SBA Research

You wouldn't STEAL a CAR?

security in automotive control units

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

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

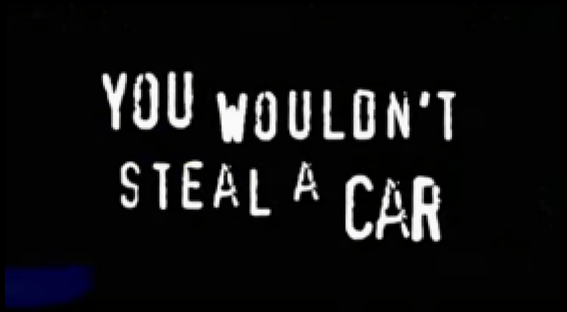
FFG
Forschung wirkt.

wirtschafts
agentur
wien
Ein Fonds der
Stadt Wien

European
Commission

FWF
Der Wissenschaftsfonds.

netidee
OPEN INNOVATIONS



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

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

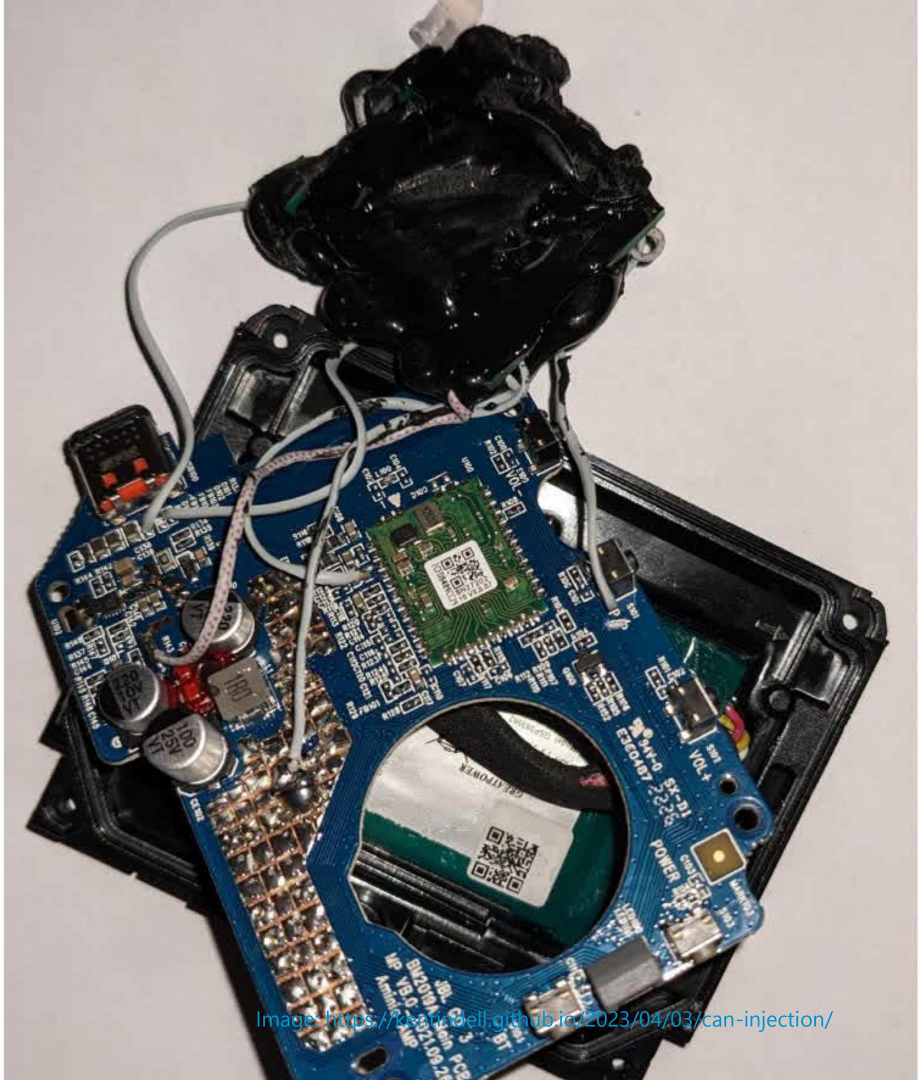
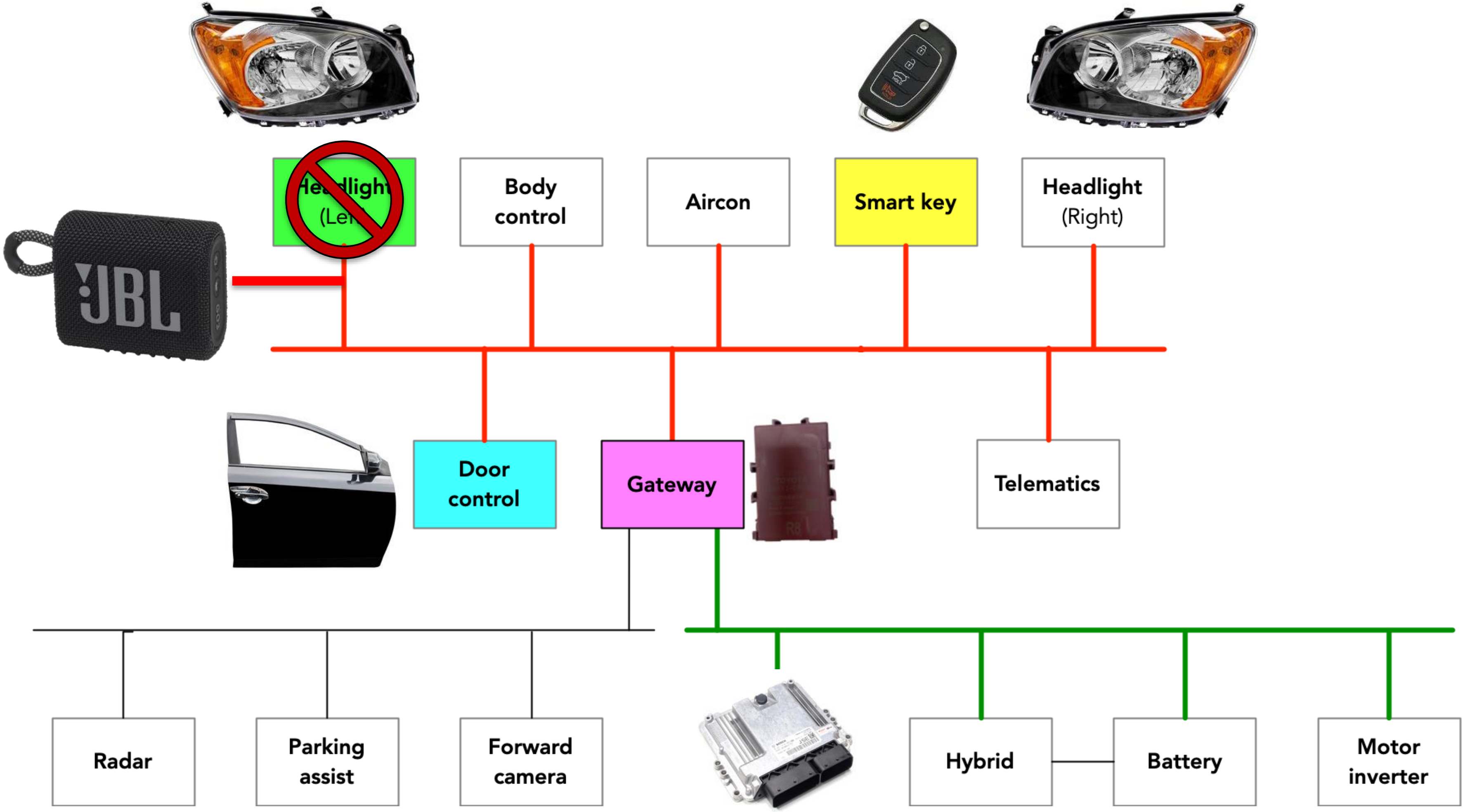
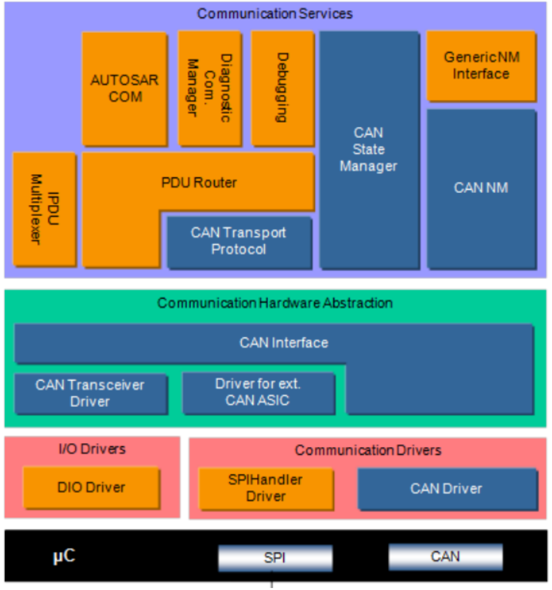


Image: https://kentindell.github.io/2023/04/03/can-injection/



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

Example: AutoSAR, Platform, Chip, Software



Communication Services

AUTOSAR COM

Diagnostic Com. Manager

Debugging

CAN State Manager

GenericNM Interface

IPDU Multiplexer

PDU Router

CAN Transport Protocol

CAN NM

Communication Hardware Abstraction

CAN Interface

CAN Transceiver Driver

Driver for ext. CAN ASIC

I/O Drivers

DIO Driver

Communication Drivers

SPIHandler Driver

CAN Driver

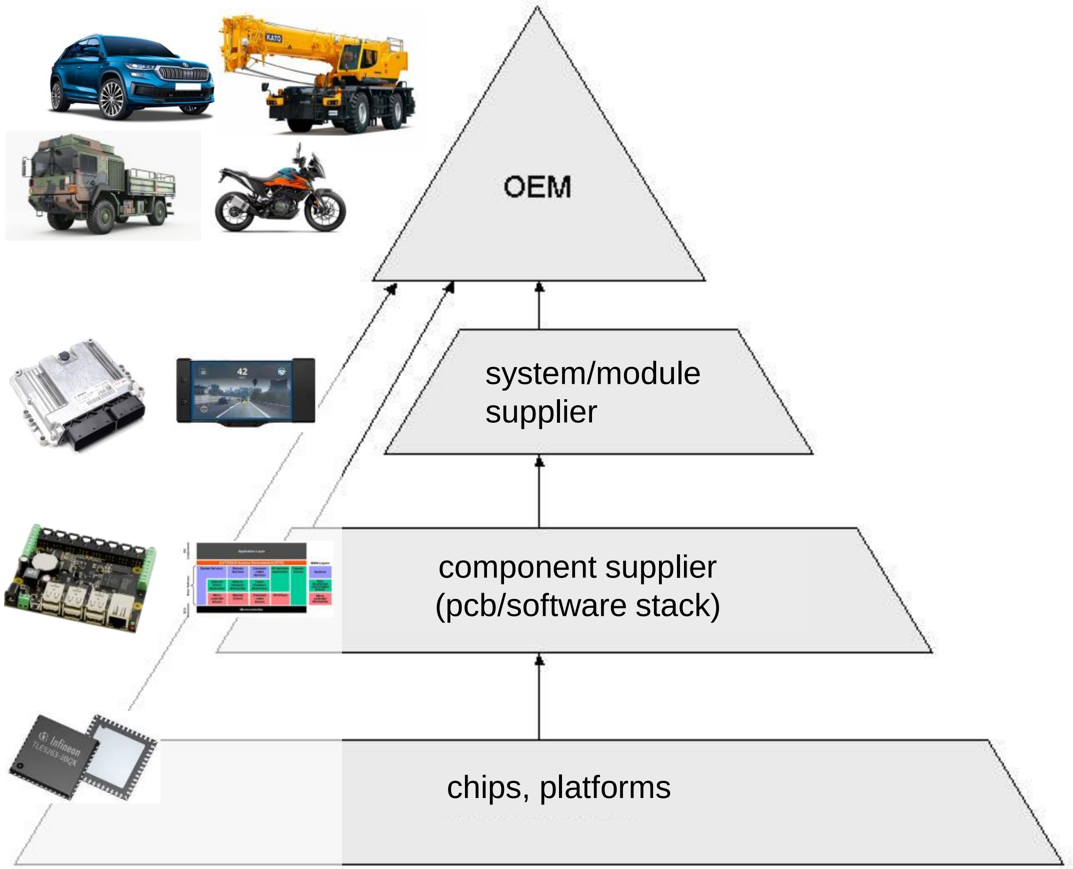
µC

SPI

CAN

between 70 and 100 ECUs being installed in every modern vehicle

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

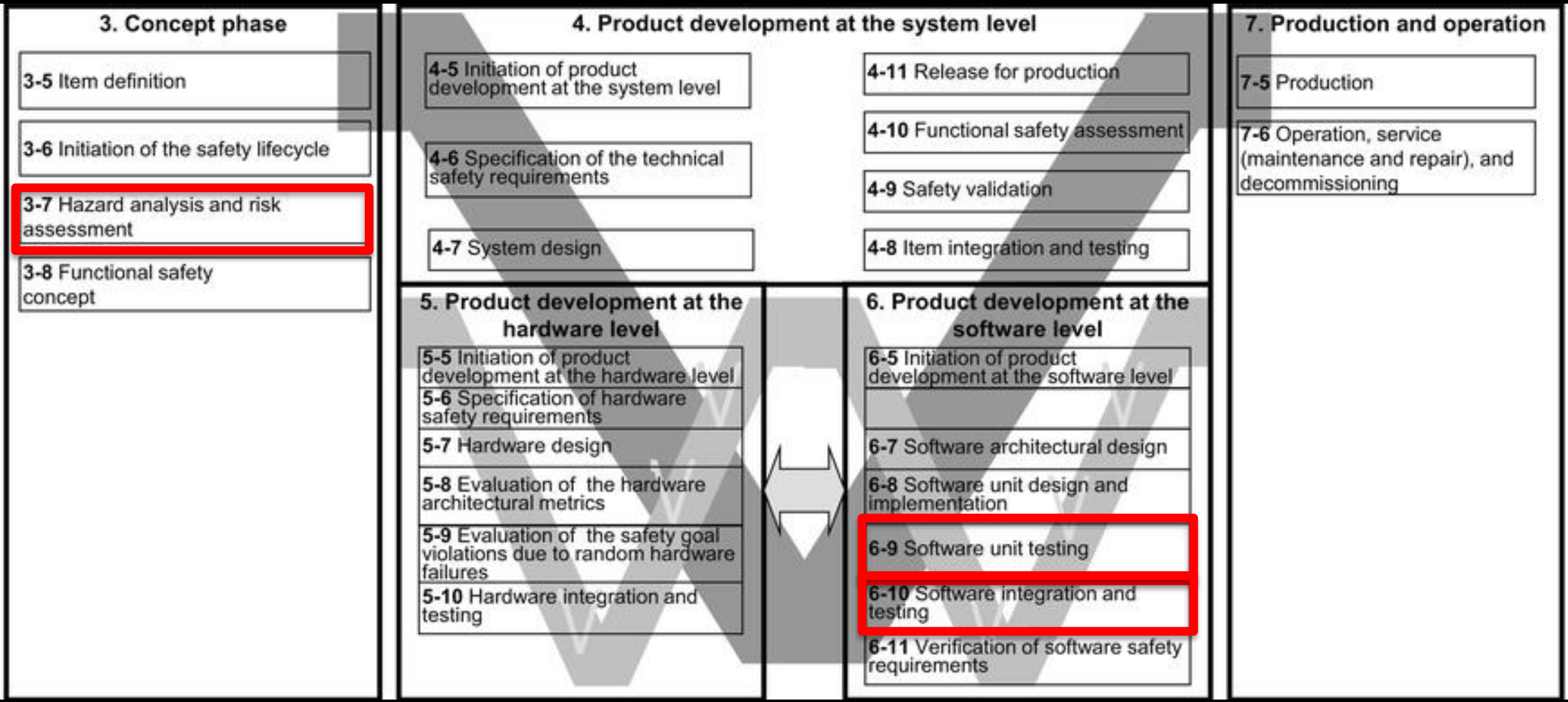


OEM

system/module supplier

component supplier (pcb/software stack)

chips, platforms



3. Concept phase

3-5 Item definition

3-6 Initiation of the safety lifecycle

3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4. Product development at the system level

4-5 Initiation of product development at the system level

4-6 Specification of the technical safety requirements

4-7 System design

4-11 Release for production

4-10 Functional safety assessment

4-9 Safety validation

4-8 Item integration and testing

5. Product development at the hardware level

5-5 Initiation of product development at the hardware level

5-6 Specification of hardware safety requirements

5-7 Hardware design

5-8 Evaluation of the hardware architectural metrics

5-9 Evaluation of the safety goal violations due to random hardware failures

5-10 Hardware integration and testing

6. Product development at the software level

6-5 Initiation of product development at the software level

6-7 Software architectural design

6-8 Software unit design and implementation

6-9 Software unit testing

6-10 Software integration and testing

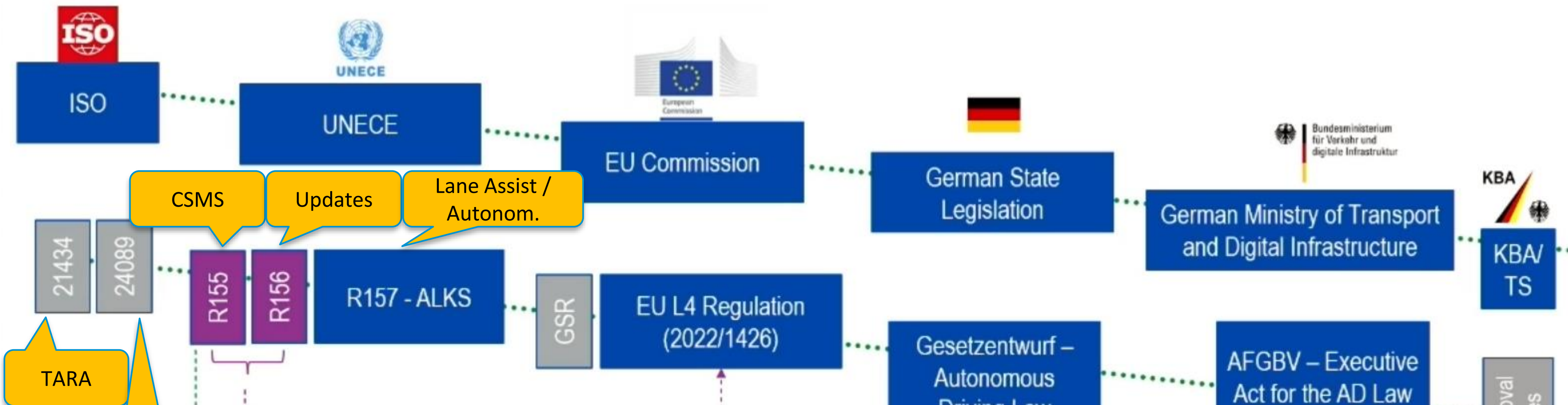
6-11 Verification of software safety requirements

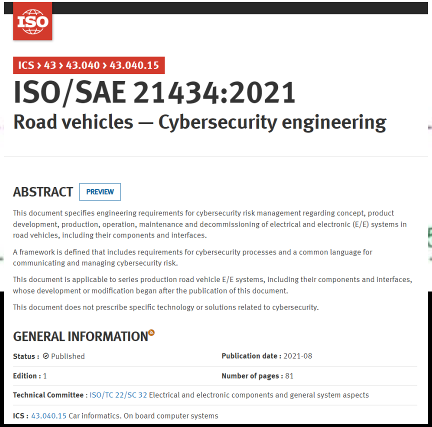
7. Production and operation

7-5 Production

7-6 Operation, service (maintenance and repair), and decommissioning

ISO 26262, https://www.iso.org/obp/ui/#iso:std:iso:26262:-9:ed-1:v1:en


ISO
ISO
UNECE
UNECE
European Commission
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
55 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.

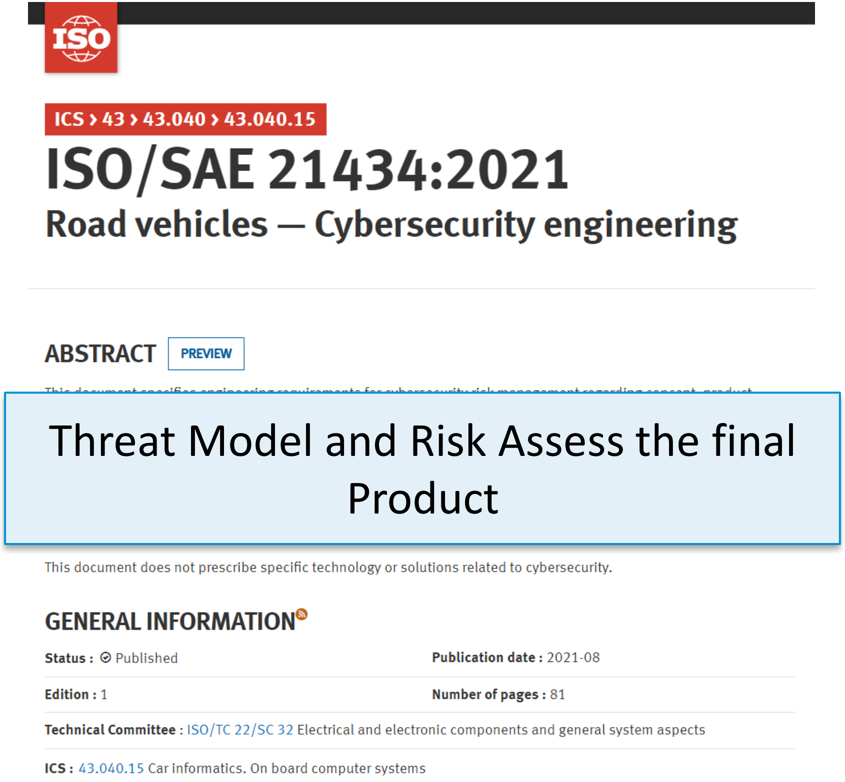
GENERAL INFORMATION

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

ICS : 43.040.15 Car informatics. On board computer systems

ISO/SAE 21434:2021



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

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

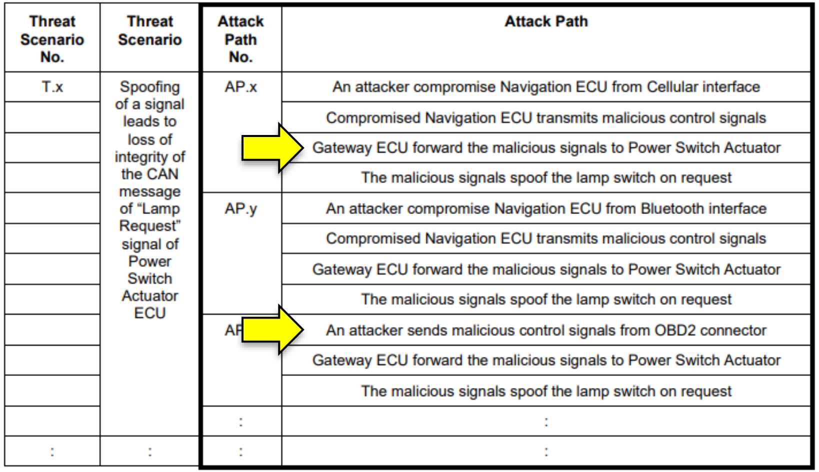
Technical Committee : ISO/TC 22/SC 32 Electrical and electronic components and general system aspects

ICS : 43.040.15 Car informatics. On board computer systems

Threat Model and Risk Assess the final Product

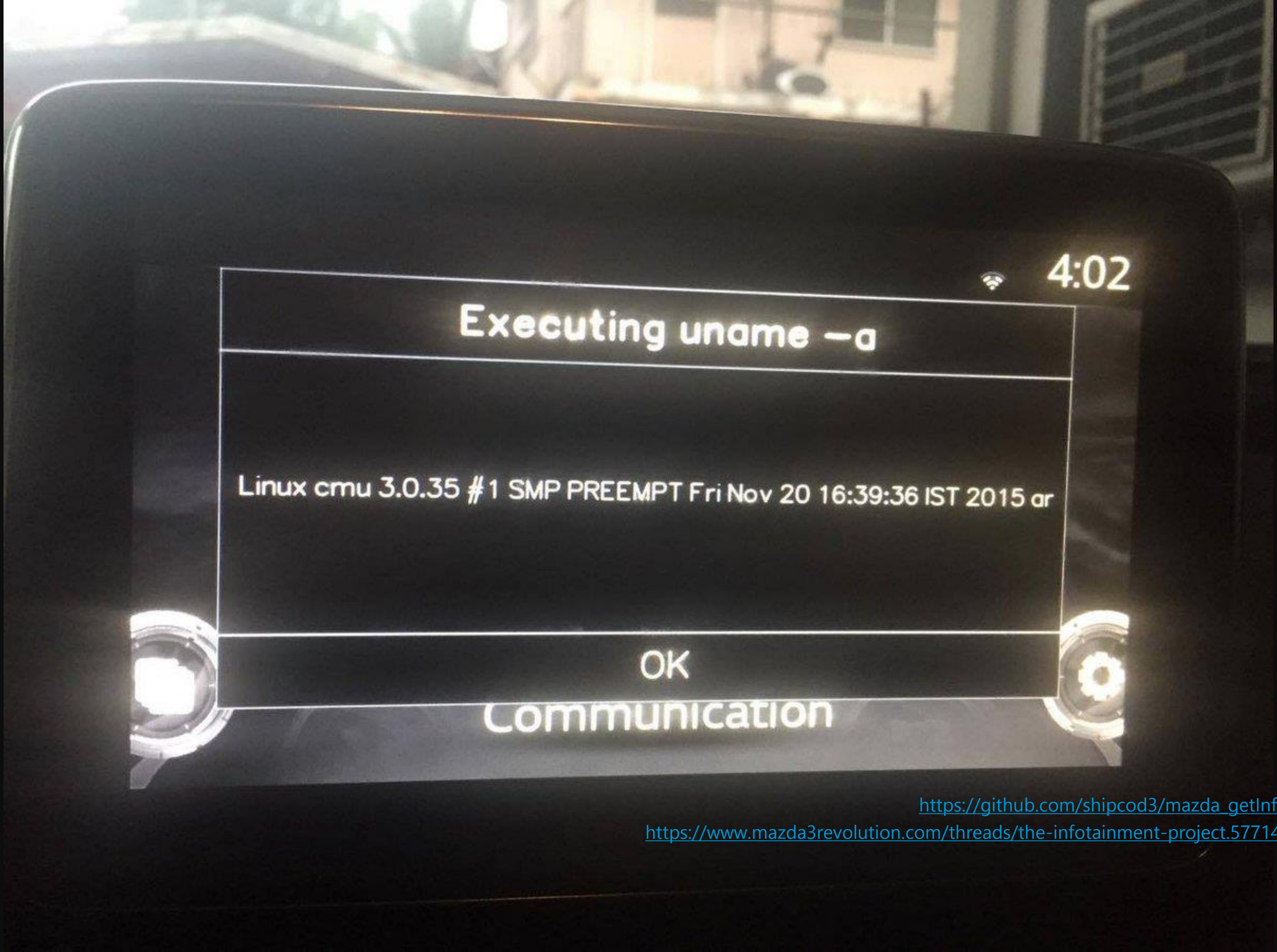
ANNEX G: EXAMPLE USE CASE AND WORK PRODUCTS: HEADLAMP SYSTEM

Table G.8 - Example of a list of attack paths for each threat scenario created by Company A



Threat Scenario No.	Threat Scenario	Attack Path No.	Attack Path
T.x	Spoofing of a signal leads to loss of integrity of the CAN message of "Lamp Request" signal of Power Switch Actuator ECU	AP.x	An attacker compromise Navigation ECU from Cellular interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AP.y	An attacker compromise Navigation ECU from Bluetooth interface
			Compromised Navigation ECU transmits malicious control signals
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		AF	An attacker sends malicious control signals from OBD2 connector
			Gateway ECU forward the malicious signals to Power Switch Actuator
			The malicious signals spoof the lamp switch on request
		:	:
:	:	:	:

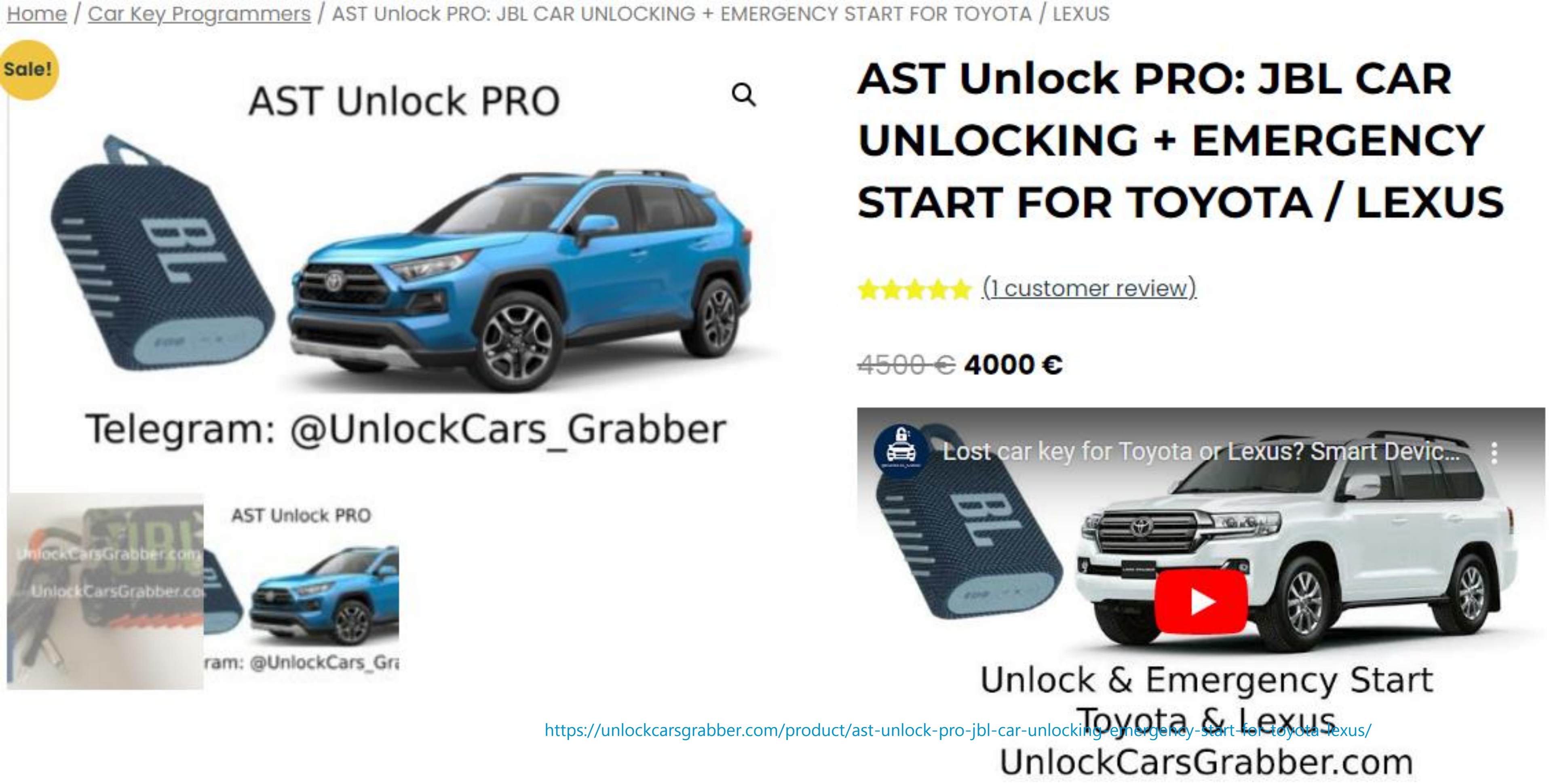
ISO/SAE 21434:2021, Table G.8, p.89



Executing uname -a

```
Linux cmu 3.0.35 #1 SMP PREEMPT Fri Nov 20 16:39:36 IST 2015 ar
```

https://github.com/shipcod3/mazda_getInfo
https://www.mazda3revolution.com/threads/the-infotainment-project.57714/



Home / Car Key Programmers / AST Unlock PRO: JBL CAR UNLOCKING + EMERGENCY START FOR TOYOTA / LEXUS

Sale!

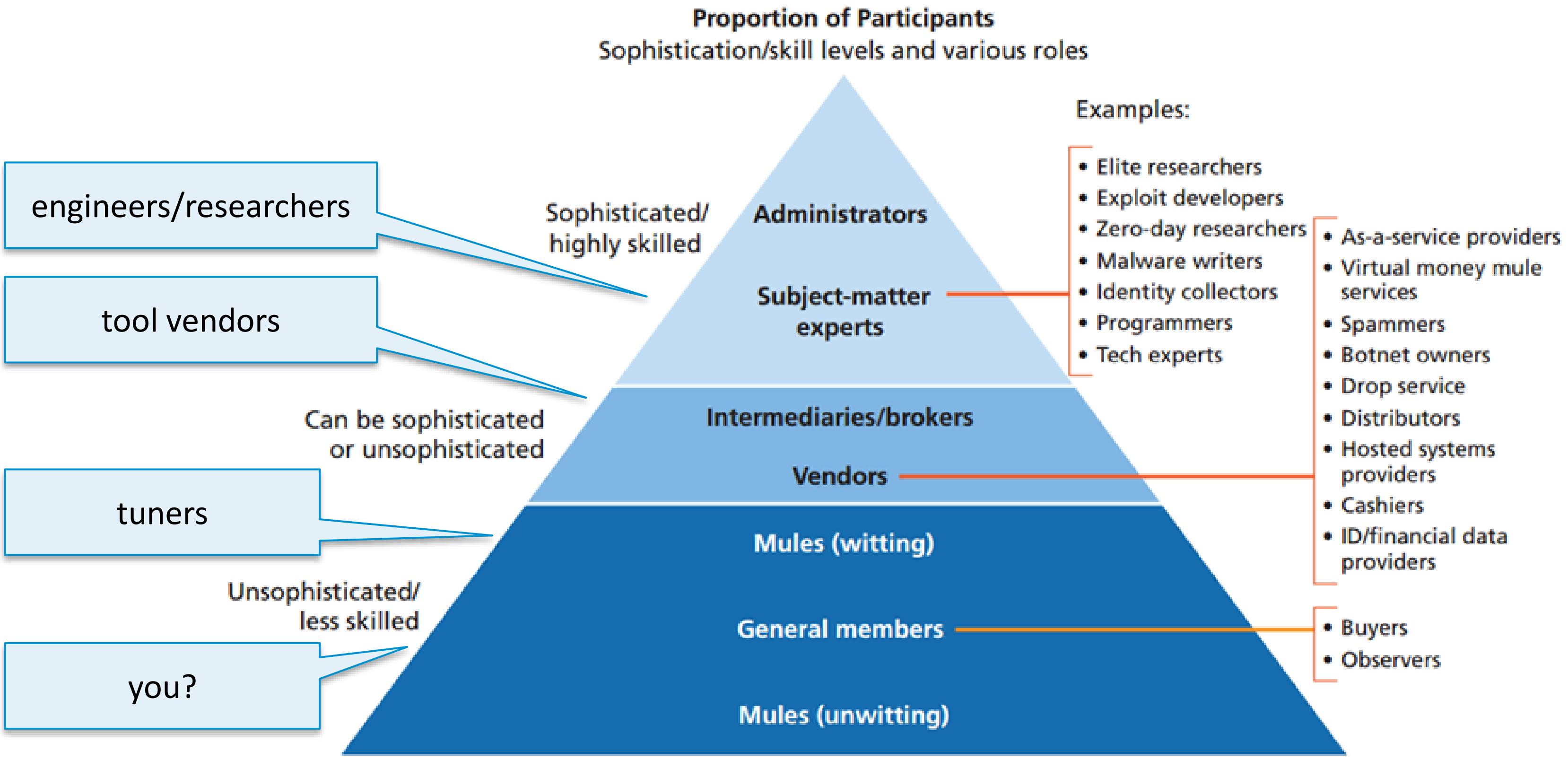
AST Unlock PRO: JBL CAR UNLOCKING + EMERGENCY START FOR TOYOTA / LEXUS

★★★★★ (1 customer review)

~~4500 €~~ **4000 €**

https://unlockcarsgrabber.com/product/ast-unlock-pro-jbl-car-unlocking-emergency-start-for-toyota-lexus/

Different Levels of Participants in the Underground Market



Proportion of Participants
Sophistication/skill levels and various roles

engineers/researchers

tool vendors

tuners

you?

Sophisticated/ highly skilled

Can be sophisticated or unsophisticated

Unsophisticated/ less skilled

Administrators

Subject-matter experts

Intermediaries/brokers

Vendors

Mules (witting)

General members

Mules (unwitting)

Examples:

- Elite researchers
- Exploit developers
- Zero-day researchers
- Malware writers
- Identity collectors
- Programmers
- Tech experts

- As-a-service providers
- Virtual money mule services
- Spammers
- Botnet owners
- Drop service
- Distributors
- Hosted systems providers
- Cashiers
- ID/financial data providers

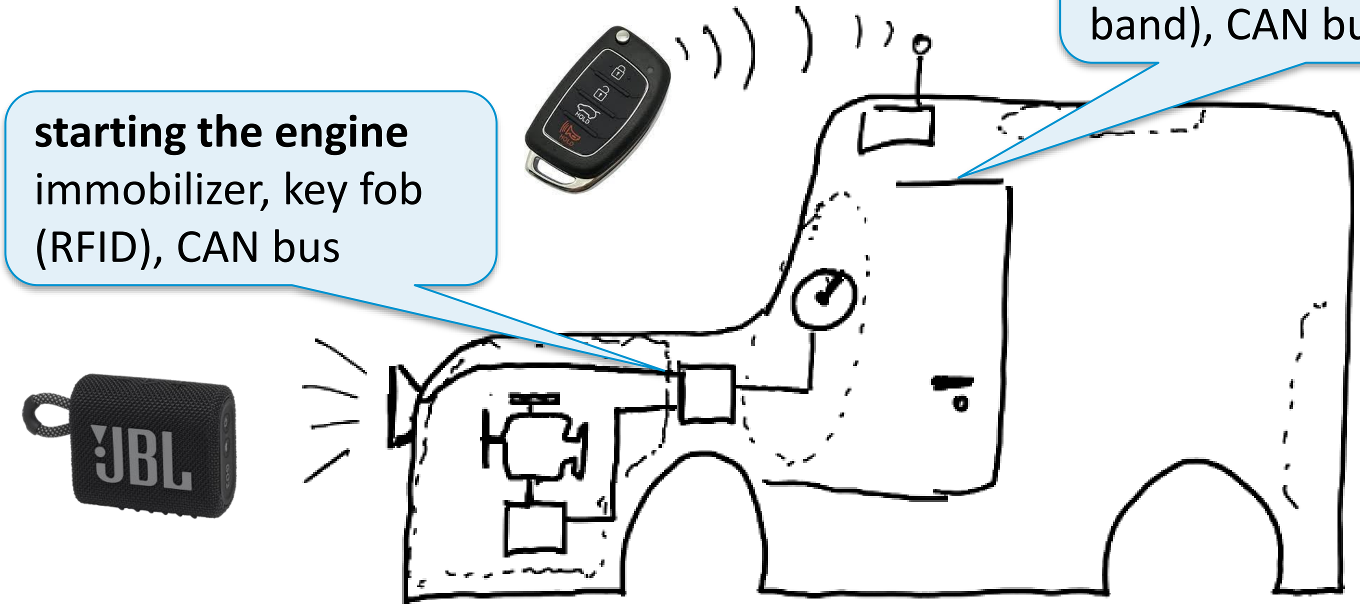
- Buyers
- Observers

SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.

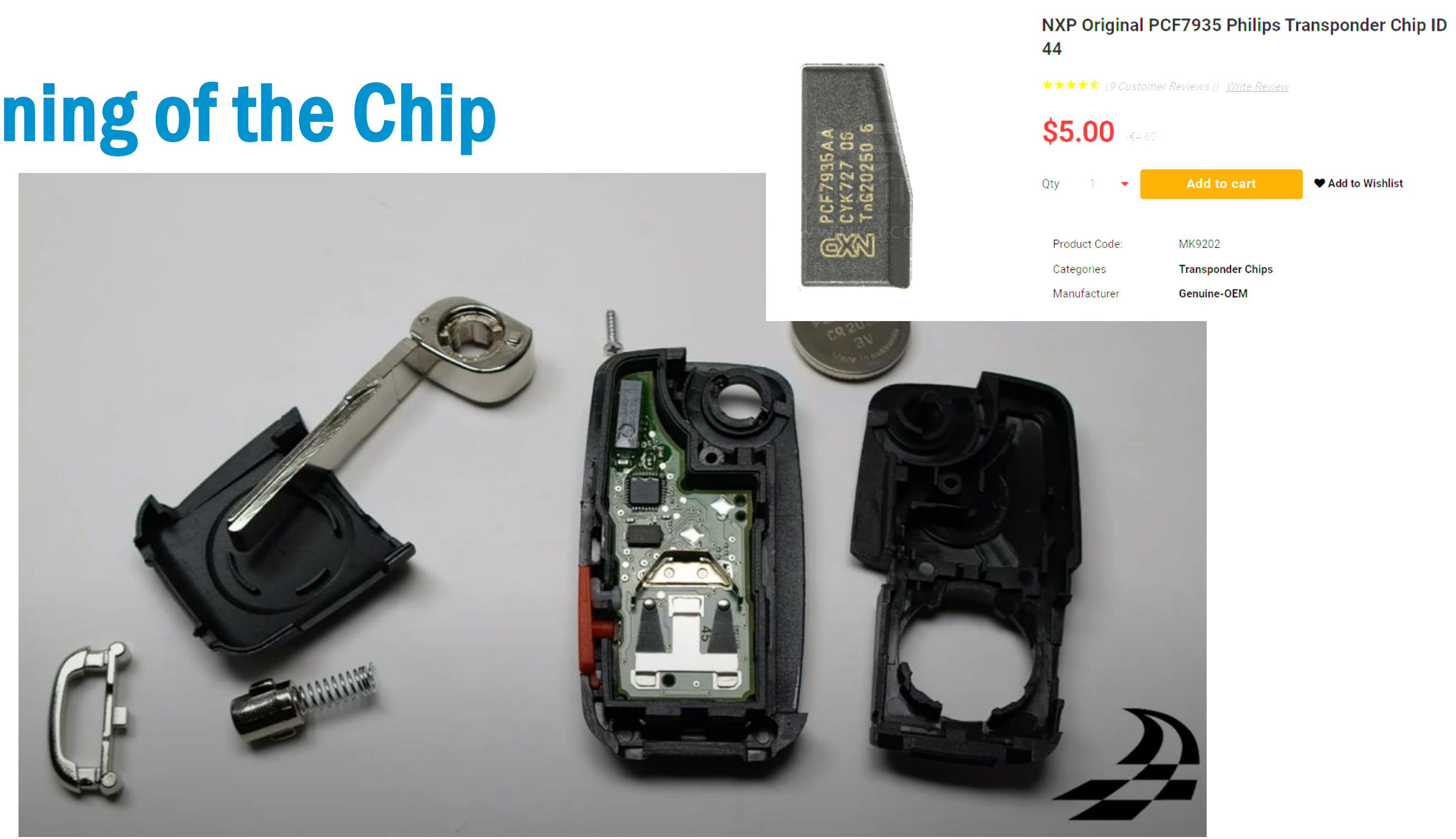
Threat Model

starting the engine
immobilizer, key fob (RFID), CAN bus

getting inside the car
doors, metal, key fob (IMS band), CAN bus



Cloning of the Chip



NXP Original PCF7935 Philips Transponder Chip ID 44

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

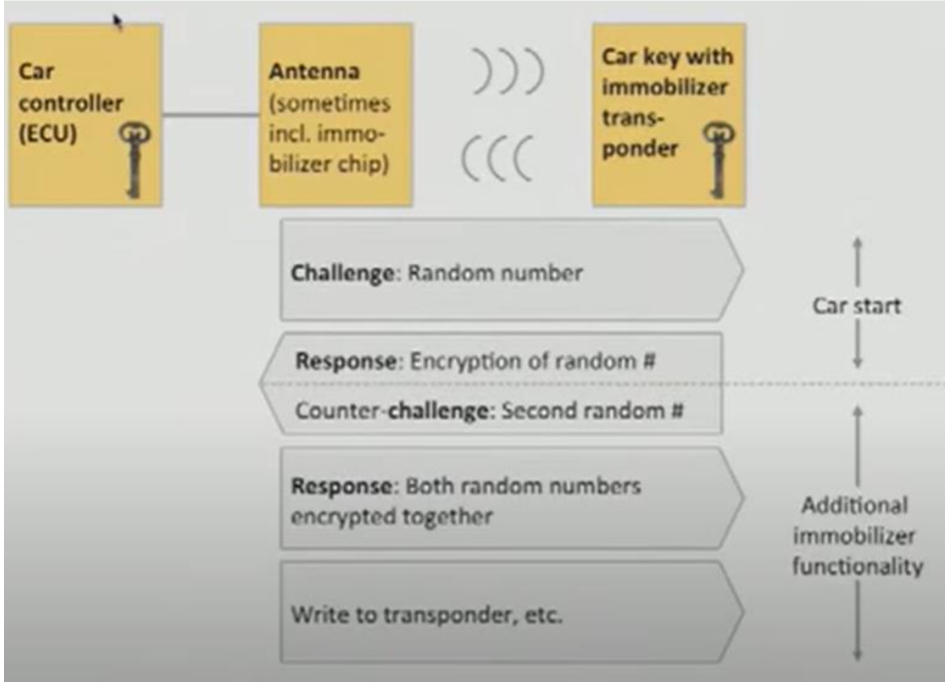
$5.00 (€4.60)

Qty 1 ▾ Add to cart ♥ Add to Wishlist

Product Code:	MK9202
Categories	**Transponder Chips**
Manufacturer	**Genuine-OEM**

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

Immobilizer



Car controller (ECU)

Antenna (sometimes incl. immobilizer chip)

Car key with immobilizer transponder

Challenge: Random number

Response: Encryption of random #

Counter-**challenge**: Second random #

Response: Both random numbers encrypted together

Write to transponder, etc.

Car start

Additional immobilizer functionality

https://media.ccc.de/v/konferenz_mp6_og_-_2013-07-05_17:00_-_car_immobilizer_hacking_-_karsten_nohl_-_5034

Karsten Nohl nohl@srlabs.de

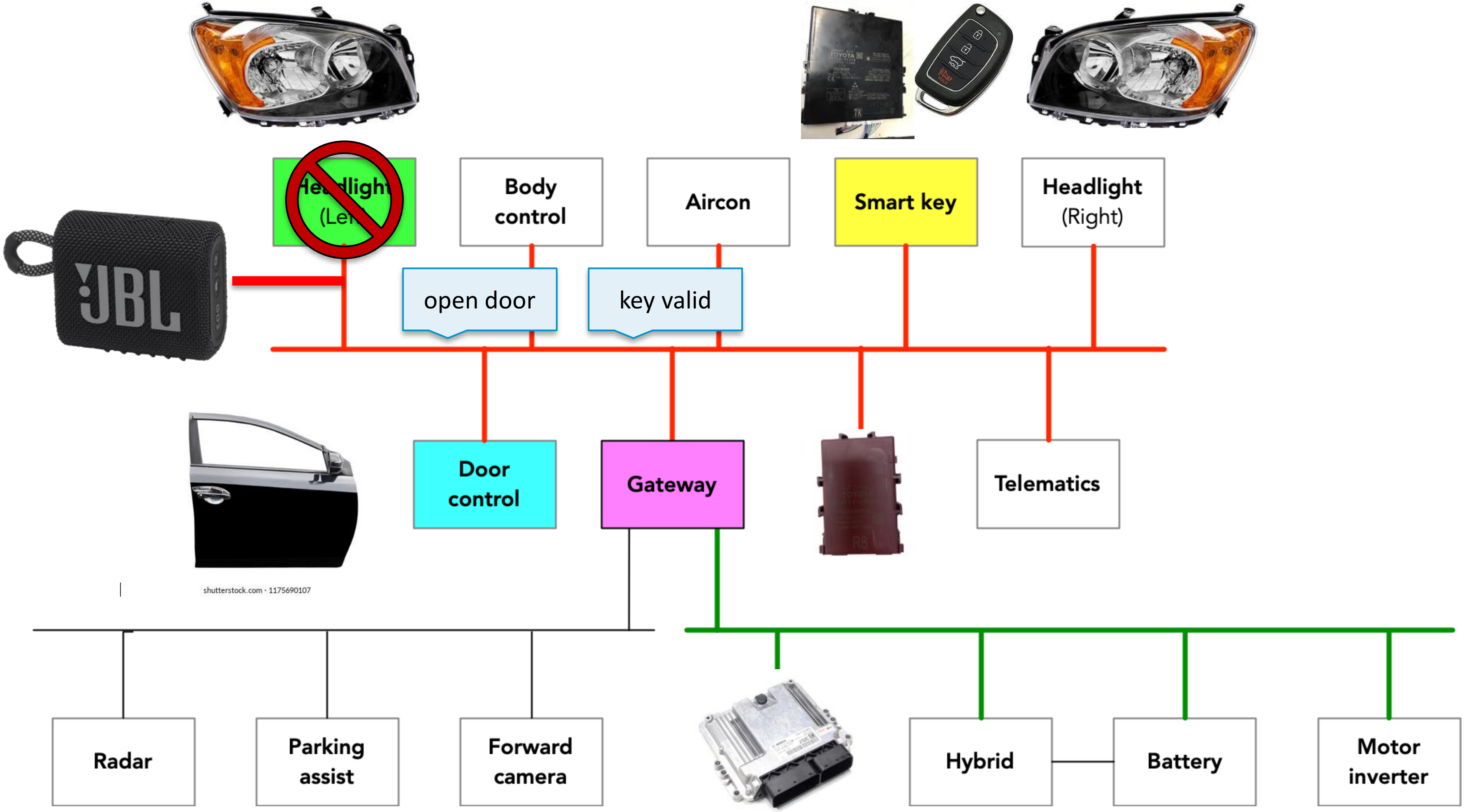


Image: https://kentindell.github.io/2023/04/03/can-injection/

The CAN frame

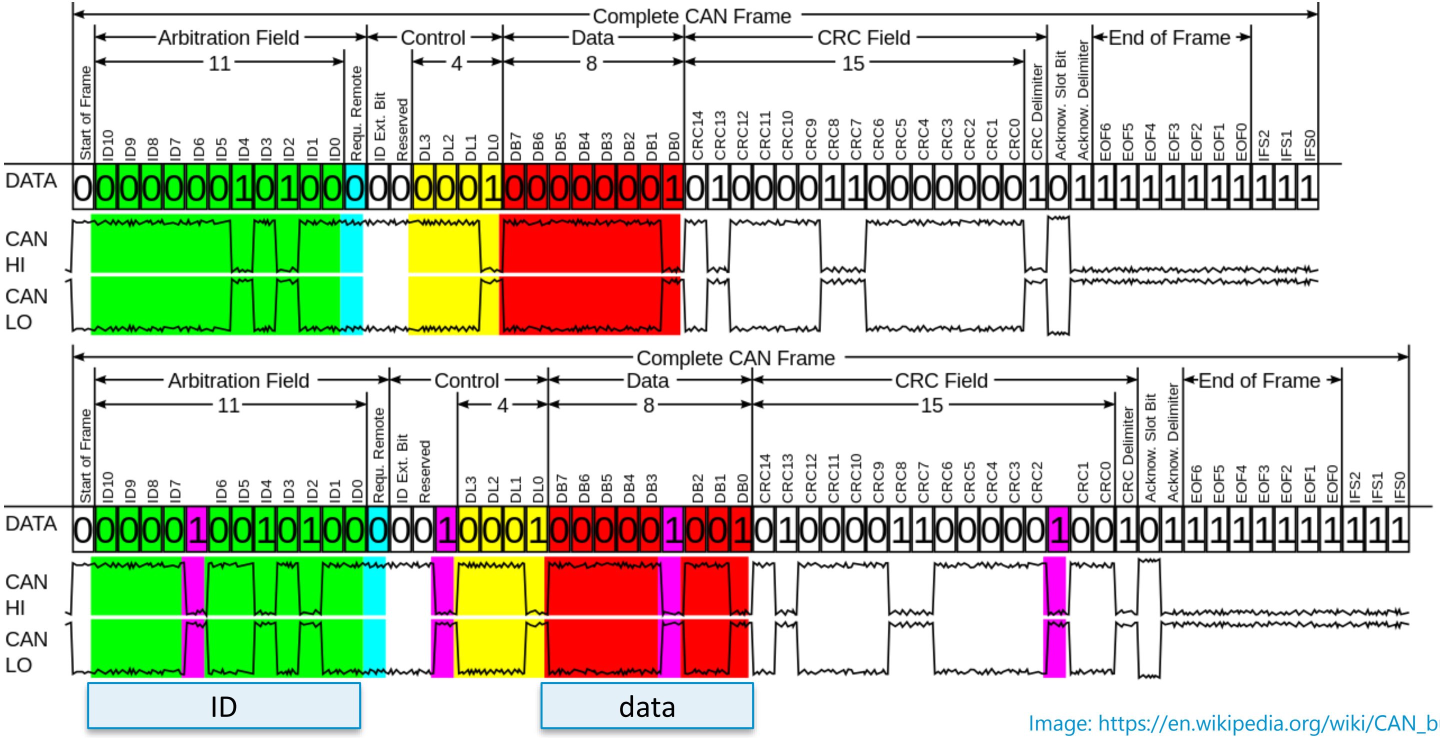


Image: https://en.wikipedia.org/wiki/CAN_bus

CAN Interfaces

Professional use:

- Intrepid ValueCAN
- Vector Can Case

Budget lab:

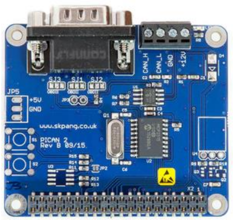
- USBTin
- Raspberry PiCAN

Intrepid ValueCAN

Vector Can Case

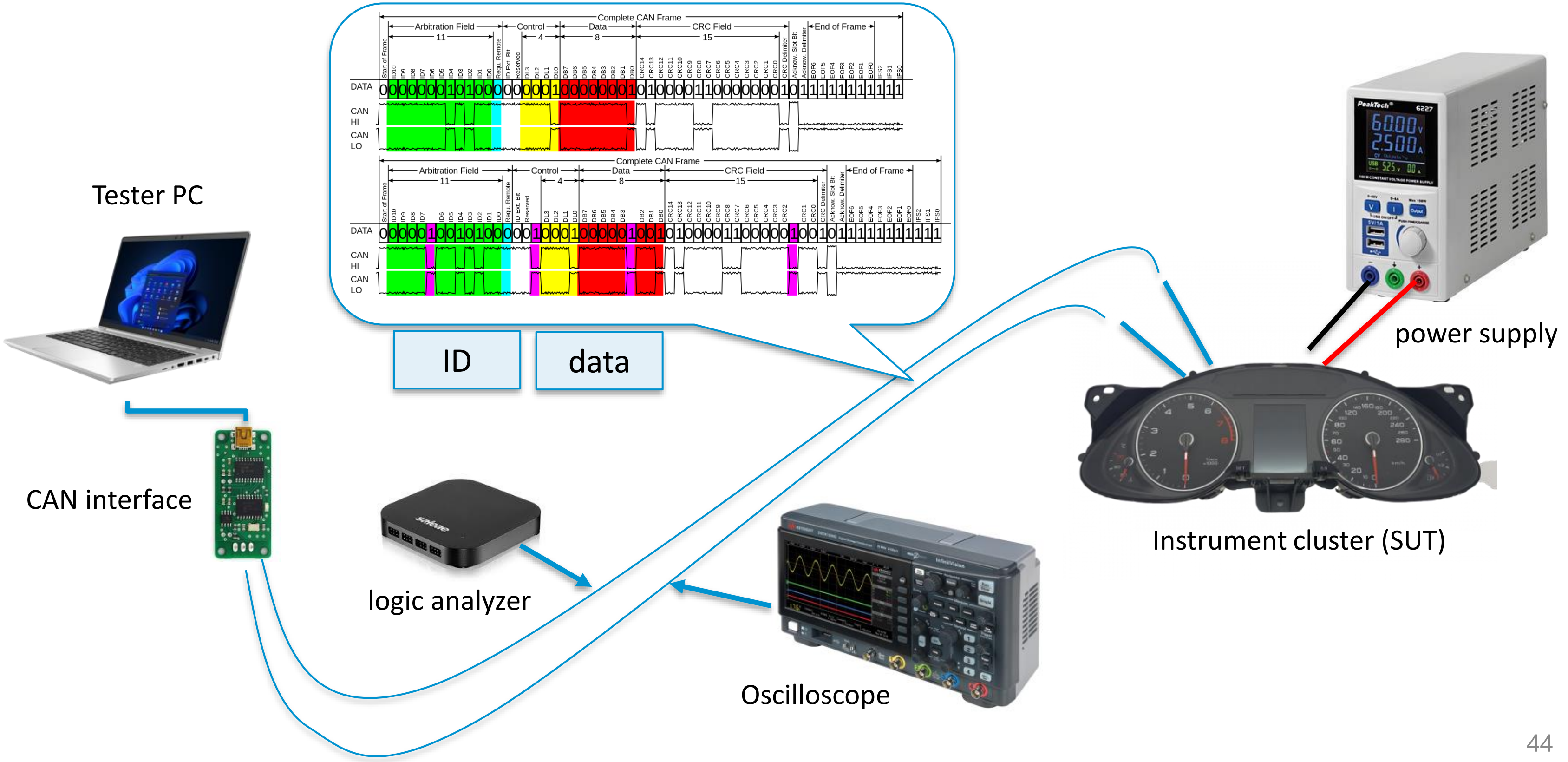
Peak PCAN-USBc

USBTin



PiCAN

Setup for Research



ID

data

Tester PC

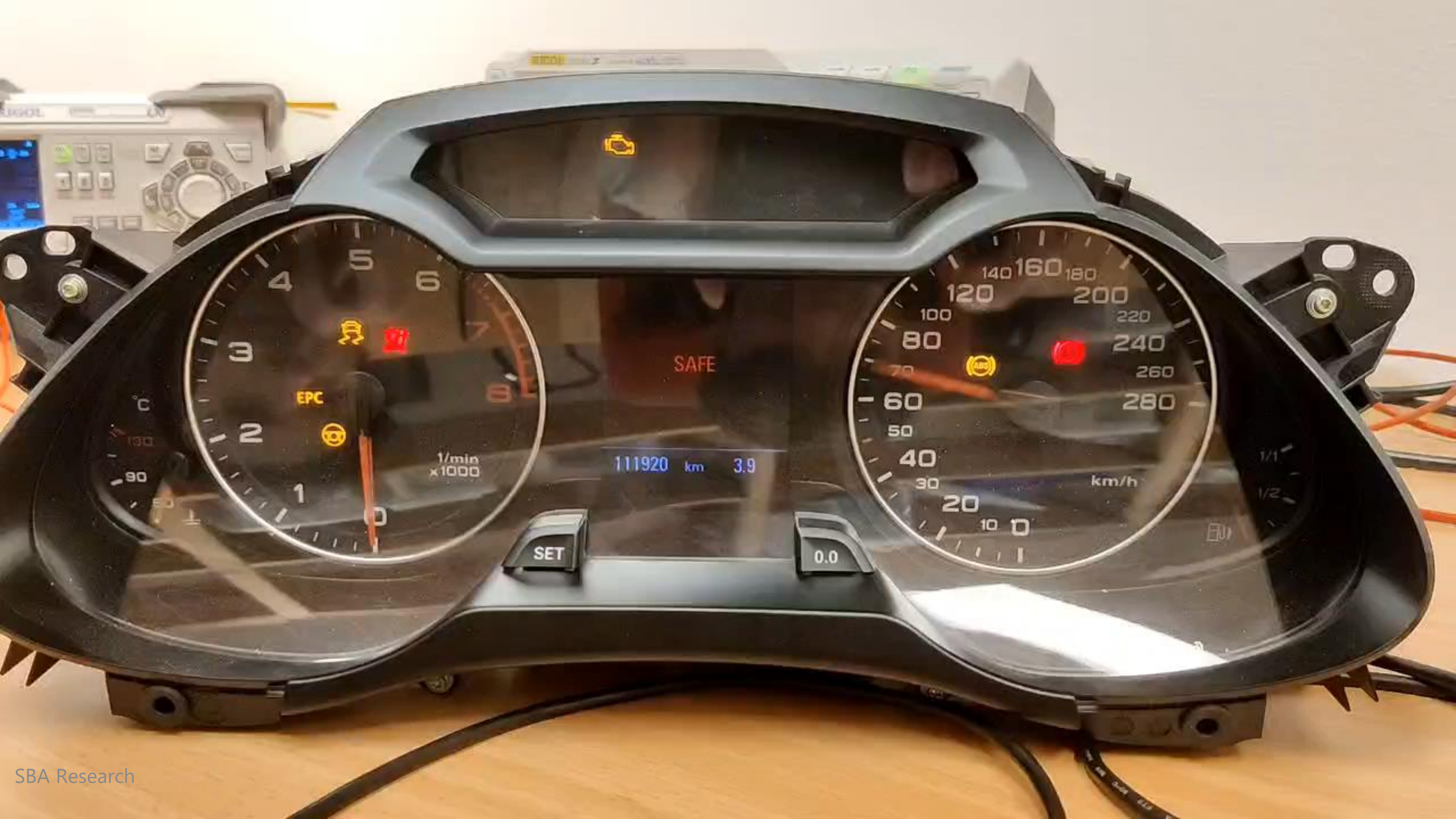
CAN interface

logic analyzer

Oscilloscope

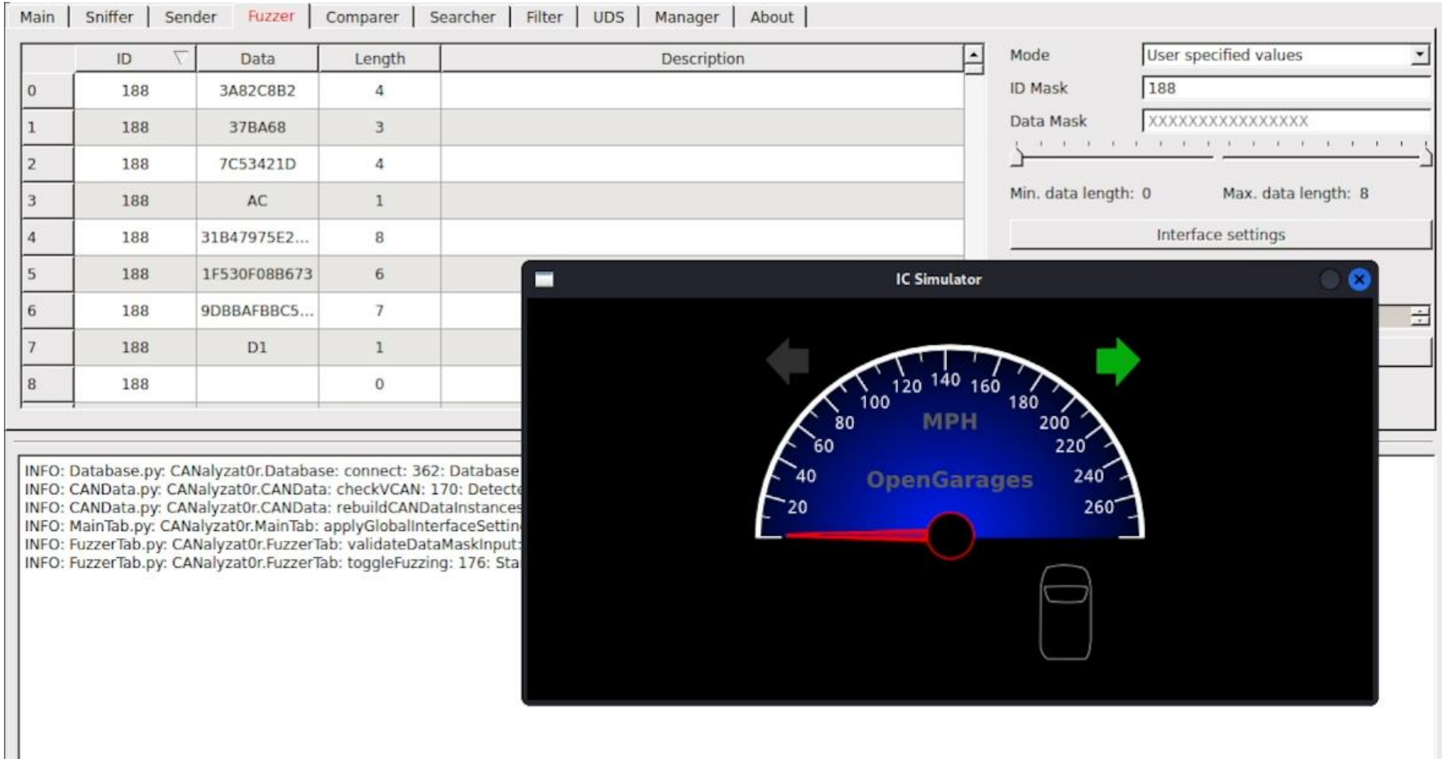
Instrument cluster (SUT)

power supply



SBA Research

Demo: Cangen / Canalyzat0r (Fuzzing)



	ID	Data	Length	Description
0	188	3A82C8B2	4	
1	188	37BA68	3	
2	188	7C53421D	4	
3	188	AC	1	
4	188	31B47975E2...	8	
5	188	1F530F08B673	6	
6	188	9DBBAFBBC5...	7	
7	188	D1	1	
8	188		0	

Mode: User specified values

ID Mask: 188

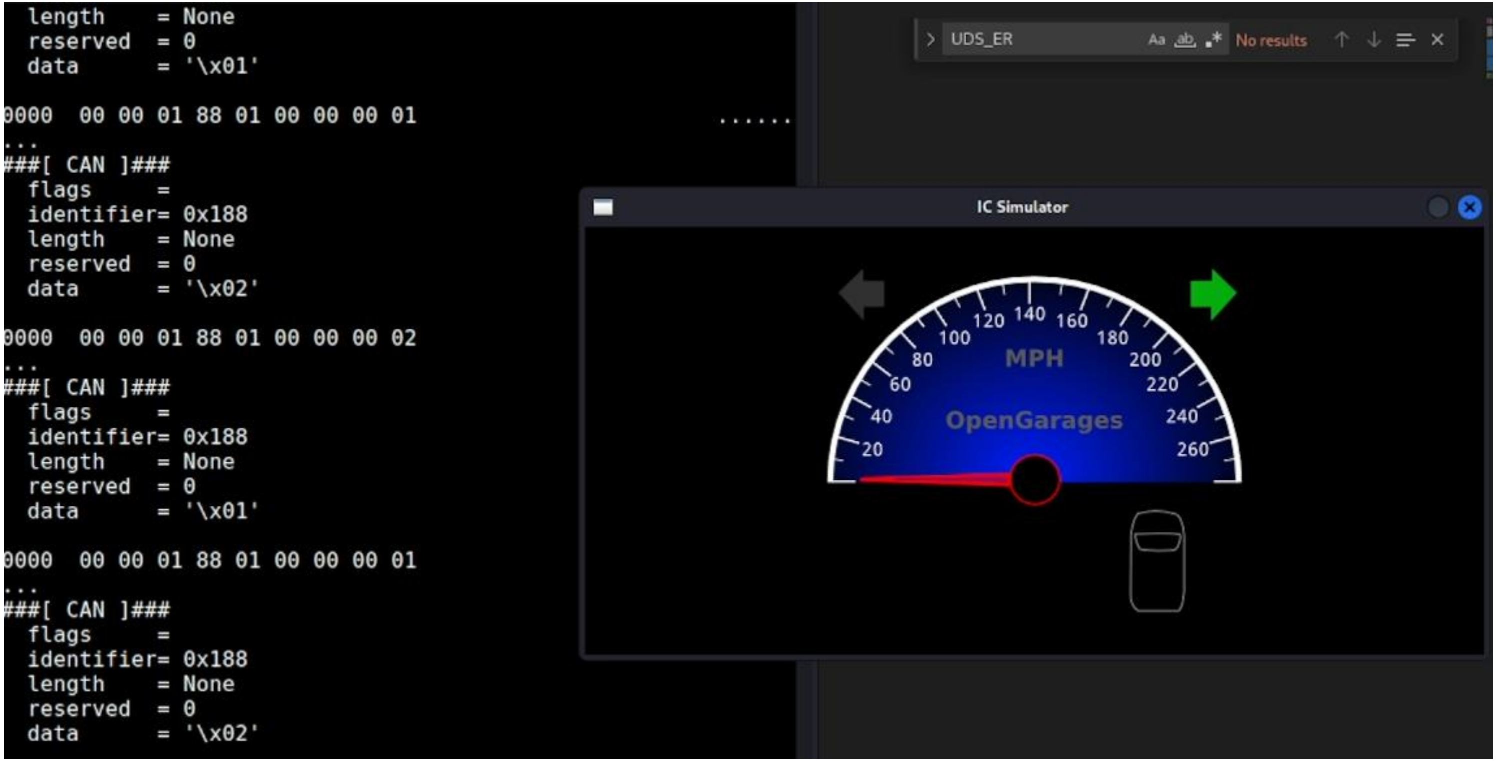
Data Mask: XXXXXXXXXXXXXXXX

Min. data length: 0

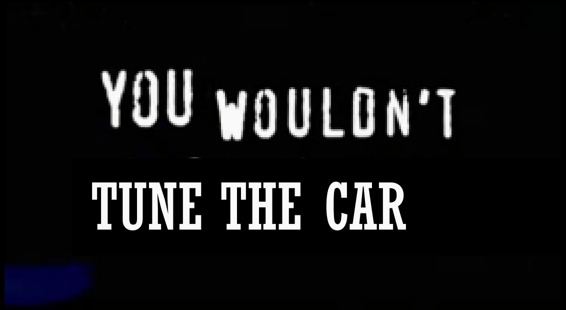
Max. data length: 8

```
INFO: Database.py: CANalyzat0r.Database: connect: 362: Database
INFO: CANData.py: CANalyzat0r.CANData: checkVCAN: 170: Detecte
INFO: CANData.py: CANalyzat0r.CANData: rebuildCANDataInstances
INFO: MainTab.py: CANalyzat0r.MainTab: applyGlobalInterfaceSettin
INFO: FuzzerTab.py: CANalyzat0r.FuzzerTab: validateDataMaskInput:
INFO: FuzzerTab.py: CANalyzat0r.FuzzerTab: toggleFuzzing: 176: Sta
```

Demo: Trigger Indicators with Scapy



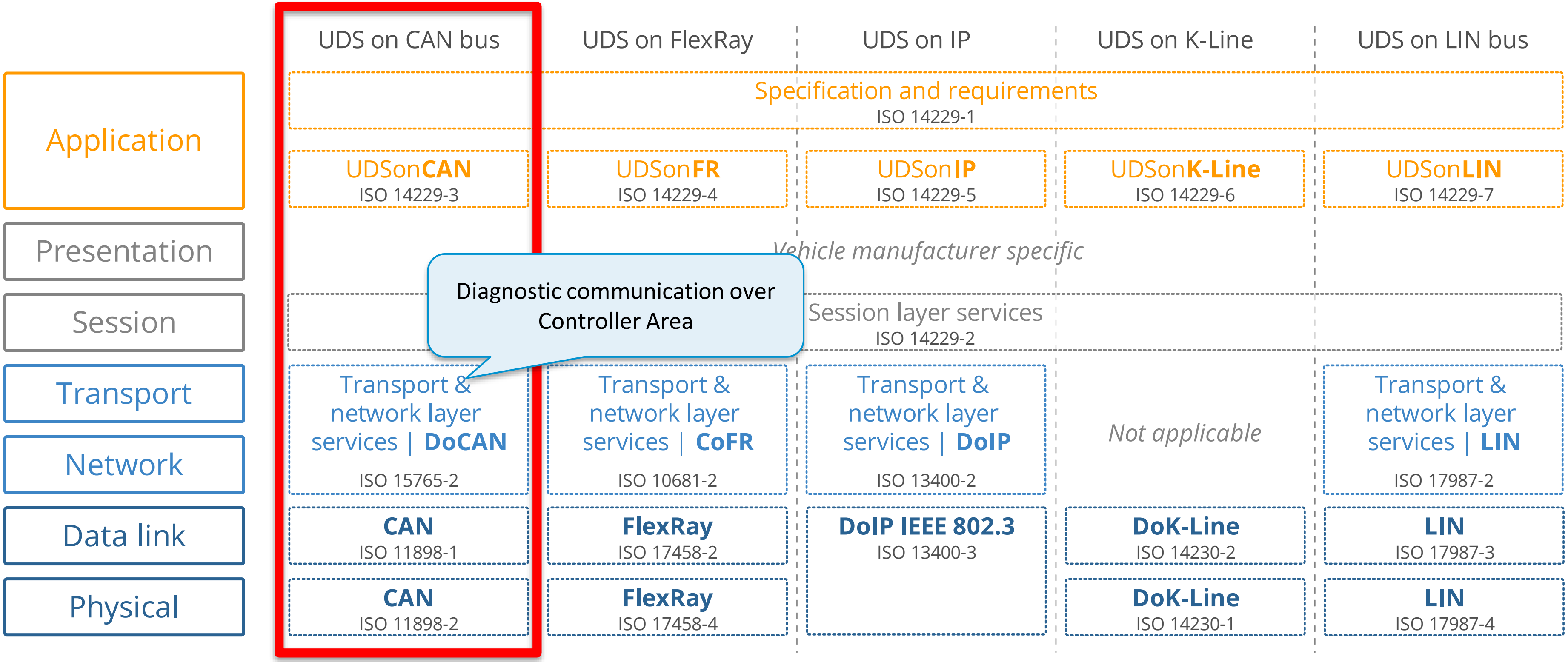
```
  length     = None
  reserved   = 0
  data       = '\x01'

0000   00 00 01 88 01 00 00 00 01                        .......
...
###[ CAN ]###
  flags      =
  identifier= 0x188
  length     = None
  reserved   = 0
  data       = '\x02'

0000   00 00 01 88 01 00 00 00 02
...
###[ CAN ]###
  flags      =
  identifier= 0x188
  length     = None
  reserved   = 0
  data       = '\x01'

0000   00 00 01 88 01 00 00 00 01
...
###[ CAN ]###
  flags      =
  identifier= 0x188
  length     = None
  reserved   = 0
  data       = '\x02'
```



TUNE THE CAR

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

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

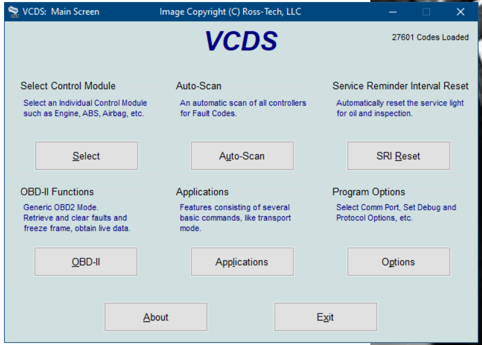


	UDS on CAN bus	UDS on FlexRay	UDS on IP	UDS on K-Line	UDS on LIN bus
Application	Specification and requirements ISO 14229-1				
	UDSon**CAN** ISO 14229-3	UDSon**FR** ISO 14229-4	UDSon**IP** ISO 14229-5	UDSon**K-Line** ISO 14229-6	UDSon**LIN** ISO 14229-7
Presentation	*Vehicle manufacturer specific*				
Session	Session layer services ISO 14229-2				
Transport	Transport & network layer services | **DoCAN** ISO 15765-2	Transport & network layer services | **CoFR** ISO 10681-2	Transport & network layer services | **DoIP** ISO 13400-2	*Not applicable*	Transport & network layer services | **LIN** ISO 17987-2
Network					
Data link	**CAN** ISO 11898-1	**FlexRay** ISO 17458-2	**DoIP IEEE 802.3** ISO 13400-3	**DoK-Line** ISO 14230-2	**LIN** ISO 17987-3
Physical	**CAN** ISO 11898-2	**FlexRay** ISO 17458-4		**DoK-Line** ISO 14230-1	**LIN** ISO 17987-4

Diagnostic communication over Controller Area

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

Diagnostics (UDS over CAN ISO 14229-3)



VCDS

27601 Codes Loaded

Select Control Module

Select an Individual Control Module such as Engine, ABS, Airbag, etc.

Auto-Scan

An automatic scan of all controllers for Fault Codes.

Service Reminder Interval Reset

Automatically reset the service light for oil and inspection.

OBD-II Functions

Generic OBD2 Mode. Retrieve and clear faults and freeze frame, obtain live data.

Applications

Features consisting of several basic commands, like transport mode.

Program Options

Select Comm Port, Set Debug and Protocol Options, etc.

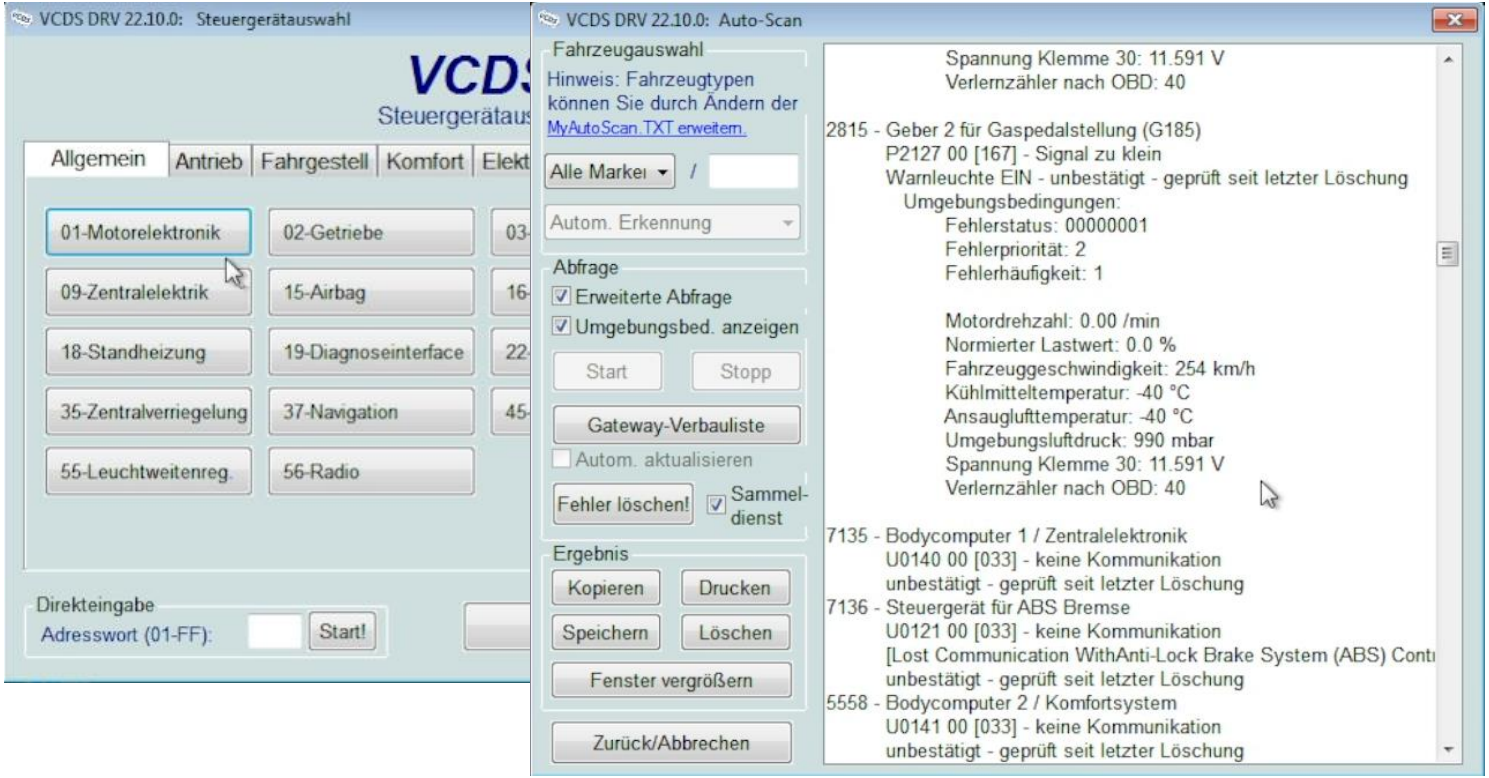
VCDS Ross Tech https://www.ross-tech.com/vag-com/

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

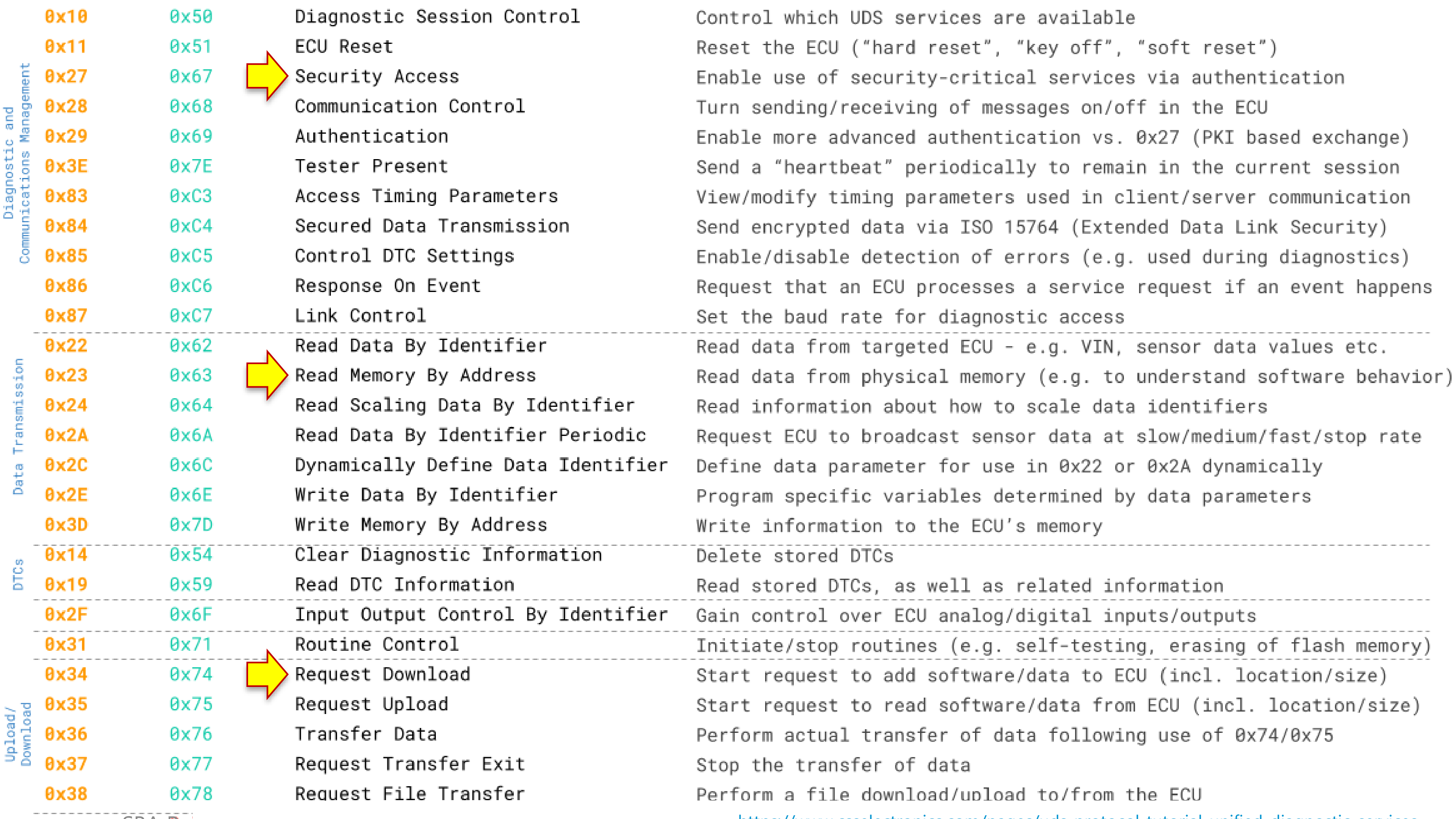
WARNING:

- do testing of hardware with a trained electrical engineer
- don‘t do this on your car [on the streets]
- manipulation could harm your car, your equipment or your personal health and safety!

Demo: Diagnostics with VCDS



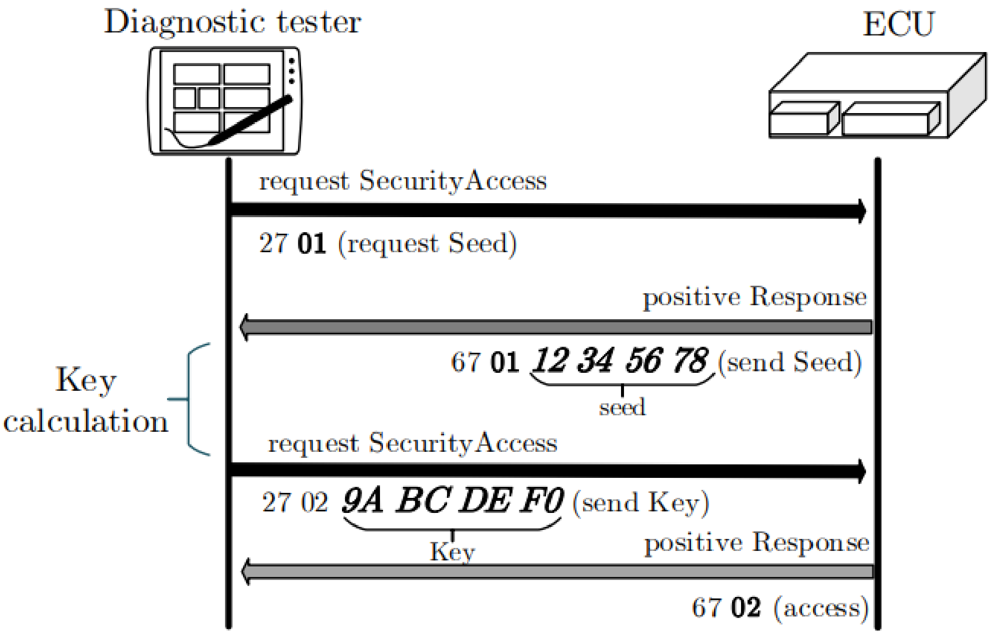
```
                Spannung Klemme 30: 11.591 V
                Verlernzähler nach OBD: 40

2815 - Geber 2 für Gaspedalstellung (G185)
          P2127 00 [167] - Signal zu klein
          Warnleuchte EIN - unbestätigt - geprüft seit letzter Löschung
             Umgebungsbedingungen:
                Fehlerstatus: 00000001
                Fehlerpriorität: 2
                Fehlerhäufigkeit: 1

                Motordrehzahl: 0.00 /min
                Normierter Lastwert: 0.0 %
                Fahrzeuggeschwindigkeit: 254 km/h
                Kühlmitteltemperatur: -40 °C
                Ansauglufttemperatur: -40 °C
                Umgebungsluftdruck: 990 mbar
                Spannung Klemme 30: 11.591 V
                Verlernzähler nach OBD: 40

7135 - Bodycomputer 1 / Zentralelektronik
          U0140 00 [033] - keine Kommunikation
          unbestätigt - geprüft seit letzter Löschung
7136 - Steuergerät für ABS Bremse
          U0121 00 [033] - keine Kommunikation
          [Lost Communication WithAnti-Lock Brake System (ABS) Conti
          unbestätigt - geprüft seit letzter Löschung
5558 - Bodycomputer 2 / Komfortsystem
          U0141 00 [033] - keine Kommunikation
          unbestätigt - geprüft seit letzter Löschung
```



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

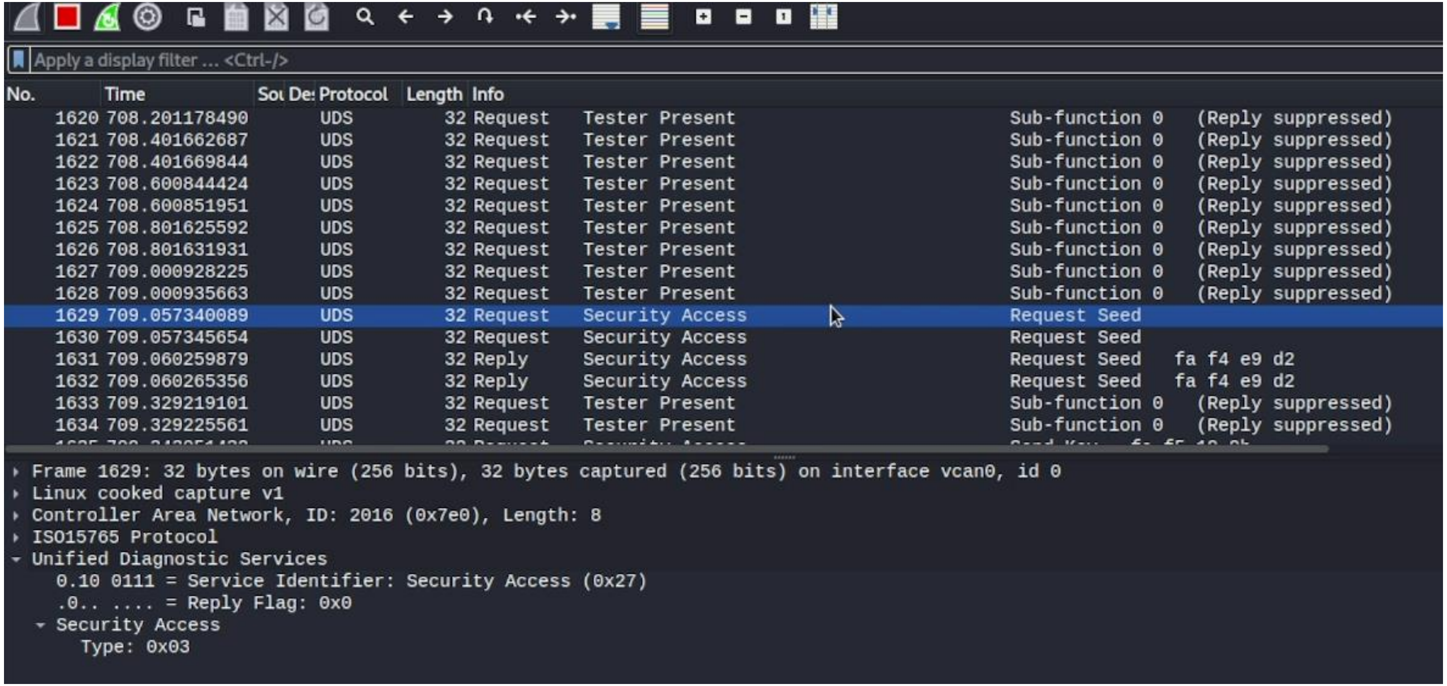
https://www.csselectronics.com/pages/uds-protocol-tutorial-unified-diagnostic-services

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

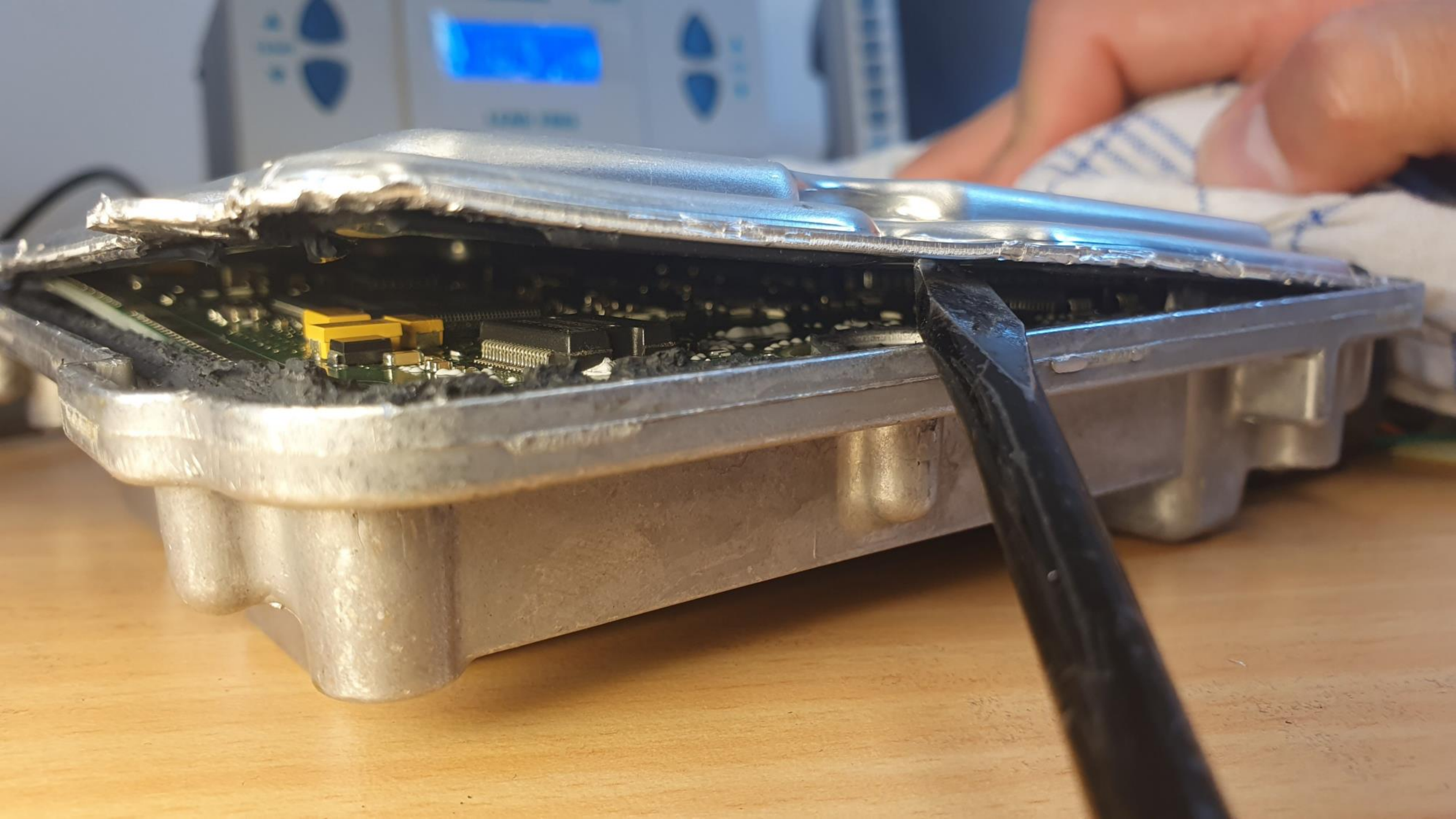
Demo: UDS Security Access Wireshark/Scapy

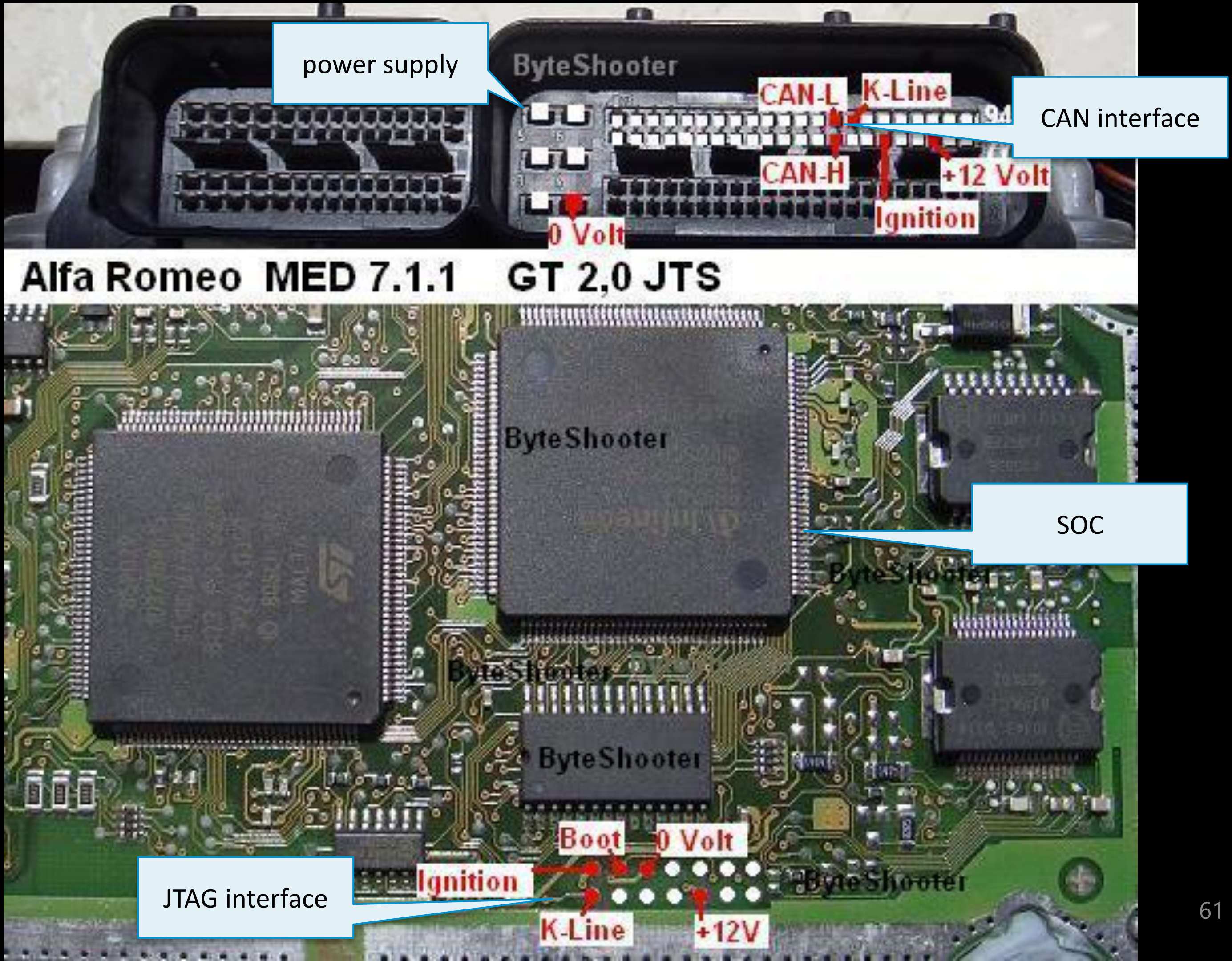


Apply a display filter … <Ctrl-/>

```
No.    Time            Sou Des Protocol  Length Info
  1620 708.201178490       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1621 708.401662687       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1622 708.401669844       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1623 708.600844424       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1624 708.600851951       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1625 708.801625592       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1626 708.801631931       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1627 709.000928225       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1628 709.000935663       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1629 709.057340089       UDS               32 Request   Security Access                      Request Seed
  1630 709.057345654       UDS               32 Request   Security Access                      Request Seed
  1631 709.060259879       UDS               32 Reply     Security Access                      Request Seed   fa f4 e9 d2
  1632 709.060265356       UDS               32 Reply     Security Access                      Request Seed   fa f4 e9 d2
  1633 709.329219101       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
  1634 709.329225561       UDS               32 Request   Tester Present                       Sub-function 0   (Reply suppressed)
```

```
▸ Frame 1629: 32 bytes on wire (256 bits), 32 bytes captured (256 bits) on interface vcan0, id 0
▸ Linux cooked capture v1
▸ Controller Area Network, ID: 2016 (0x7e0), Length: 8
▸ ISO15765 Protocol
▾ Unified Diagnostic Services
    0.10 0111 = Service Identifier: Security Access (0x27)
    .0.. .... = Reply Flag: 0x0
  ▾ Security Access
      Type: 0x03
```





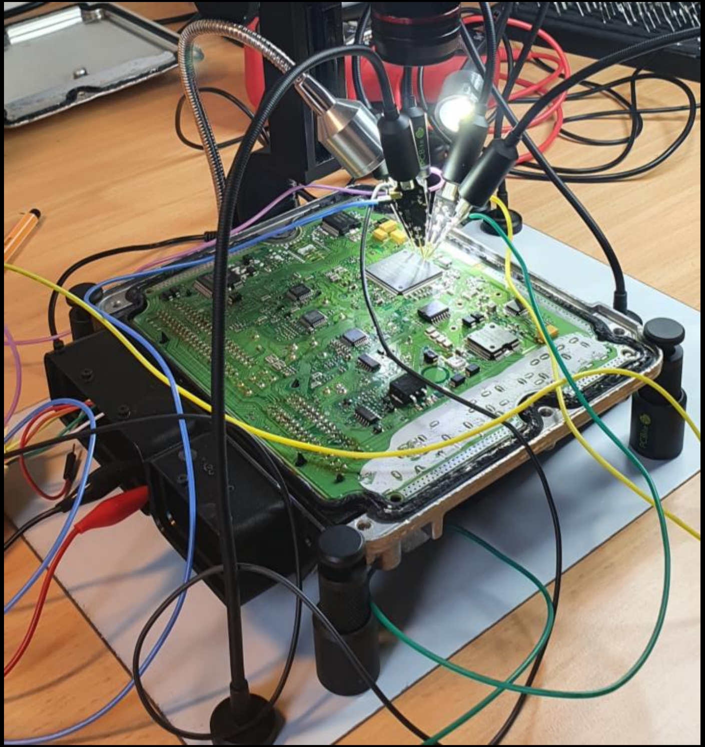
power supply

CAN interface

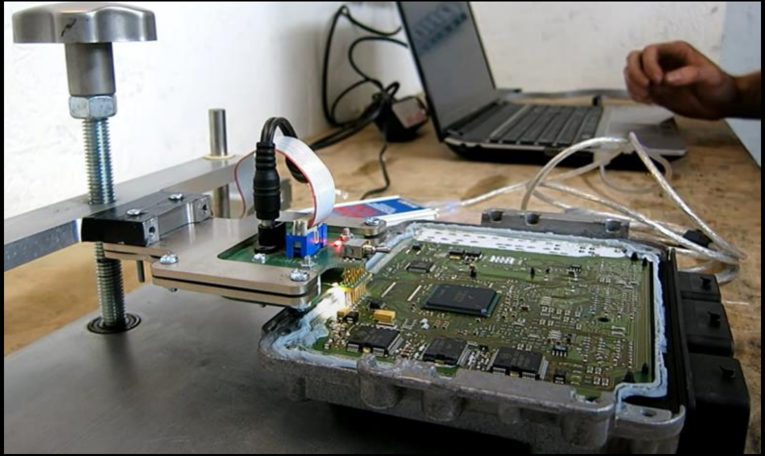
SOC

JTAG interface

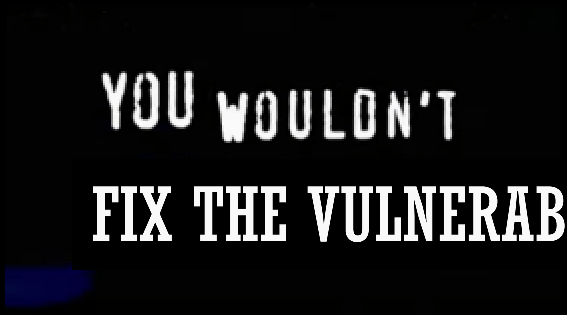
Side Channel Attacks and Debug Interfaces



JTAG access on the PCB



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



FIX THE VULNERABILITIES

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

Generic Solution Pattern: Zoning

- how small should the zones be?
- how are zones implemented? vlan, physical
- what is filtered?
- how is the wireing affected? cost, weight, assembly
- how is real time behavior affected?
- is this feasable in a complex supply chain?

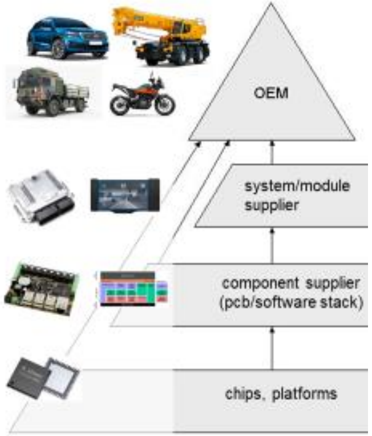
Generic Solution Pattern: Access Control

- who defines the access control architecture?
- who configures the rules on all devices?
- is this possible across multiple vendors?
- who is allowed to troubleshoot?
- what equipment is needed?
- how is a person/equipment authenticated?
- fail safe or sail secure?

Generic Solution Pattern: Cryptography

- who generates keys? how are keys renewed?
- diversity of keys: fleet/device/car/owner?
- what algorithm should we be using (post-quantum)?
- who (official/unofficial repair shops) gets the keys?
- who can debug encrypted traffic?
- how does this effect safety and realtime behavior?
- how are keys stored? in firmware, TPM, TPE?
- what happens with updates?

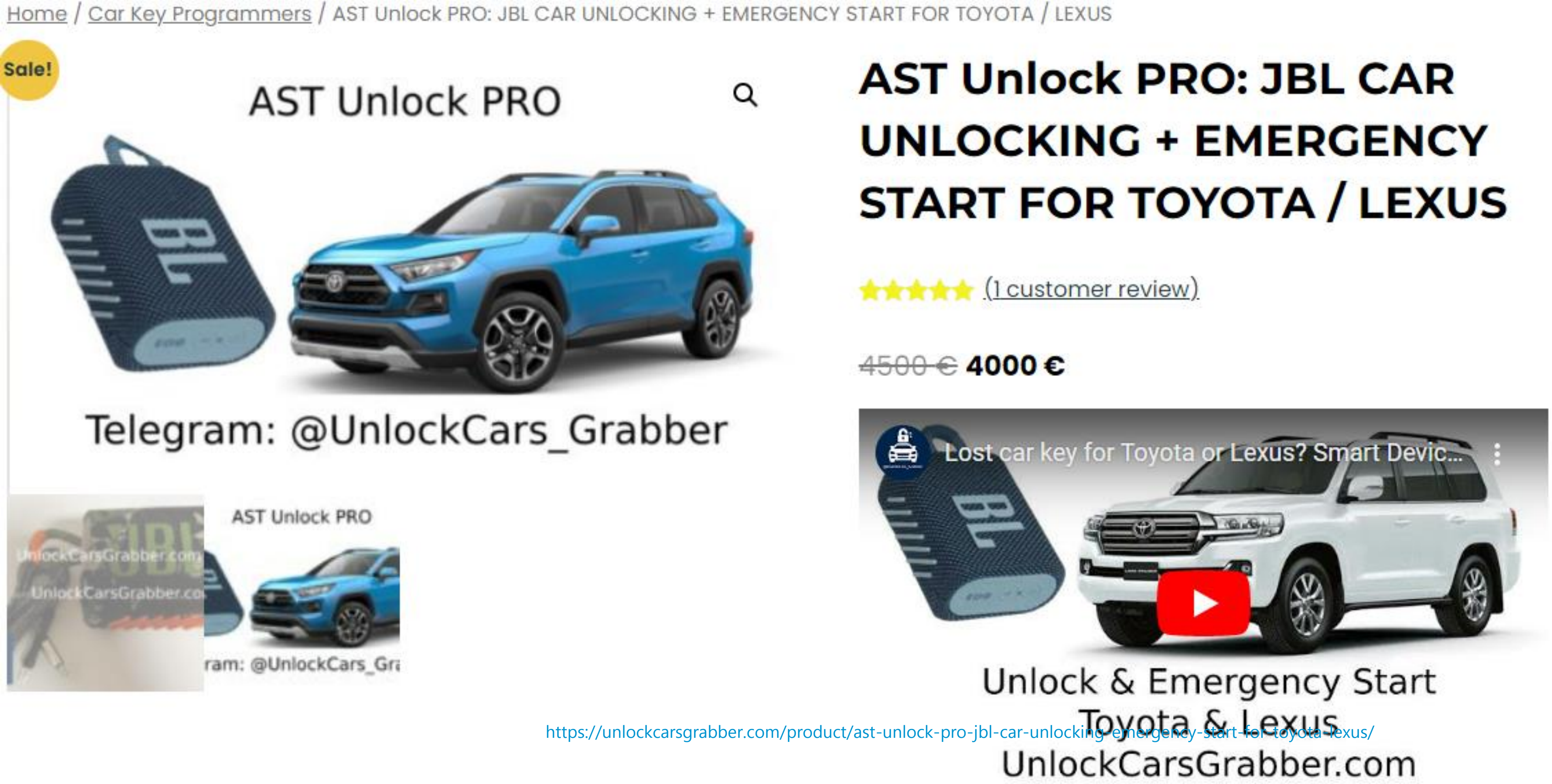
People, processes technology



Engineering / Manufacturing / Supply chain

Runtime / Usability / Safety / Availability

Maintainability / Troubleshooting



Home / Car Key Programmers / AST Unlock PRO: JBL CAR UNLOCKING + EMERGENCY START FOR TOYOTA / LEXUS

Sale!

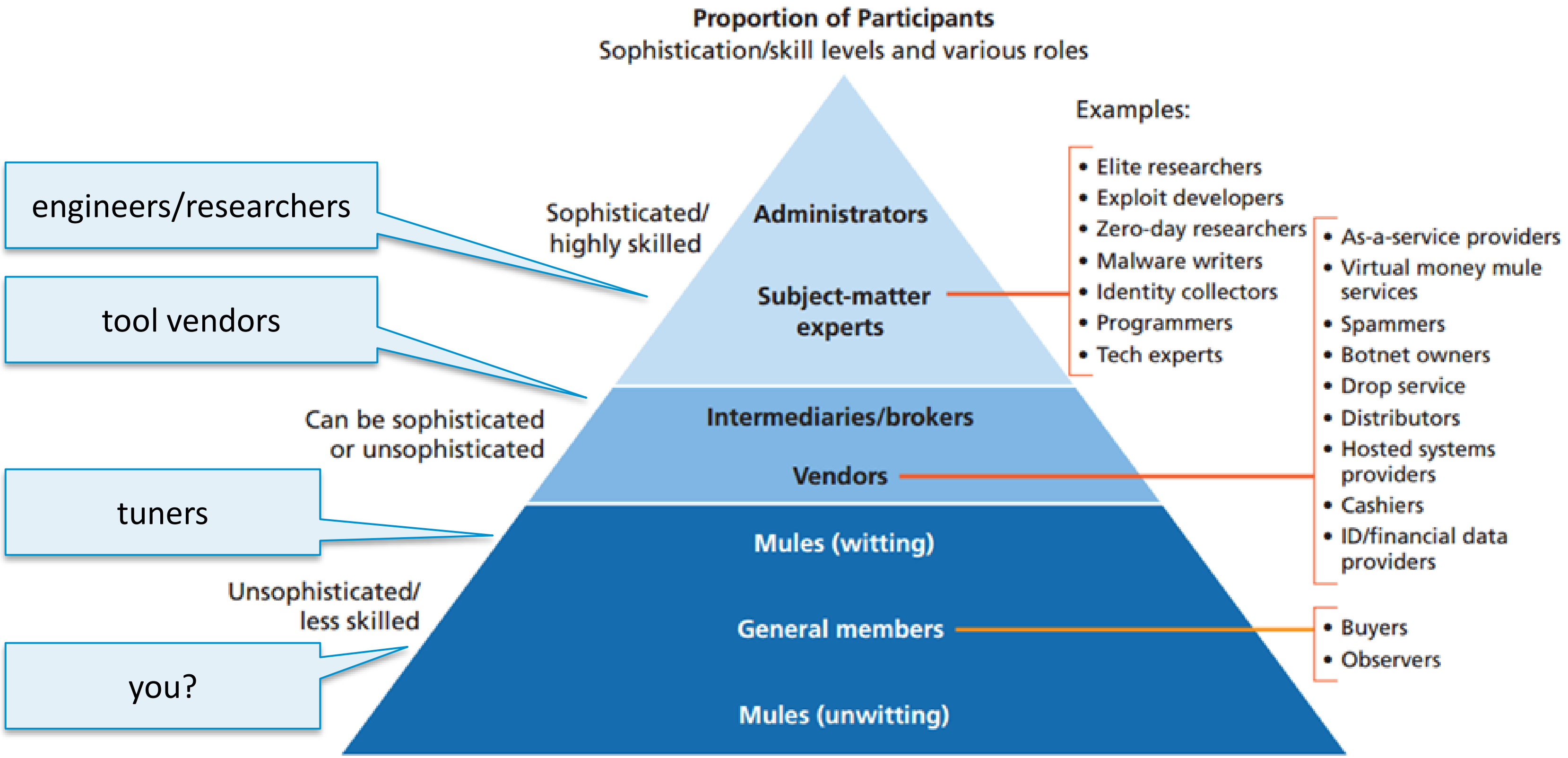
AST Unlock PRO: JBL CAR UNLOCKING + EMERGENCY START FOR TOYOTA / LEXUS

★★★★★ (1 customer review)

~~4500 €~~ **4000 €**

https://unlockcarsgrabber.com/product/ast-unlock-pro-jbl-car-unlocking-emergency-start-for-toyota-lexus/

Different Levels of Participants in the Underground Market



Proportion of Participants

Sophistication/skill levels and various roles

Sophisticated/ highly skilled

Administrators

Subject-matter experts

Can be sophisticated or unsophisticated

Intermediaries/brokers

Vendors

Unsophisticated/ less skilled

Mules (witting)

General members

Mules (unwitting)

Examples:

- Elite researchers
- Exploit developers
- Zero-day researchers
- Malware writers
- Identity collectors
- Programmers
- Tech experts

- As-a-service providers
- Virtual money mule services
- Spammers
- Botnet owners
- Drop service
- Distributors
- Hosted systems providers
- Cashiers
- ID/financial data providers

- Buyers
- Observers

engineers/researchers

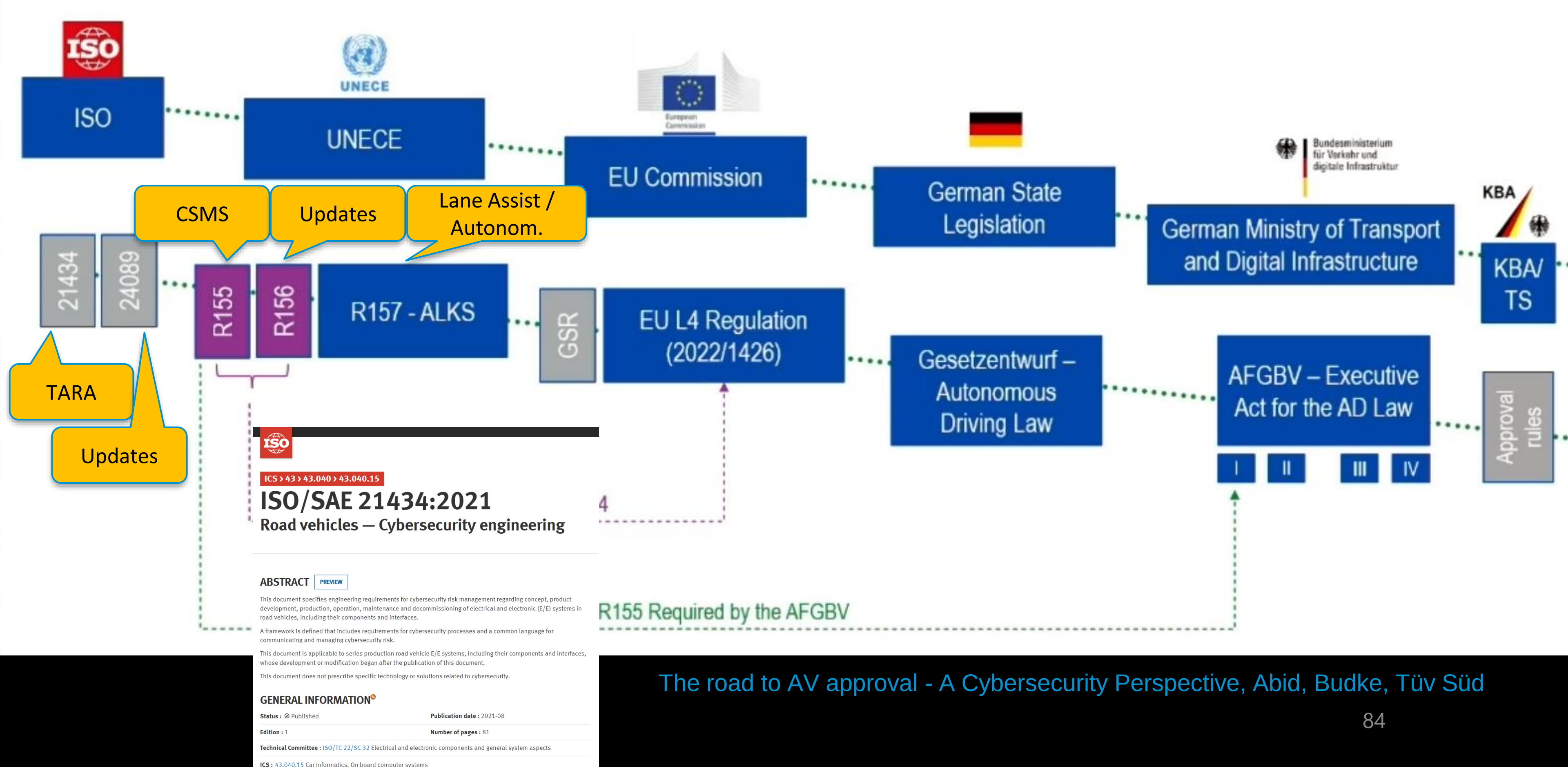
tool vendors

tuners

you?

SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.

How can it be verified or proven?


ISO
ISO
UNECE
UNECE
European Commission
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
4
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

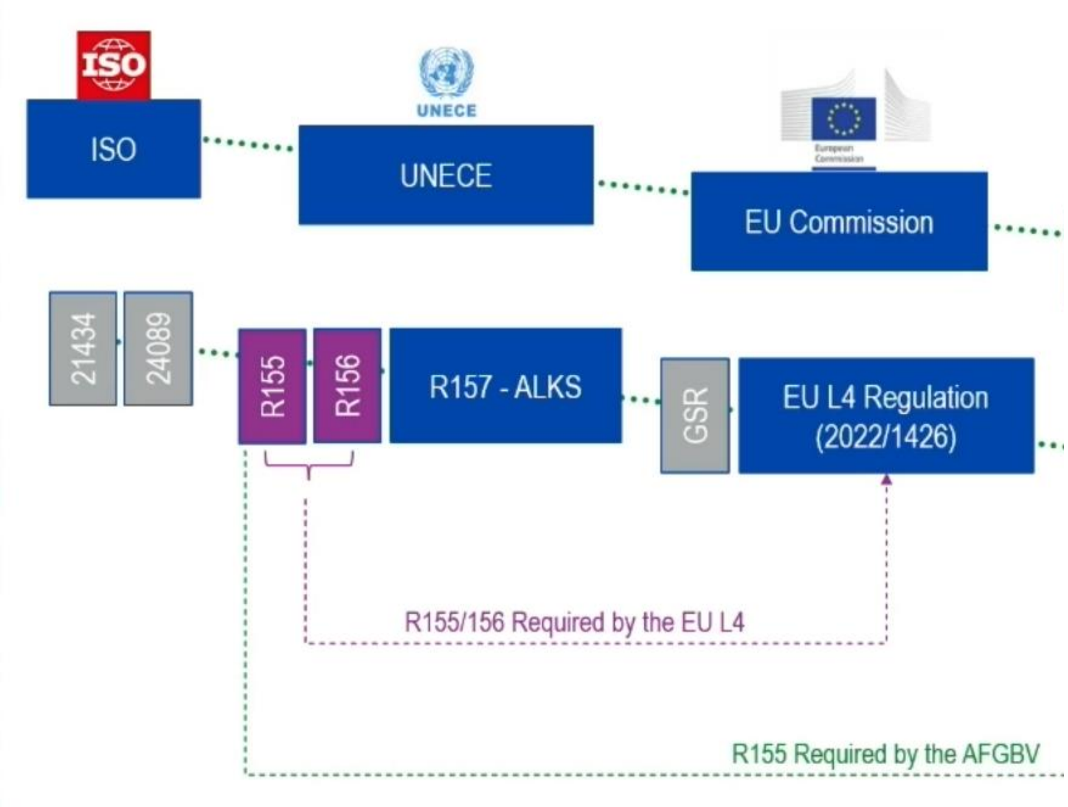
Publication date : 2021-08

Edition : 1

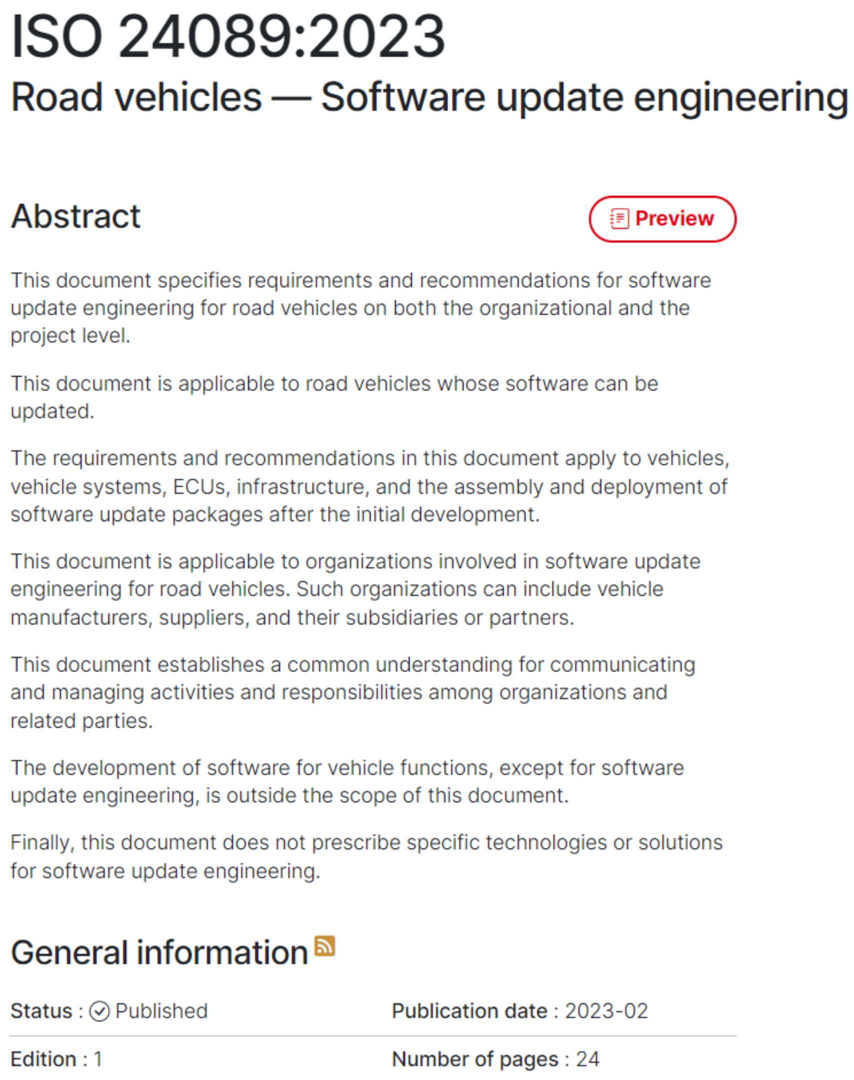
Number of pages : 81

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

ICS : 43.040.15 Car informatics. On board computer systems


ISO
UNECE
European Commission
ISO
UNECE
EU Commission
21434
24089
R155
R156
R157 - ALKS
GSR
EU L4 Regulation (2022/1426)
R155/156 Required by the EU L4
R155 Required by the AFGBV

The road to AV app



ISO 24089:2023

Road vehicles — Software update engineering

Abstract

This document specifies requirements and recommendations for software update engineering for road vehicles on both the organizational and the project level.

This document is applicable to road vehicles whose software can be updated.

The requirements and recommendations in this document apply to vehicles, vehicle systems, ECUs, infrastructure, and the assembly and deployment of software update packages after the initial development.

This document is applicable to organizations involved in software update engineering for road vehicles. Such organizations can include vehicle manufacturers, suppliers, and their subsidiaries or partners.

This document establishes a common understanding for communicating and managing activities and responsibilities among organizations and related parties.

The development of software for vehicle functions, except for software update engineering, is outside the scope of this document.

Finally, this document does not prescribe specific technologies or solutions for software update engineering.

General information

Status : ✓ Published	**Publication date** : 2023-02
Edition : 1	**Number of pages** : 24

Outlook

- Software-Defined Vehicle
  - less cables, less ECUs, less weight
  - High Performance Computer (HPC)
  - Adaptive AUTOSAR (virtualized)
- Data exchange with Cloud services
- Automotive Ethernet instead of CAN?
- Updates Over-the-Air + Firmware (FOTA)

References and further reading

- Socket CAN
  - https://docs.kernel.org/networking/can.html
- Can-utils
  - https://github.com/linux-can/can-utils
- CANalyzat0r
  - https://github.com/schutzwerk/CANalyzat0r
- Caring Caribou
  - https://github.com/CaringCaribou/caringcaribou
- Scapy CAN layer
  - https://scapy.readthedocs.io/en/latest/api/scapy.layers.can.html
- Raspberry Pi/PiCan 3 shield
  - https://buyzero.de/products/pican-3
- ICSim
  - https://github.com/zombieCraig/ICSim
- Automotive Security Research Group (ASRG)
  - https://asrg.io/

- Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S.: Experimental Security Analysis of a Modern Automobile. In: 2010 IEEE Symposium on Security and Privacy. pp. 447–462 (May 2010). https://doi.org/10.1109/SP.2010.34
- Antonioli, Daniele, and Mathias Payer. "On the Insecurity of Vehicles Against Protocol-Level Bluetooth Threats." 2022 IEEE Security and Privacy Workshops (SPW). IEEE, 2022.
- Dr. Charlie Miller and Chris Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. DEF CON 23 Hacking Conference. Las Vegas, NV: DEF CON. Aug. 2015.
- Florian Sommer, Jürgen Dürrwang, and Reiner Kriesten. “Survey and Classification of Automotive Security Attacks”. In: Information 10.4 (Apr. 2019), p. 148. ISSN: 2078-2489. DOI: 10.3390/info10040148. URL: http://dx.doi.org/10.3390/info10040148.
- ISO Central Secretary: Road vehicles – Unified diagnostic services (UDS) – Part 3: Unified diagnostic services on CAN implementation (UDSonCAN). Standard ISO 14229-3:2012, International Organization for Standardization, Geneva, CH (2012), https://www.iso.org/standard/55284.html
- Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T.: Comprehensive Experimental Analyses of Automotive Attack Surfaces. In: Proceedings of the 20th USENIX Conference on Security. pp. 1–6. SEC’11, USENIX Association, USA (2011)

Reinhard Kugler

MATRIS Applied Research Consulting

SBA Research

Floragasse 7, 1040 Vienna

rkugler@sba-research.org

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