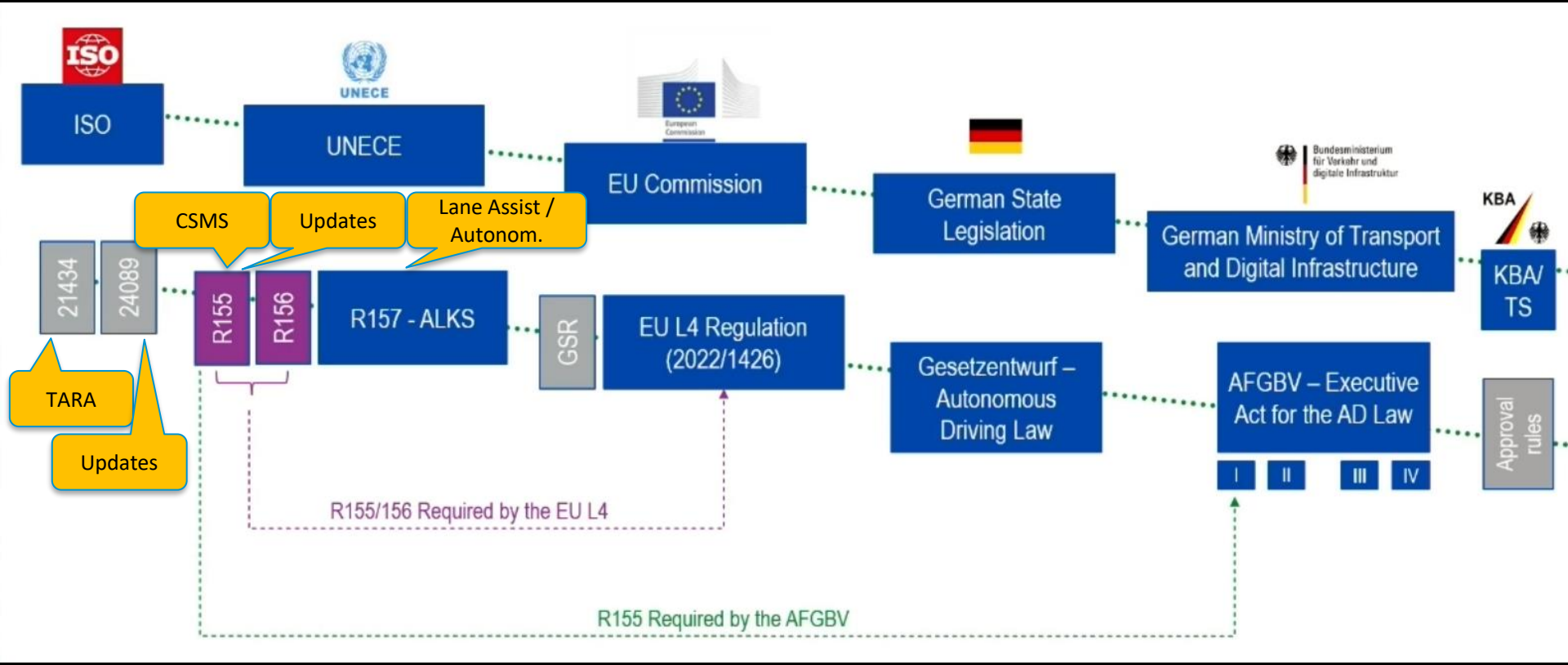
https://www.youtube.com/watch?v=3Wd4H91qfso

Tesla Infotainment at Pwn2Own (2023)



- Tesla Model 3 infotainment through bluetooth
- elevated privileges to root

https://twitter.com/Synacktiv/status/1638996681260781574/photo/1


ISO
ISO
UNECE
UNECE
EU Commission
German State Legislation
Bundesministerium für Verkehr und digitale Infrastruktur
German Ministry of Transport and Digital Infrastructure
KBA
KBA/ TS
CSMS
Updates
Lane Assist / Autonom.
21434
24089
R155
R156
R157 - ALKS
GSR
EU L4 Regulation (2022/1426)
Gesetzentwurf – Autonomous Driving Law
AFGBV – Executive Act for the AD Law
I
II
III
IV
Approval rules
TARA
Updates
R155/156 Required by the EU L4
R155 Required by the AFGBV

ICS › 43 › 43.040 › 43.040.15

ISO/SAE 21434:2021

Road vehicles — Cybersecurity engineering

ABSTRACT

PREVIEW

This document specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

This document is applicable to series production road vehicle E/E systems, including their components and interfaces, whose development or modification began after the publication of this document.

This document does not prescribe specific technology or solutions related to cybersecurity.

GENERAL INFORMATION

Status : Published

Publication date : 2021-08

Edition : 1

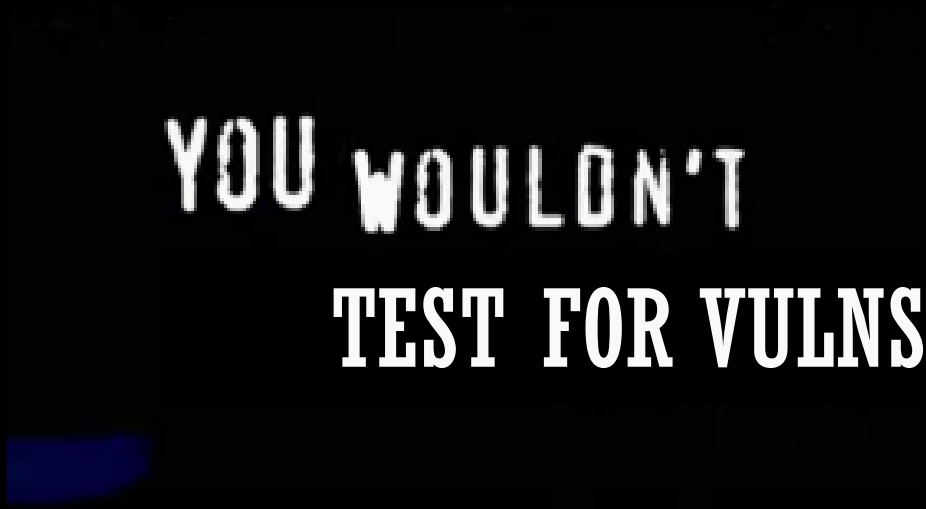
Number of pages : 81

Technical Committee : ISO/TC 22/SC 32 Electrical and electronic components and general system aspects

GENERAL INFORMATION

Status : Published

Publication date : 2021-08



https://torrentfreak.com/sorry-the-you-wouldnt-steal-a-car-anti-piracy-ad-wasnt-pirated-170625/

OWASP IOT Top 10 with automotive aspects

1. **Weak Guessable, or Hardcoded Passwords**
2. **Insecure Network Services**
3. **Insecure Ecosystem Interfaces**
4. **Lack of Secure Update Mechanism**
5. **Use of Insecure or Outdated Components**
5. **Insufficient Privacy Protection**
6. **Insecure Data Transfer and Storage**
7. **Lack of Device Management**
8. **Insecure Default Settings**
9. **Lack of Physical Hardening**

OWASP Internet of Things Project https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

Car Architecture

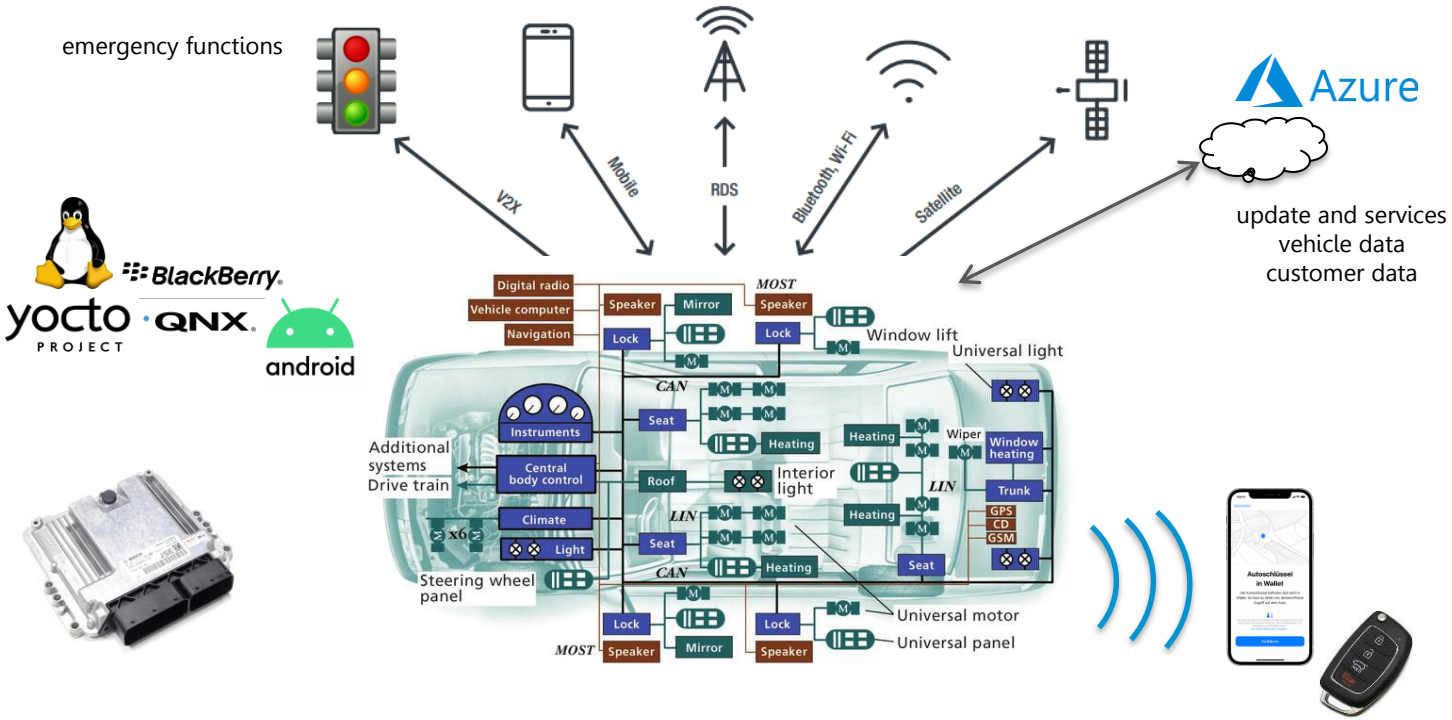


Image: https://www.researchgate.net/figure/One-subset-of-a-modern-vehicles-network-architecture-showing-the-trend-toward_fig1_2955571

Cloning of the Chip

NXP Original PCF7935 Philips Transponder Chip ID 44

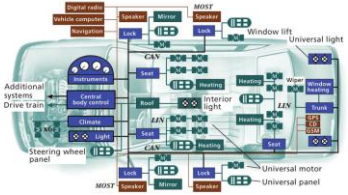
★★★★★ (9 Customer Reviews) Write Review

$5.00 (€4.60)

Qty 1 Add to cart ♥ Add to Wishlist

Product Code:	MK9202
Categories	Transponder Chips
Manufacturer	Genuine-OEM

https://www.youtube.com/watch?v=JmcxyVachho



Headlight (Left)

Body control

Aircon

Smart key

Headlight (Right)

shutterstock.com · 1175690107

Door control

Gateway

Parking brake

Telematics

Radar

Parking assist

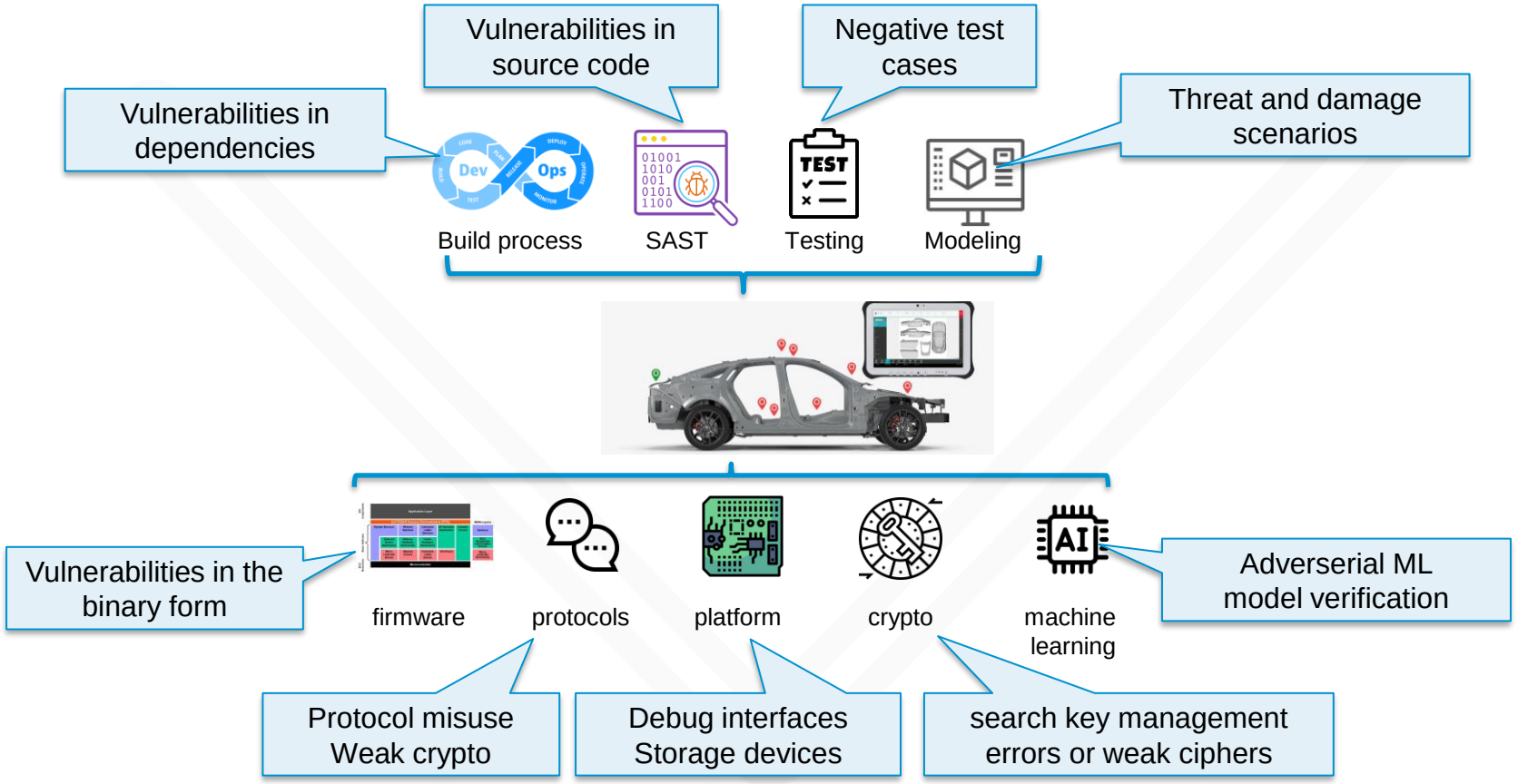
Forward camera

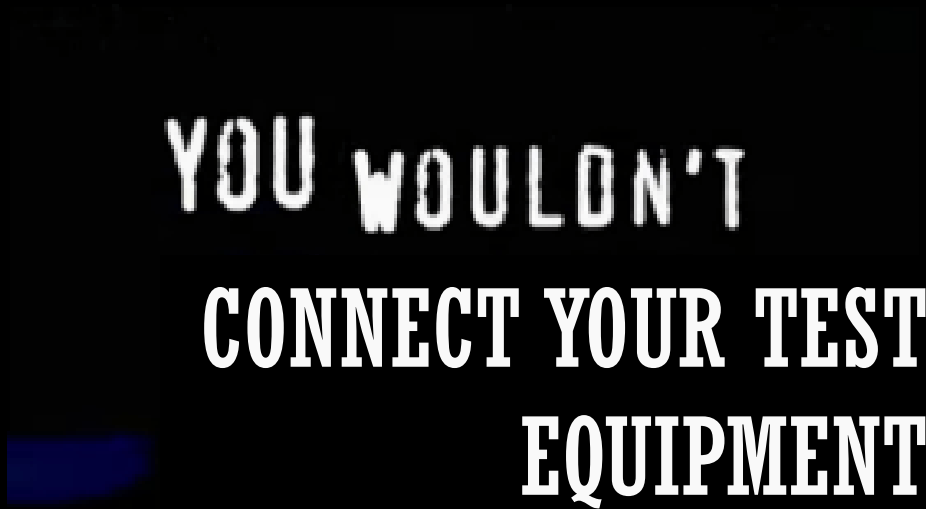
Hybrid

Battery

Motor inverter

Image: https://kentindell.github.io/2023/04/03/can-injection/

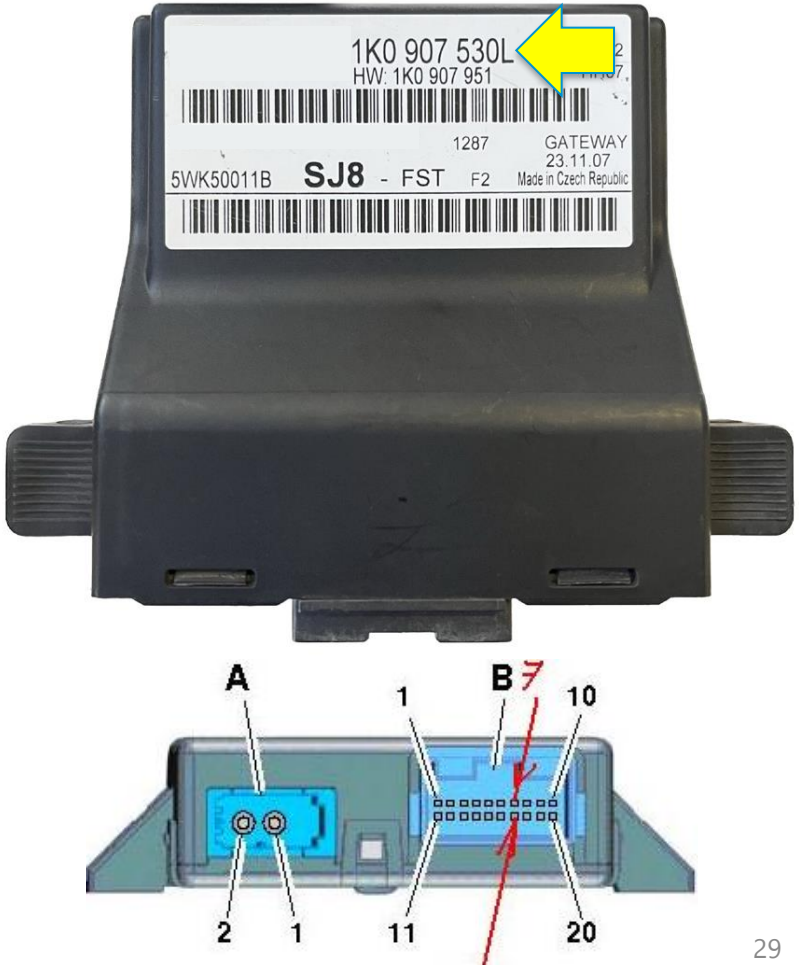

Vulnerabilities in source code
Negative test cases
Vulnerabilities in dependencies
Threat and damage scenarios
Dev
Ops
Build process
SAST
Testing
Modeling
firmware
protocols
platform
crypto
machine learning
Vulnerabilities in the binary form
Adverserial ML model verification
Protocol misuse
Weak crypto
Debug interfaces
Storage devices
search key management
errors or weak ciphers

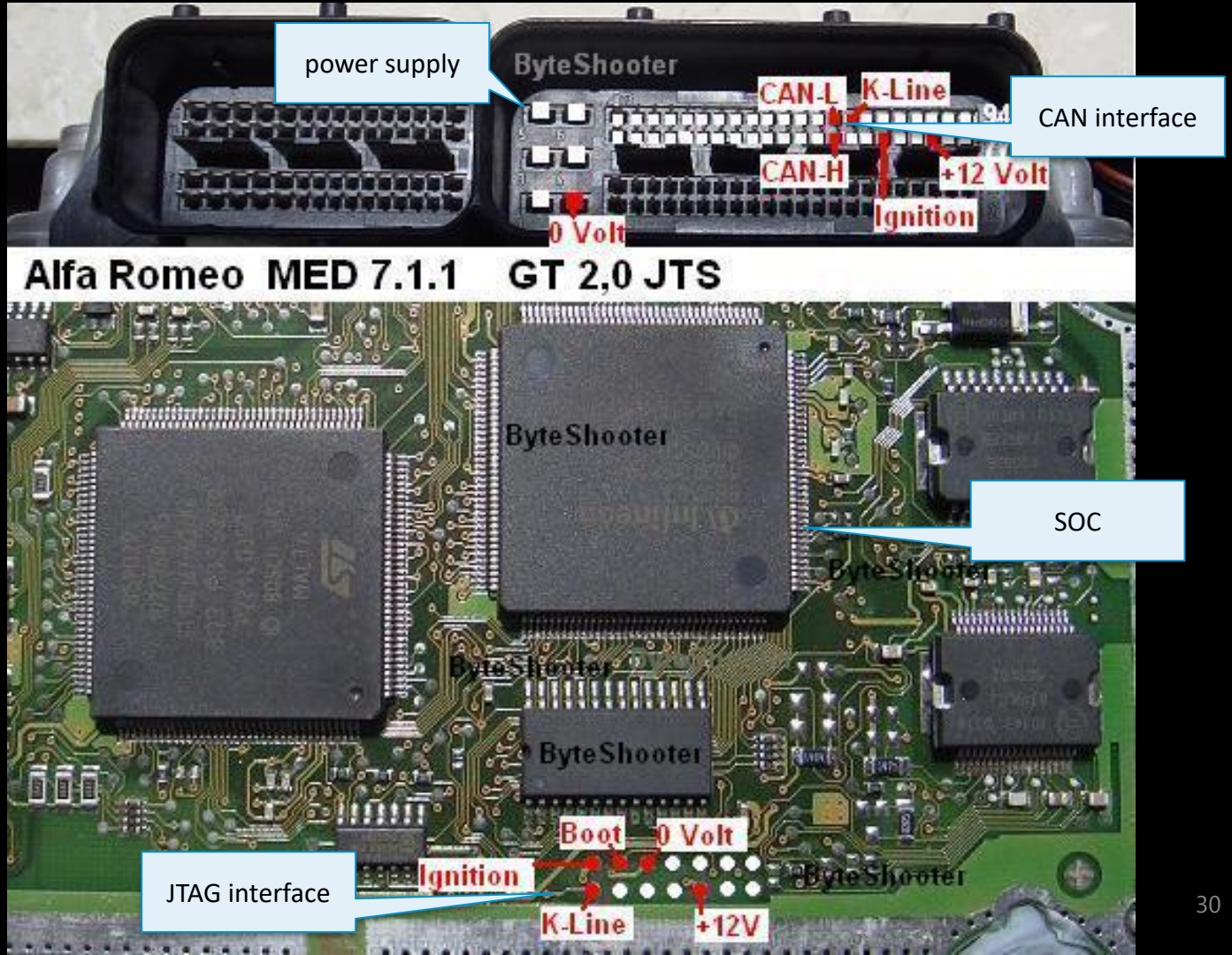


https://torrentfreak.com/sorry-the-you-wouldnt-steal-a-car-anti-piracy-ad-wasnt-pirated-170625/

Device Gateway

- search for part numbers
- search for pinouts
- look for cars using this device
- tuning-forums are a nice source




power supply
ByteShooter
CAN-L
K-Line
CAN interface
CAN-H
+12 Volt
Ignition
0 Volt
Alfa Romeo MED 7.1.1 GT 2,0 JTS
ByteShooter
SOC
ByteShooter
ByteShooter
ByteShooter
Boot
0 Volt
Ignition
JTAG interface
ByteShooter
K-Line
+12V

CAN Interfaces

Professional use:

- Intrepid ValueCAN
- Vector Can Case

Budget lab:

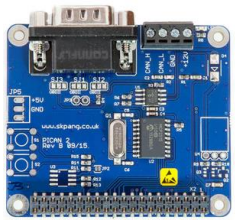
- USBTin
- Raspberry PiCAN

Intrepid ValueCAN

Vector Can Case

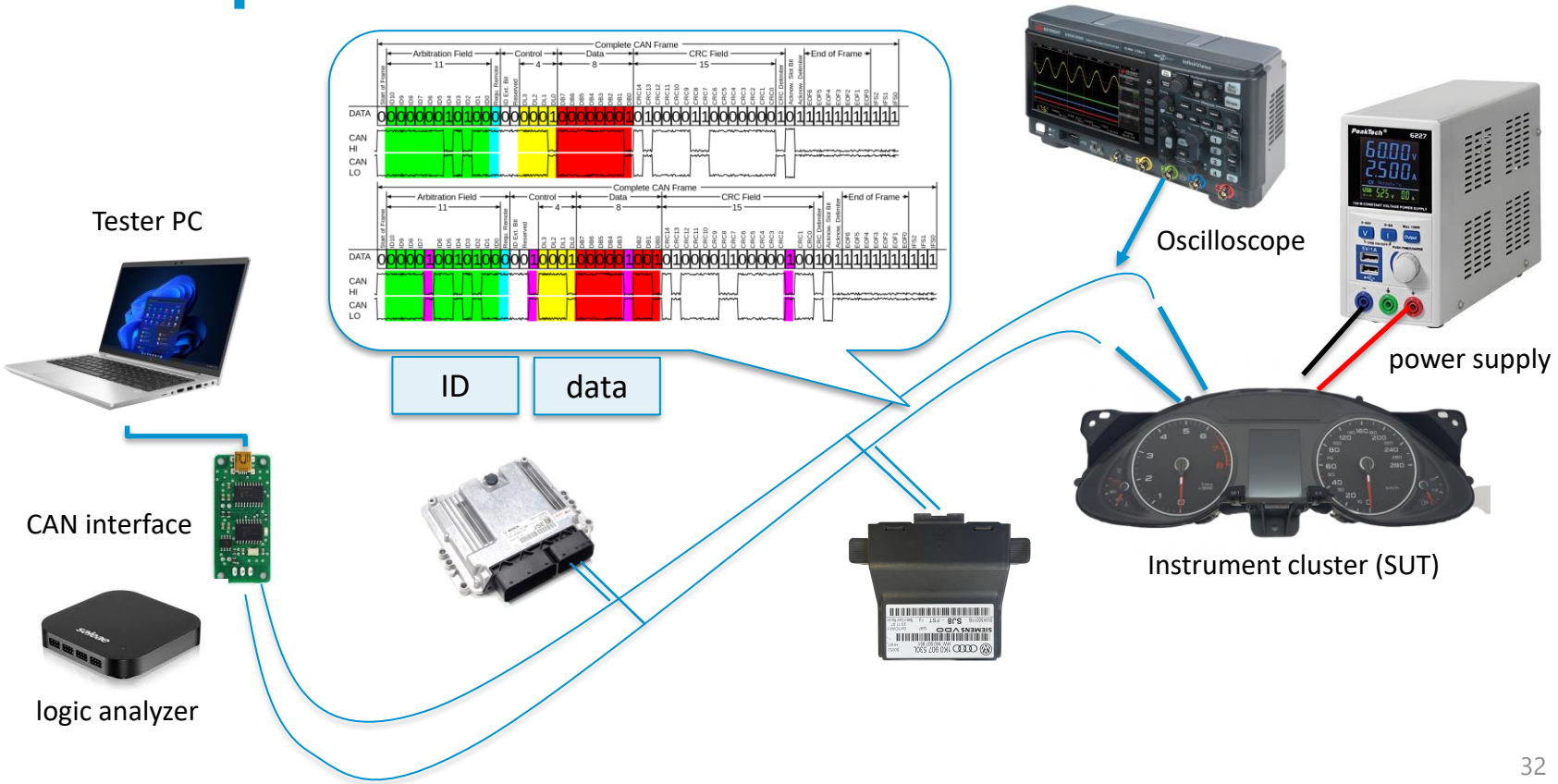
Peak PCAN-USB

USBTin



PiCAN

Setup for Research



The CAN frame

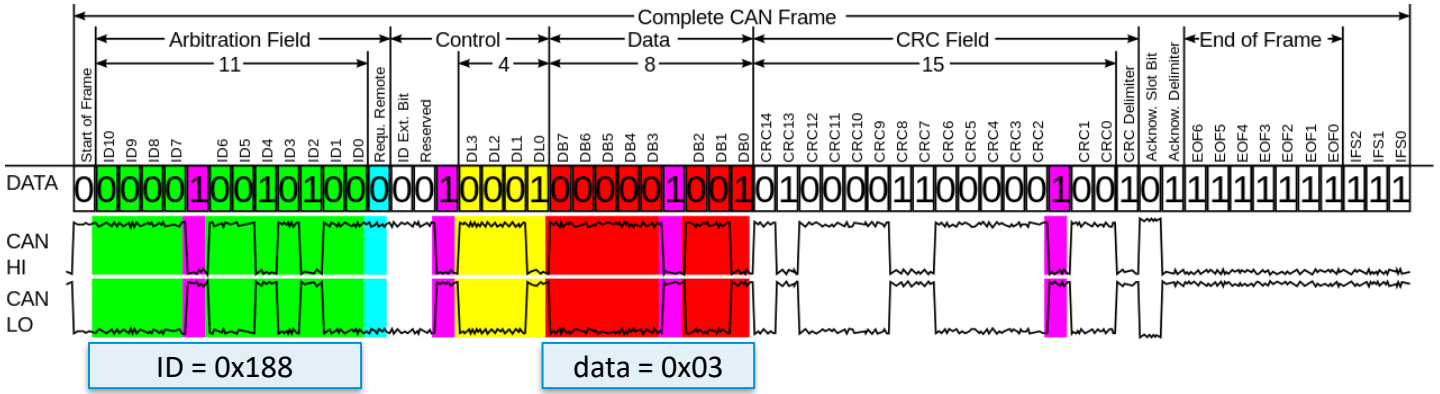
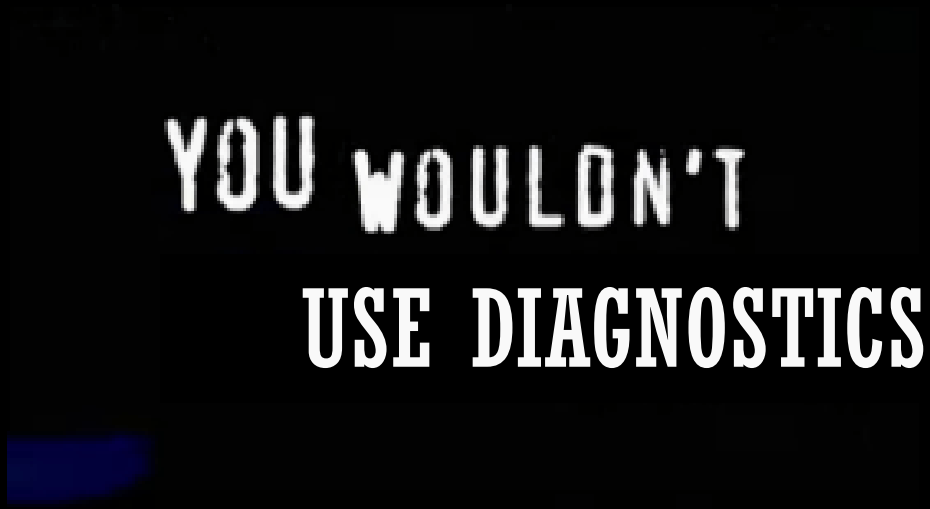


Image: https://en.wikipedia.org/wiki/CAN_bus

WARNING:
- do testing of hardware with a trained electrical engineer
- don‘t do this on your car [on the street]
- it could harm your car, your devices or your health



https://torrentfreak.com/sorry-the-you-wouldnt-steal-a-car-anti-piracy-ad-wasnt-pirated-170625/

7 layer OSI model | **Unified Diagnostic Services (UDS)**

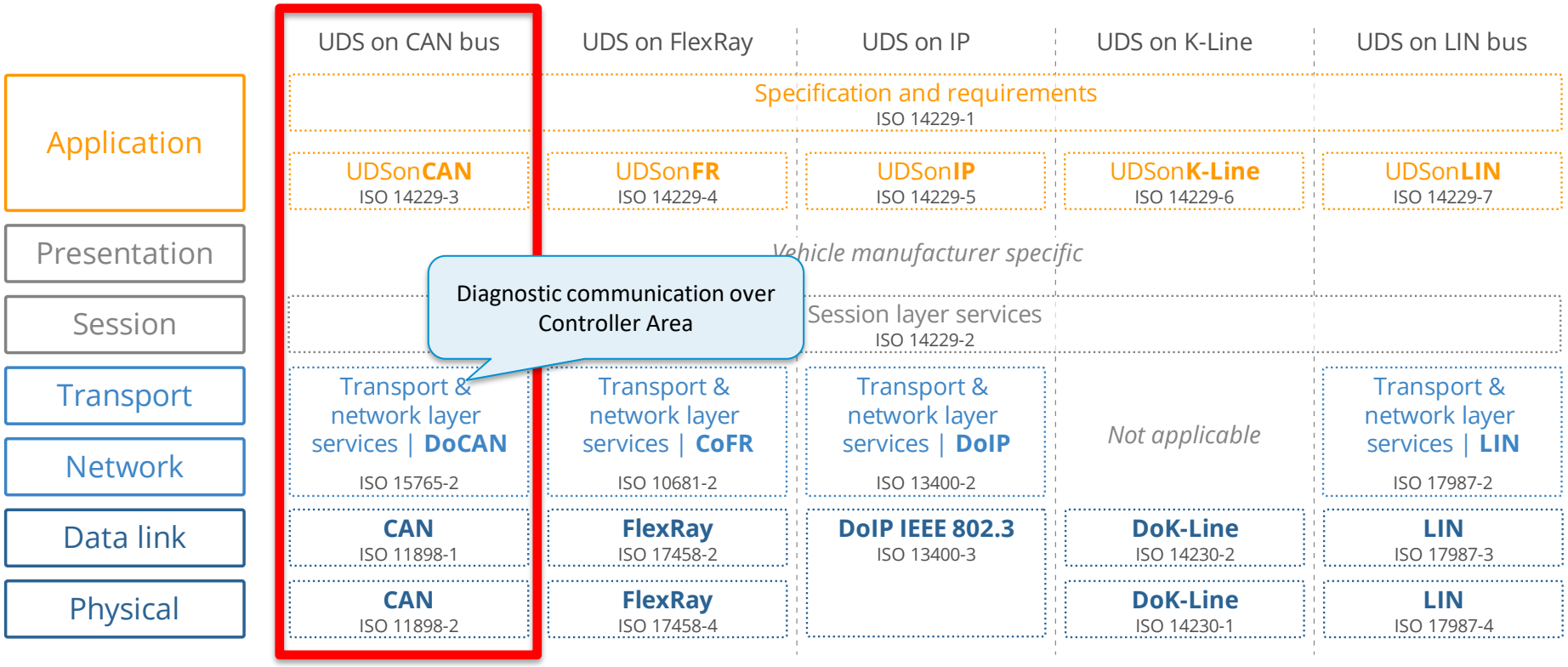
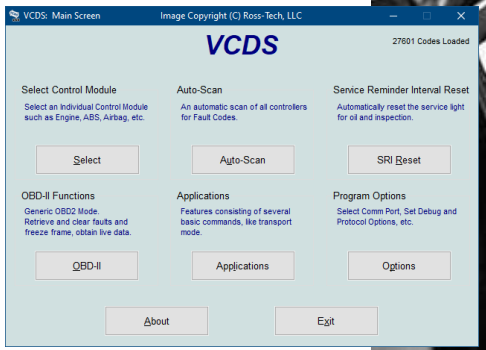


Image: https://www.csselectronics.com/pages/uds-protocol-tutorial-unified-diagnostic-services

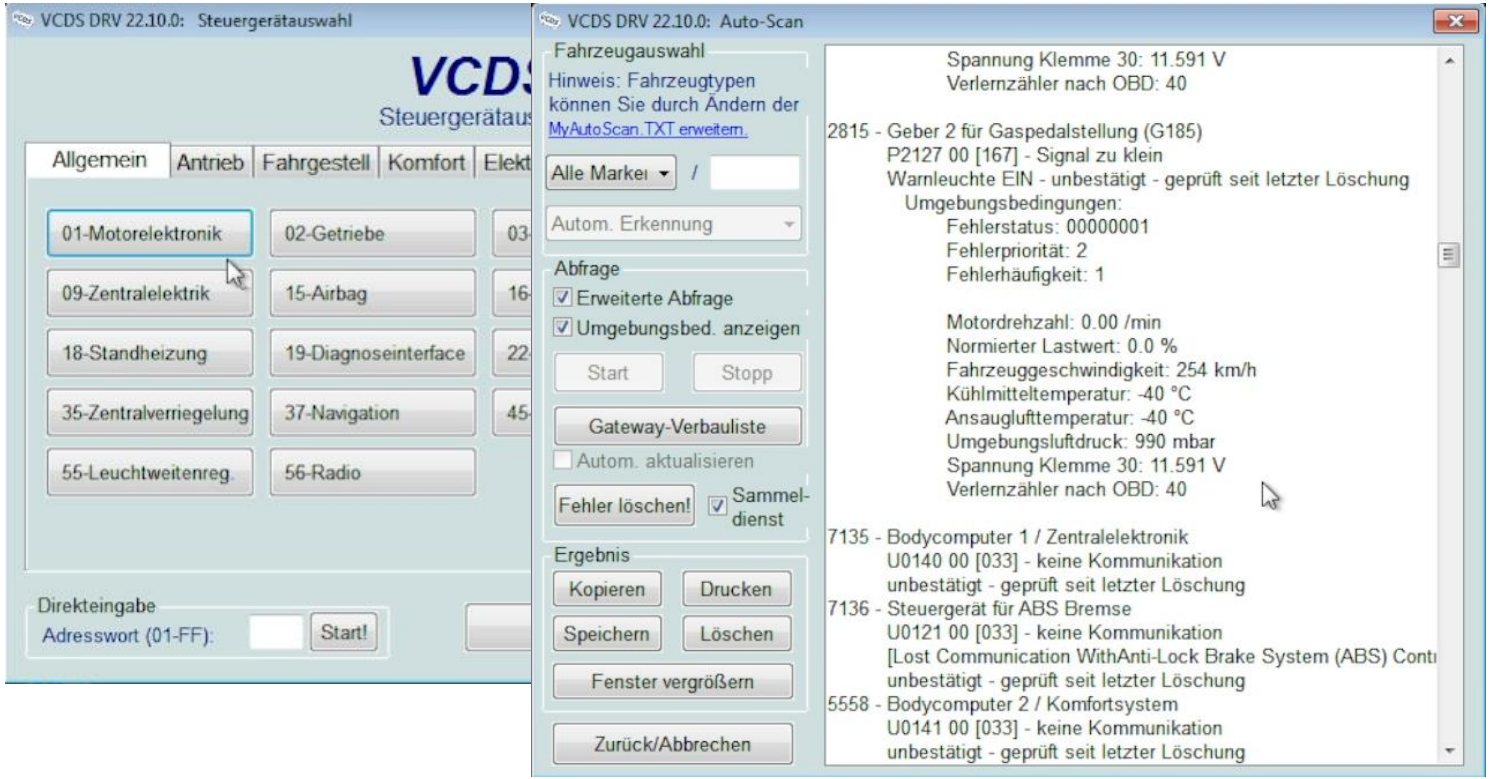
Diagnostics (UDS over CAN ISO 14229-3)



VCDS Ross Tech https://www.ross-tech.com/vag-com/

Image: https://www.influxbigdata.in/post/uds-unified-diagnostic-services-protocol-iso-14229-pdf

Demo: Diagnostics with VCDS

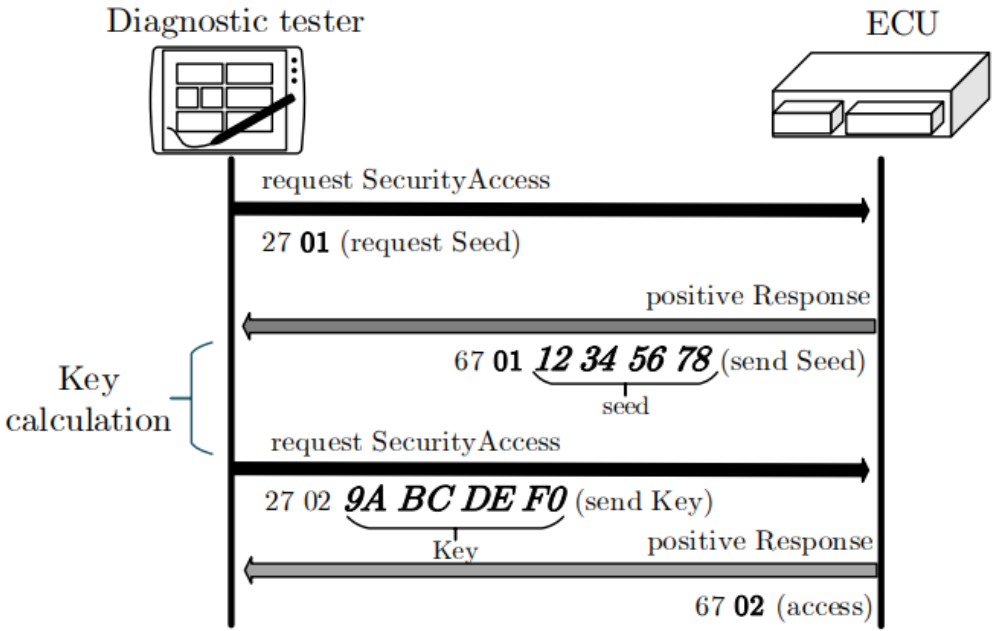


Diagnostic and Communications Management	0x10	0x50	Diagnostic Session Control	Control which UDS services are available
	0x11	0x51	ECU Reset	Reset the ECU ("hard reset", "key off", "soft reset")
	0x27	0x67	Security Access	Enable use of security-critical services via authentication
	0x28	0x68	Communication Control	Turn sending/receiving of messages on/off in the ECU
	0x29	0x69	Authentication	Enable more advanced authentication vs. 0x27 (PKI based exchange)
	0x3E	0x7E	Tester Present	Send a "heartbeat" periodically to remain in the current session
	0x83	0xC3	Access Timing Parameters	View/modify timing parameters used in client/server communication
	0x84	0xC4	Secured Data Transmission	Send encrypted data via ISO 15764 (Extended Data Link Security)
	0x85	0xC5	Control DTC Settings	Enable/disable detection of errors (e.g. used during diagnostics)
	0x86	0xC6	Response On Event	Request that an ECU processes a service request if an event happens
	0x87	0xC7	Link Control	Set the baud rate for diagnostic access
Data Transmission	0x22	0x62	Read Data By Identifier	Read data from targeted ECU - e.g. VIN, sensor data values etc.
	0x23	0x63	Read Memory By Address	Read data from physical memory (e.g. to understand software behavior)
	0x24	0x64	Read Scaling Data By Identifier	Read information about how to scale data identifiers
	0x2A	0x6A	Read Data By Identifier Periodic	Request ECU to broadcast sensor data at slow/medium/fast/stop rate
	0x2C	0x6C	Dynamically Define Data Identifier	Define data parameter for use in 0x22 or 0x2A dynamically
	0x2E	0x6E	Write Data By Identifier	Program specific variables determined by data parameters
	0x3D	0x7D	Write Memory By Address	Write information to the ECU's memory
DTCs	0x14	0x54	Clear Diagnostic Information	Delete stored DTCs
	0x19	0x59	Read DTC Information	Read stored DTCs, as well as related information
	0x2F	0x6F	Input Output Control By Identifier	Gain control over ECU analog/digital inputs/outputs
	0x31	0x71	Routine Control	Initiate/stop routines (e.g. self-testing, erasing of flash memory)
Upload/ Download	0x34	0x74	Request Download	Start request to add software/data to ECU (incl. location/size)
	0x35	0x75	Request Upload	Start request to read software/data from ECU (incl. location/size)
	0x36	0x76	Transfer Data	Perform actual transfer of data following use of 0x74/0x75
	0x37	0x77	Request Transfer Exit	Stop the transfer of data
	0x38	0x78	Request File Transfer	Perform a file download/upload to/from the ECU

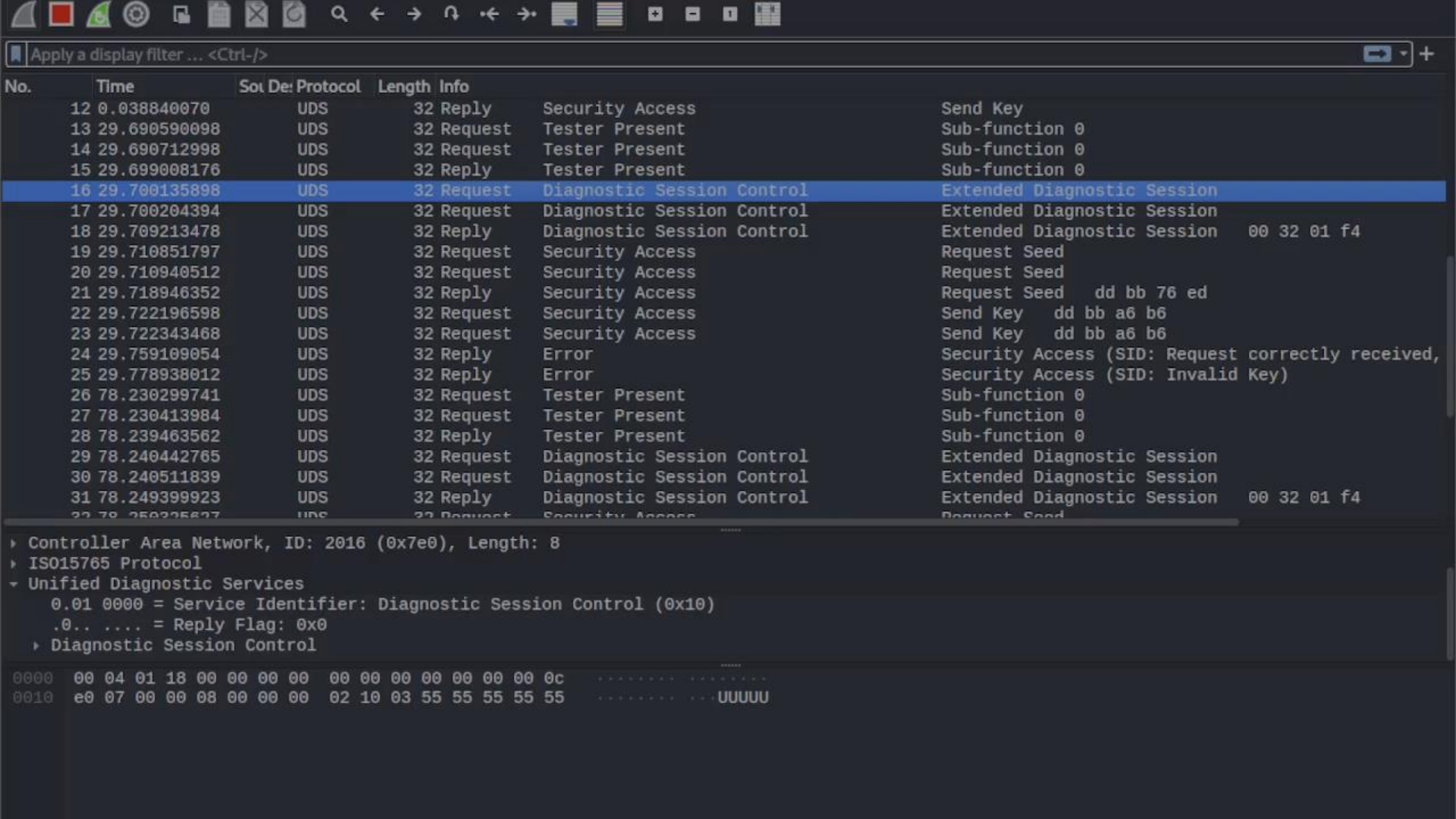
SBA Re

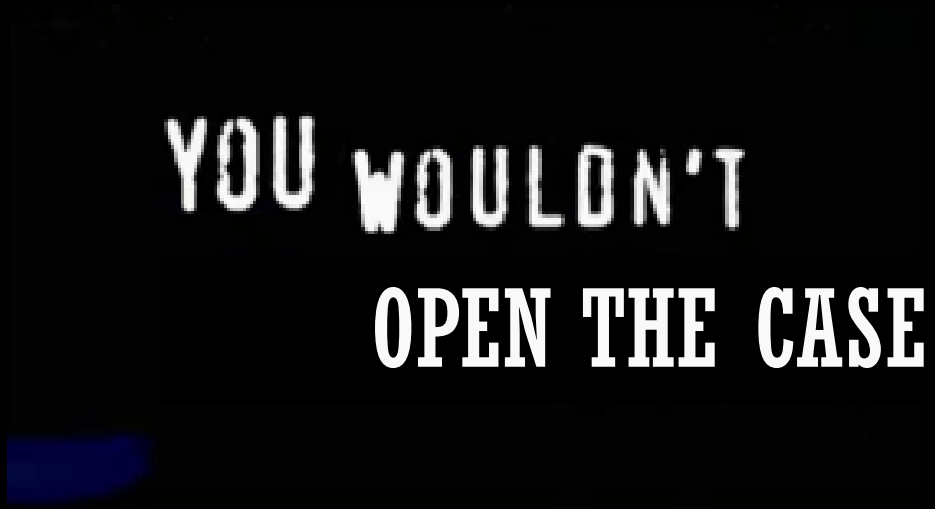
https://www.csselectronics.com/pages/uds-protocol-tutorial-unified-diagnostic-services

UDS Security Access Challenge Response

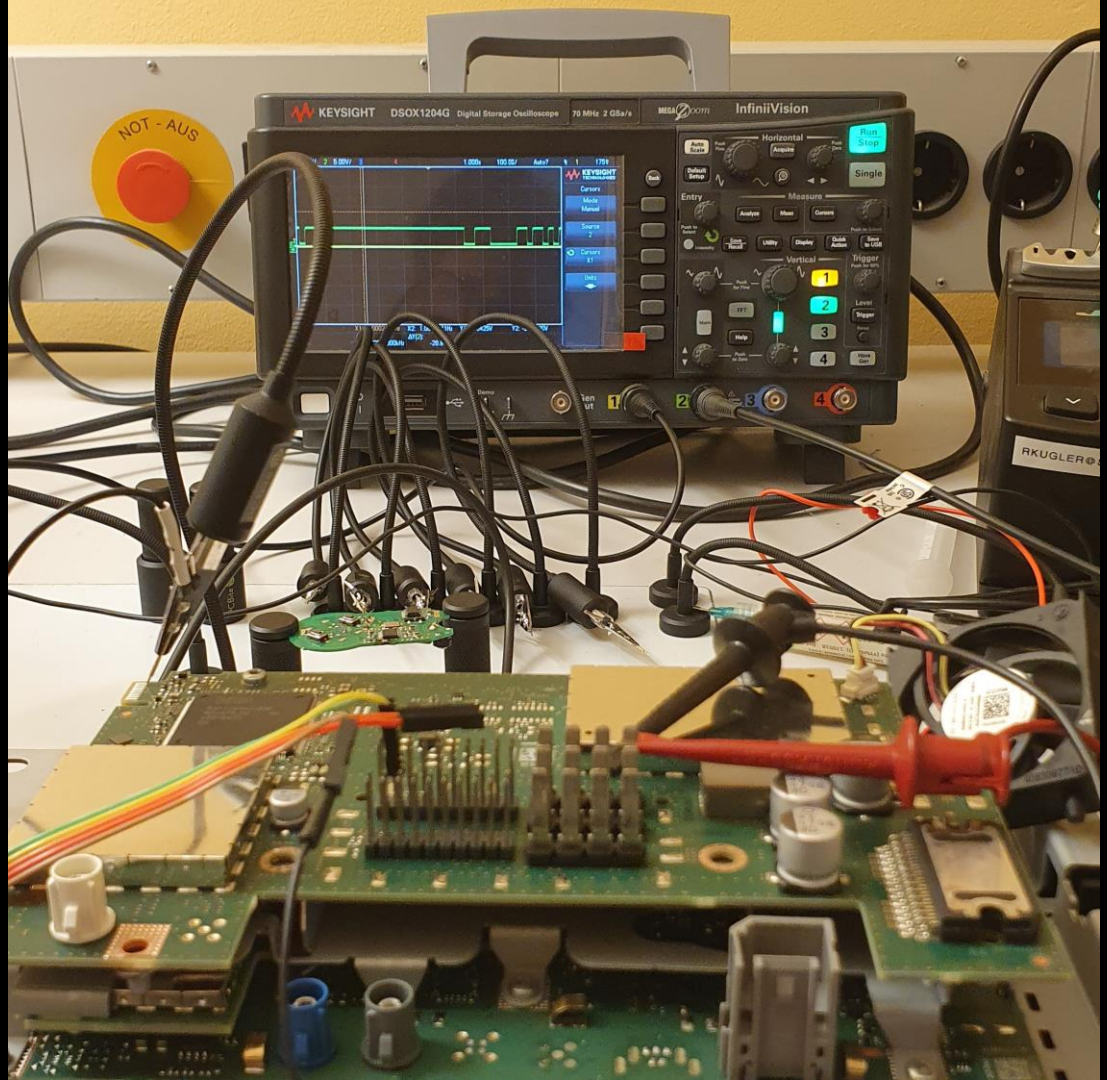


Evaluation of Vehicle Diagnostics Security – Implementation of a Reproducible Security Access, Martin Ring, Tobias Rensen and Reiner Kriesten (2014), p.204

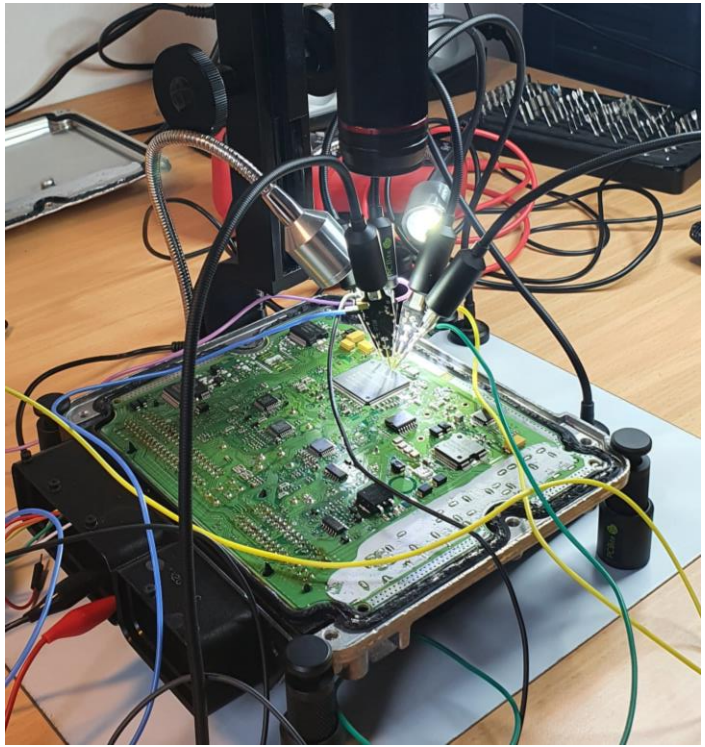

Apply a display filter ... <Ctrl-/>
No. Time Sou De: Protocol Length Info
12 0.038840070 UDS 32 Reply Security Access Send Key
13 29.690590098 UDS 32 Request Tester Present Sub-function 0
14 29.690712998 UDS 32 Request Tester Present Sub-function 0
15 29.699008176 UDS 32 Reply Tester Present Sub-function 0
16 29.700135898 UDS 32 Request Diagnostic Session Control Extended Diagnostic Session
17 29.700204394 UDS 32 Request Diagnostic Session Control Extended Diagnostic Session
18 29.709213478 UDS 32 Reply Diagnostic Session Control Extended Diagnostic Session 00 32 01 f4
19 29.710851797 UDS 32 Request Security Access Request Seed
20 29.710940512 UDS 32 Request Security Access Request Seed
21 29.718946352 UDS 32 Reply Security Access Request Seed dd bb 76 ed
22 29.722196598 UDS 32 Request Security Access Send Key dd bb a6 b6
23 29.722343468 UDS 32 Request Security Access Send Key dd bb a6 b6
24 29.759109054 UDS 32 Reply Error Security Access (SID: Request correctly received,
25 29.778938012 UDS 32 Reply Error Security Access (SID: Invalid Key)
26 78.230299741 UDS 32 Request Tester Present Sub-function 0
27 78.230413984 UDS 32 Request Tester Present Sub-function 0
28 78.239463562 UDS 32 Reply Tester Present Sub-function 0
29 78.240442765 UDS 32 Request Diagnostic Session Control Extended Diagnostic Session
30 78.240511839 UDS 32 Request Diagnostic Session Control Extended Diagnostic Session
31 78.249399923 UDS 32 Reply Diagnostic Session Control Extended Diagnostic Session 00 32 01 f4
Controller Area Network, ID: 2016 (0x7e0), Length: 8
ISO15765 Protocol
Unified Diagnostic Services
0.01 0000 = Service Identifier: Diagnostic Session Control (0x10)
.0.. .... = Reply Flag: 0x0
Diagnostic Session Control
0000 00 04 01 18 00 00 00 00 00 00 00 00 00 00 00 0c
0010 e0 07 00 00 08 00 00 00 02 10 03 55 55 55 55 55
UUUUU



https://torrentfreak.com/sorry-the-you-wouldnt-steal-a-car-anti-piracy-ad-wasnt-pirated-170625/


NOT - AUS
KEYSIGHT
DSOX1204G
Digital Storage Oscilloscope
70 MHz 2 GSa/s
InfiniiVision
Horizontal
Run Stop
Single
Measure
Vertical
RKUGLER

Side Channel Attacks and Debug Interfaces



- JTAG access
- SPI bus access
- Change boot modes via exposed pins/pads
- Desolder Flash and use a socket
- Dump Flash and load it in Ghidra

JTAG access on the PCB

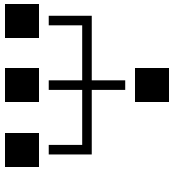
https://www.youtube.com/watch?v=kynXjan7O0Q&t=1s

"We will produce tablets on wheels“

Christian Senger (VW, 2017)

OWASP IOT Top 10 (Automotive Aspects)

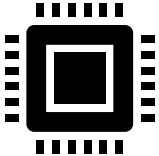
Weak passwords



Insecure network unprotected data transfer

Ecosystem and Cloud

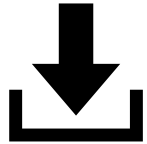
Hardening



Debug ports

Update

Secure Defaults

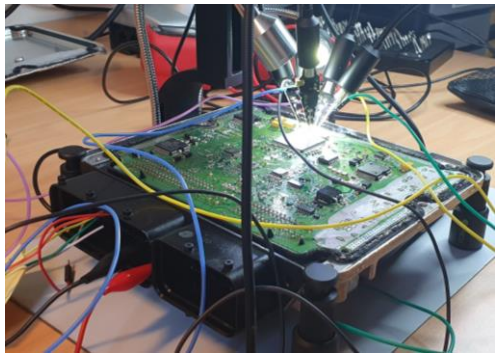


Secure Storage

The Software Defined Vehicle

- **High Performance Computer** (HPC) to centralize software on one platform
- **Software defined networks:** less cables, less ECUs, less weight -> software defined
- **Cloud services and Updates** Over-the-Air Updates incl. firmware updates (FOTA)

SBA Meetup // ASRG Vienna // eBPF Vienna



MATRIS
Research Group

SBA Research

Applied Research Consulting in Customer Projects

ASSESS

Threats and Security Architecture

- Security Requirements
- Crypto Designs
- Threat Modelling

EVALUATE

Identify Attacks and Defenses

- Static Code Analysis
- Security Test Case Generation
- Defense in Depth (DiD)

VALIDATE

Software and System Testing

- Fuzz Testing
- Black- and Grey-box Testing
- Proof of Concept Validation

Tailored Security Trainings

Threat Analysis	Coding and Exploitation	Container Security
Crypto Engineering	IoT Hacking	Combinatorial Security Testing

Embedded Systems

Containers

Servers and Data Centers

Industrial IoT

MATRIS Research Group

SBA Research

Reinhard Kugler

MATRIS Research Lab

SBA Research

Floragasse 7, 1040 Vienna

rkugler@sba-research.org

https://matris.sba-research.org/marc/

MATRIS Research Group

SBA Research