From speedometer fraud to cyber security

ADAC Initiative gegen Tacho-Betrug

2.11.2023

Arnulf Volkmar Thiemel

Tacho fraud - the simplest form of inadequate IT security

Speedometer fraud was widespread long before IT was introduced in cars.

In the past, this form of fraud was carried out by twisting odometer rollers or using a drill. This required a sure instinct and usually left traces.

With the introduction of digital mileage displays, however, it has become child's play. Only the programmer, who writes a small program for each car that manipulates the mileage, needs to be skilled. Using specially (and exclusively) designed devices, on the other hand, is child's play.

The suppliers of speedometer manipulation devices have unwittingly become hacker pioneers. With almost every model, they easily overcome the often far too low hurdles that car manufacturers put in their way.

How widespread is speedometer fraud?

- "Munich method": Following a raid on over 100 used car dealers in 2011, the police compared the purchase contracts of the used cars (**low** price, high mileage) with the sales contracts (**higher price**, low mileage)
- On the basis of the confiscated documents, the police determined that one third of the Used car is manipulated
- Since Munich is the safest city in Germany according to crime statistics, the police assume that the manipulation rate in other cities is not significantly different (although precise figures can never be determined for this shadow economy)
- This means that **one third of used cars** in Germany **are manipulated** - that is **Two million vehicles** per year
- the illegal increase in value per car amounts to an average of **3000 euros** according to the Munich investigation results
- Total loss for German used car buyers per year: **six billion euros**
- **Figures are also confirmed by TÜV Rheinland (press conference on 22.10.2015), the CDU/CSU consumer protection commissioner Mechthild Heil, the AvD and others**

The devices are freely available

- produced in large quantities
- Very easy to operate

Photo: ADAC/Ralph Wagner

Manipulation usually within minutes via diagnostic socket

Photos: ADAC/Thiemel, Wagner

Regular updates for all new models (1/2)

Update Paket 10/2023

First in the World !

Jeep Wrangler Diag 2023 High Crypted version !

Chevrolet Cruze 93C56 2001-2006

Chrysler 300 RFHM Continental

Dodge Challenger RFHM Continental
Dodge Charger RFHM Continental
Dodge Durango RFHM Continental
Dodge Journey RFHM Continental

Fiat 500X RFHM Continental
Fiat Freemont RFHM Continental

Ford Kuga 2023 New Version
Ford Transit 2023 New Version

Geely Boyue 24CXX

The update lists are freely accessible

Source: www.dashcoder.com

Regular updates for all new models (2/2)

DiagProg diagnostic tester is an undisputed leader on the market. **DiagProg** users were the first who could program following car models:

News

2023-10-17

DIAGPROG4 – DIAGNOSTIC TESTER - UPDATE 2024 - NEW SOFTWARE: FORD, JEEP!!!

We would like to invite you to buy new software for:

Jeep Compass 2022 - M.Marelli with TFT 3.5" - programming/testing by diagnostic way (C22) and OBDII - Program number 385.
Ford EcoSport 2019 with R7F701403 - programming/testing via OBDII - Program number 352.

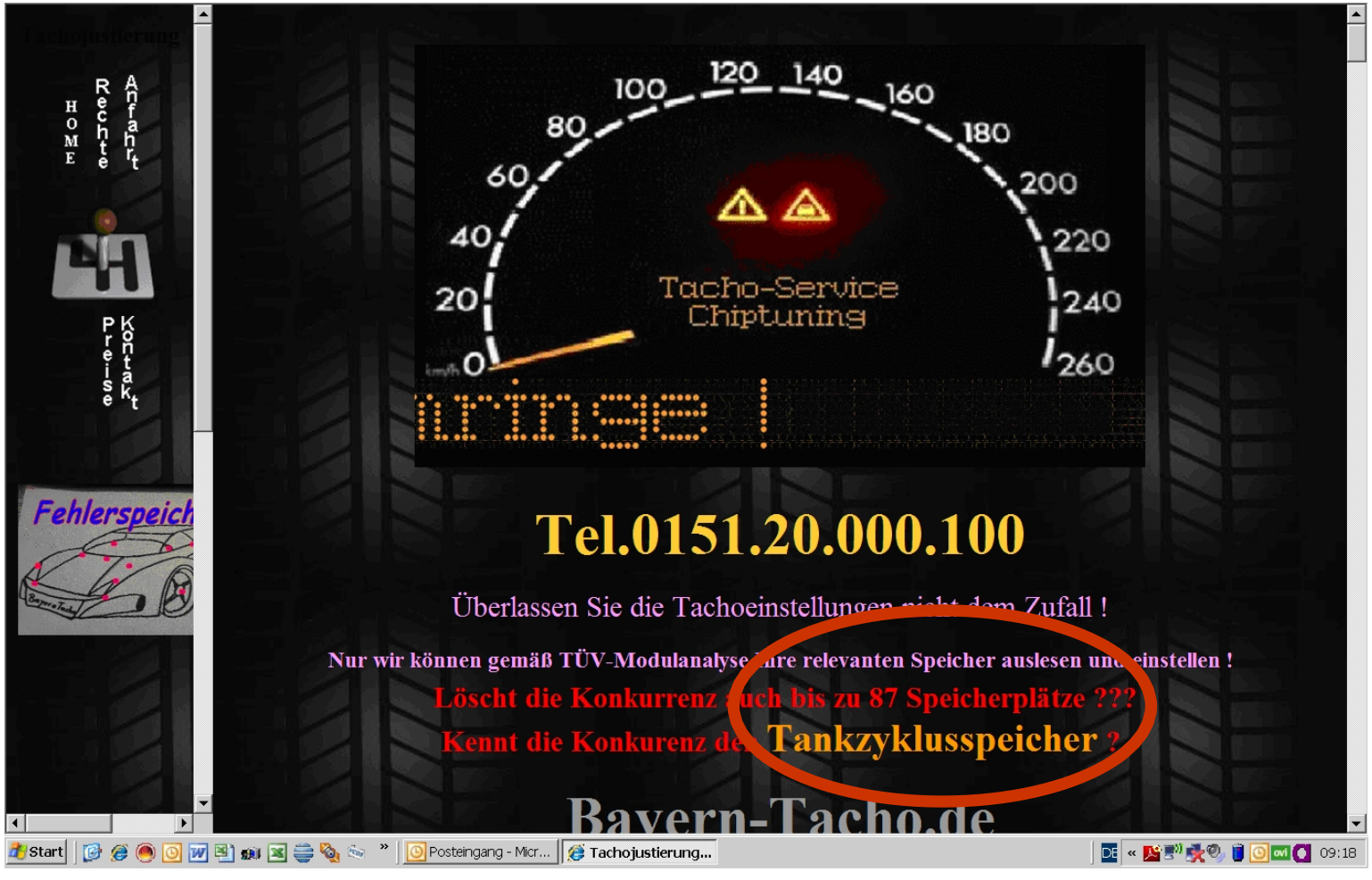
Source:
www.diagprog4.com

All relevant control units are manipulated (1/2)

- Mercedes-Benz E 200 CDI S212 / W212
  - inkl. Wartungsintervall, Zündschloss, Assyst, Assyst Plus, ESP Steuergerät, Sitzsteuergerät, Fehlerspeicher, ZGW Zentralgateway, CDI Injektorsteuergerät & Getriebesteuergerät, Batteriesteuergerät
- Mercedes-Benz E 200 S211 / W211
  - inkl. Wartungsintervall, Zündschloss, Assyst, Assyst Plus, ESP Steuergerät, Fehlerspeicher, ZGW Zentralgateway & Getriebesteuergerät
- Mercedes-Benz E 200 S212 / W212
  - inkl. Wartungsintervall, Zündschloss, Assyst, Assyst Plus, ESP Steuergerät, Sitzsteuergerät, Fehlerspeicher, ZGW Zentralgateway

Source: www.tachoteam.de

All relevant control units are manipulated (2/2)



Source: *www.bayern-tacho.de*

Manipulation devices from 150 euros free delivery

The fully functional China copies are easy to use

Source: www.carsets.co.uk

"Tacho-adjustment" will continue to be offered openly

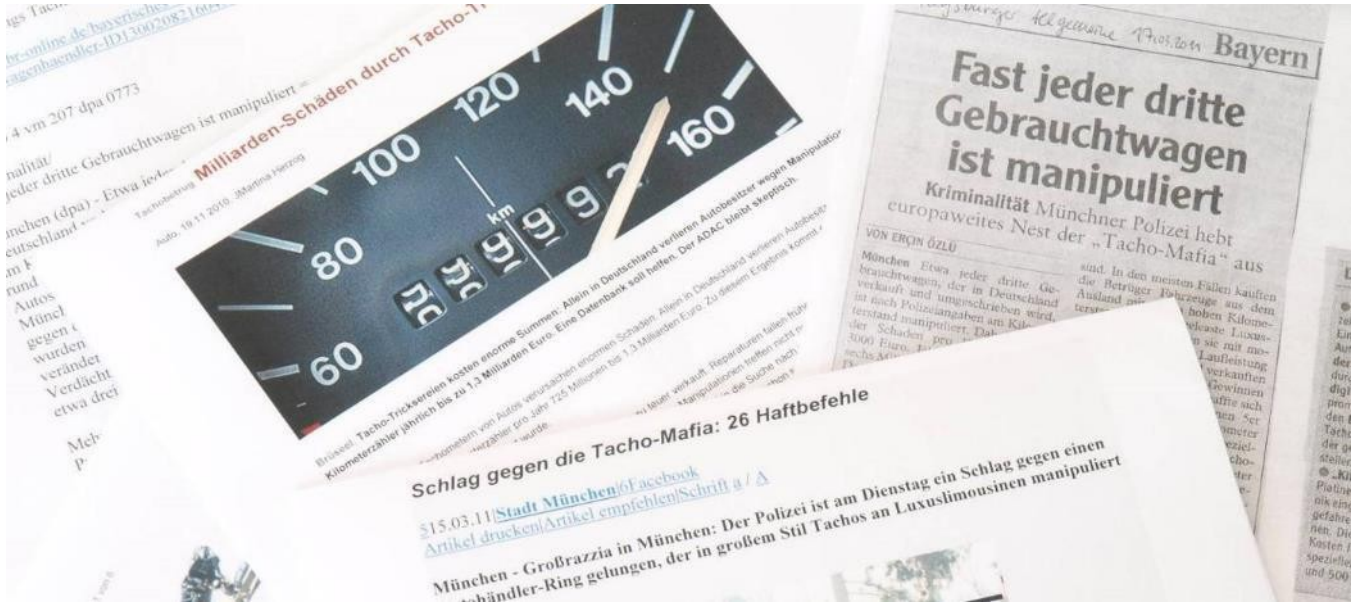
"All storage in one vehicle" - "...stands up to the Carly test"

Source: www.tacho-programmierung.de

The victim is the used car buyer

- Vehicle manufacturers suffer no damage from speedometer fraud
- Insurers are not measurably affected
- Lessors can pass on the damage

What has the ADAC done about it so far? (1/5)



- Raid in Munich in March 2011: 500 police officers search over 100 used car dealers, confiscate files and 300 cars; approx. 200 arrests; last court proceedings ended in 2015
- The ADAC Technical Center provided the police with specialist information a year in advance - and reported exclusively on the raid in ADAC Motorwelt

What has the ADAC done about it so far? (2/5)

- Warning the public - through over 200 publications on the Internet, press, TV and radio to date
- ADAC press conference 10/2013 with over 120 million media contacts - the most successful ADAC press conference to date
- Foundation of the "ADAC initiative against speedometer fraud" with expert hearings

- Intensive consultation with political decision-makers at national and EU level
- Formulation of a concrete proposal (R39) on how the odometer and its modern safeguarding could be described in the international type approval - where it is not yet represented at all

UNECE-type-approval for the distance counter (3/5)

- Anchor distance counter (odometer) as well as speedometer in the UNECE-type-approval

  Advantage: applies to all manufacturers, no unequal treatment due to national or EU regulations

- Tamper protection is also described in the UNECE type-approval (see FIA proposal for R39)

  Advantage: <u>one</u> regulation for technology and protection

- Application of Common Criteria for verifiable, modern protection against manipulation; already proven in other areas (e.g. SmartMeter for household power supply)

  Advantage: low adaptation effort, numerous internationally available test centers such as the Federal Office for Information Security (BSI) in Bonn

ADAC Initiative gegen Tacho-Betrug

UNECE-type-approval for the distance counter (4/5)

- If the odometer is part of the UNECE type-approval, only one additional verification point is required for type-approval - in addition to the already known points from exhaust gas to lighting

  Advantage: Processes remain uncomplicated

- Practical limits of the security system

  Advantage: rest of the vehicle can be changed without compromising tamper protection

- Procedure description and evaluation methodology available free of charge at www.commoncriteriaportal.org (internationally recognized under ISO standards 15408 and 18045)

  Advantage: no additional costs, no additional effort

ADAC Initiative gegen Tacho-Betrug

UNECE-type-approval for the distance counter (5/5)

- protection profile to describe the risks to be covered can be developed jointly by OEMs and ADAC

  Advantage: practical relevance, shared effort

- Technology (hardware and key databases) is already available from suppliers such as Freescale, Infineon, Renesas, etc.

  Advantage: low additional costs

Photos: Freescale, Infineon

- Certification of the odometer has a lighthouse function

  Advantage: good practice for future security applications such as Car2X, autonomous driving, etc.

- "A little more effort for in-house security is still cheaper than the damage to our image caused by security problems becoming public knowledge"

Milestone: new EU regulation from June 1, 2017

II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

VERORDNUNG (EU) 2017/1151 DER KOMMISSION

vom 1. Juni 2017

zur Ergänzung der Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Fahrzeugreparatur- und -wartungsinformationen, zur Änderung der Richtlinie 2007/46/EG des Europäischen Parlaments und des Rates, der Verordnung (EG) Nr. 692/2008 der Kommission sowie der Verordnung (EU) Nr. 1230/2012 der Kommission und zur Aufhebung der Verordnung (EG) Nr. 692/2008 der Kommission

(Text von Bedeutung für den EWR)

Important new content comparable to ADAC recommendations

3. „Kilometerzähler“ den Teil der Kilometerzählerausrüstung, der dem Fahrer die vom Fahrzeug seit seiner Inbetriebnahme erfasste Gesamtstrecke anzeigt;

f) eine Beschreibung der getroffenen Maßnahmen zur Verhinderung eines unbefugten Eingriffs oder einer Veränderung am Emissionsüberwachungsrechner und dem Kilometerzähler einschließlich der Aufzeichnung der Werte des Kilometerstands für die Zwecke der Anhänge XI und XVI;

3. Die Maßnahmen zur Gewährleistung der Übereinstimmung in Betrieb befindlicher Fahrzeuge sind während eines Zeitraums von bis zu fünf Jahren oder bis zu einer Laufleistung von 100 000 km zu kontrollieren; es gilt der Wert, der zuerst erreicht wird.

2.3.3. Die Hersteller müssen wirkungsvolle Maßnahmen im Fahrzeugnetz vorsehen, um die Fälschung des Kilometerstands in der Steuerung des Antriebsstrangs sowie in der Übertragungseinheit für den Datenfernaustausch (falls vorhanden) zu verhindern. Die Hersteller müssen systematische Techniken zum Schutz gegen unbefugte Benutzung sowie Schreibschutzvorrichtungen anwenden, die die Integrität des Kilometerstands sichern. Die Genehmigungsbehörde genehmigt Verfahren, die einen ausreichenden Schutz gegen unbefugte Benutzung bieten.

Thus must:

- Concrete protective measures are described
- measures are checked over five years/100,000 kilometers
- **systematic techniques and approved procedures** are used

A proven systematic method

Möchte eine Organisation den Nachweis erbringen, dass sie definierte Sicherheitsstandards erfüllt, bietet sich eine Zertifizierung an. Der folgende Überblick zeigt die Ausrichtungen der verschiedenen Verfahren auf. Dabei werden auch bekannte Standards erwähnt, nach denen keine offizielle Zertifizierung möglich ist, da es hier immer wieder zu Missverständnissen kommt.

Zertifizierung nach Common Criteria (ISO/IEC 15408)

Die Common Criteria (CC) sind ein international anerkannter Standard zur Zertifizierung von Hardware- oder Software-Produkten. Ziel ist der Nachweis, dass die Sicherheitsanforderungen eines IT-Produktes oder IT-Systems vollständig und korrekt realisiert worden sind. Insbesondere wird nachgewiesen, dass die Sicherheitsfunktionen nicht durch Schwachstellen umgehbar sind. Der Aufwand der Prüfung – und daraus resultierend das Vertrauen in die Wirksamkeit der Sicherheitsleistungen des zertifizierten Produktes – hängt von der Prüftiefe ab. Die CC unterscheiden sieben Stufen (EAL-Stufen 1 bis 7), die sich am angenommenen Täterprofil, der Motivation des Täters, dessen Know-how und dem erforderlichen Zeit- und Ausstattungsaufwand zur Durchführung eines Angriffes orientieren.

Common Criteria - systematic review

Studie: IT-Sicherheit auf Basis der Common Criteria – ein Leitfaden

Von Dr. Markus Mackenbrock, BSI

Die Common Criteria (CC) [1] sind nicht nur ein Kriterienkatalog für die systematische Evaluation, sondern bieten auch IT-Herstellern und -Anwendern einen Überblick über mögliche Sicherheitsmaßnahmen in IT-Produkten. Die CC beschreiben derzeit gängige Sicherheitsanforderungen, die durch Sicherheitsfunktionen umgesetzt werden sollen. Über Struktur und Gliederung dieser Sicherheitsfunktionen gibt der Leitfaden Auskunft.

Common Criteria offers:

- Recognized risk assessment and systematic evaluation by independent third parties
- international standard: ISO 15408 - free of charge and almost identical in text at www.commoncriteriaportal.org
- Technology-neutral (no technical implementation specifications for manufacturers)
- Certification body in Germany: BSI (Federal Office for Information Security, Bonn; subordinate to the Ministry of the Interior)

Databases are not a solution (1/3)

Mileage databases are often offered as a quick solution, in which the vehicle's current mileage is entered when the vehicle is visited at the garage or undergoes a general inspection. This is supposed to make the mileage of a car traceable. In reality, however, databases ...

unsafe - as odometer readings cannot be technically checked for accuracy before entry. This means that it remains hidden if the vehicle has already been tampered with beforehand.

The data is incomplete - as many databases only start with the first main inspection (vehicle age: three years). At this point, leased vehicles in particular are often already tampered with.

Databases are not a solution (2/3)

expensive - each retrieval of a mileage reading costs money (around ten to 20 euros), and garages and other reporting bodies must first pay fees before they are allowed to make entries. Ultimately, these costs are passed on to the consumer. In contrast, the modern technical backup of the mileage in the car would be significantly cheaper - around one euro per vehicle.

Databases are not a solution (3/3)

promote crime - an increasing spread of mileage databases will lead to even more systematic manipulation of mileage readings: either via the cheaply available manipulation devices or via the increasingly widespread OBD dongles (for plugging into the car's diagnostic socket). It is to be expected that suitable apps will soon be available for smartphones, which will then enable speedometer manipulation at the touch of a finger.

EU legislation has also recognized this - and has therefore opted for a "systematic Protection of the odometer reading in the car" (see previous slides)

Speedometer fraud despite database - practical example

RDW

NAP Nationale Auto Pas

VDS AUTO EXPORT SERVICES B.V.
HEEREWEGH 28
2731 BM BENTHUIZEN

Tellerrapport

Kenteken	Merk/Model/Uitvoering	Huidige tellerstand
04-XVP-8	BMW 3ER REIHE	Stand nu 129.520 km
		GEEN OORDEEL *

1e afgifte datum kentekenbewijs in Nederland	Bouwjaar	Rapportnummer
21-08-2012	2008	0000979672

Datum	Tellerstand	Datum	Tellerstand	Datum	Tellerstand
06-01-2015	129.520				
03-10-2014	129.520				
02-10-2014	129.520				
13-09-2014	129.502				
31-07-2014	118.487				
28-08-2013	83.097				
27-08-2012	46.213				

Toelichting

De RDW registreert vanaf 1 januari 2014 tellerstanden van personenauto's en lichte bedrijfswagens en houdt toezicht op de betrouwbaarheid van deze metingen. De RDW heeft de metingen van vóór 1 januari 2014 overgenomen uit de registratie van de Stichting Nationale Auto Pas (NAP). U kunt geen rechten ontlenen aan de gegevens op dit rapport voor zover deze betrekking hebben op metingen van vóór 1 januari 2014.

*** Geen oordeel**

De RDW geeft geen oordeel over de reeks tellerstanden van dit voertuig. Dit kan twee oorzaken hebben: dit voertuig is buiten Nederland geregistreerd geweest, of aan dit voertuig is iets gewijzigd waardoor het een ander kenteken heeft gekregen.

Postbus 30200
9640 RA Veendam

Telefoon 0900 0729 (€ 0,10 per minuut)

3 E 16758

A BMW 330xd is sold from Holland to Germany. According to the "Tellerrapport" (excerpt from the Dutch mileage database), it is just under 130,000 kilometers run. Shortly afterwards, the engine breaks down. A brand workshop sees in the repair history that the car already had over 180,000 kilometers on the clock almost three years ago. A short time later, it was sold to Holland with 140,000 kilometers less - and ran another 80,000 kilometers there. So at least 260,000 kilometers in total - twice as much as stated. And neatly recorded in the database - but with incorrect initial and final values.

ADAC has the latest manipulation devices

Manipulation devices worth 29,000 euros for investigations and media appointments (Photo: ADAC/Thiemel)

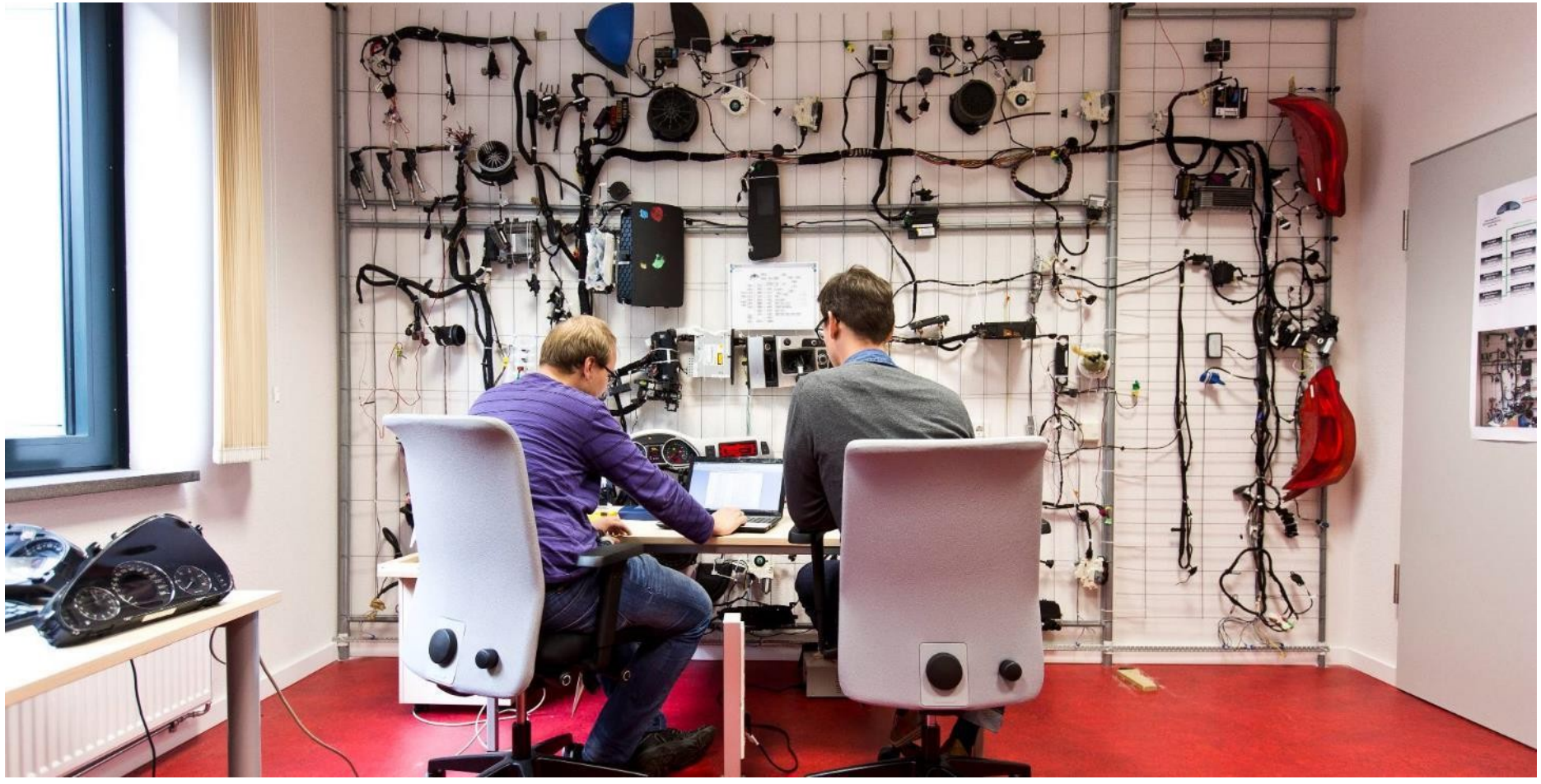
Study for FIA (Federation of European Automobile Clubs)

"No evidence was found that falsified mileage can be detected with speedometer manipulation devices. (...) Rather, the devices investigated are intended exclusively for the modification of odometer counters in vehicle control units." (Photo: ADAC/Thiemel)

ADAC commission: Study "Tacho fraud prepared ex works" ...

... with the "Multimedia and Security" working group at the University of Magdeburg (2012) (Photos: ADAC/Nils Hendrik Müller)

The scientists' analysis (1)



Researchers in the examination room with vehicle electronics

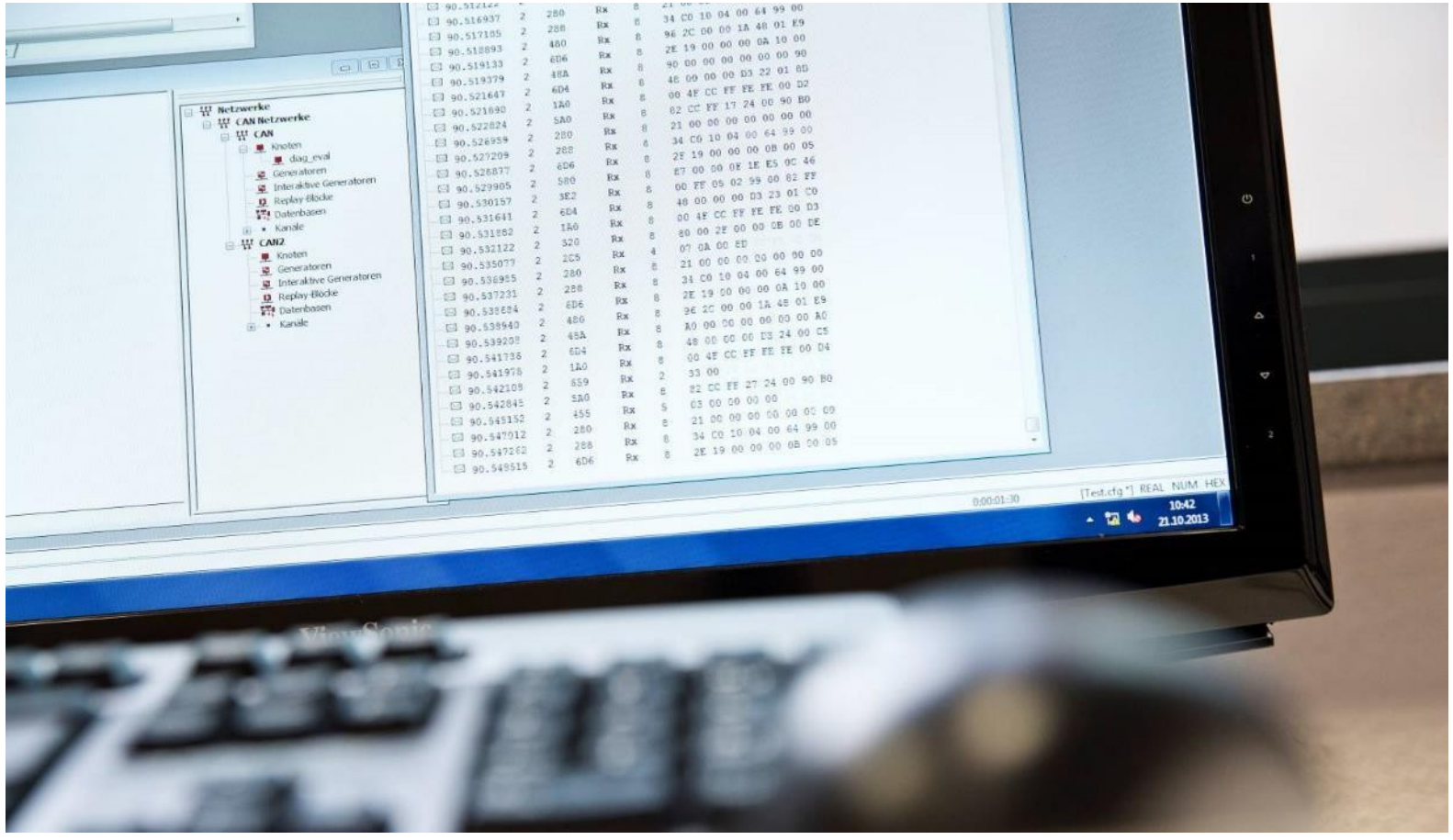
The scientists' analysis (2)

Recording of electrical signals between manipulation device and car with *"CANcaseXL"* etc.

The scientists' analysis (3)

Various manipulation devices were used, such as this Chinese copy of the *Digiprog III*

The scientists' analysis (4)



Analysis of the data with automotive tools such as *Vector CANoe*

Results

- Many cars are prepared for speedometer fraud ex works
- Specific commands for manipulating the mileage were anchored in the speedometers
- This is intended to "delete" longer test drives in the factory
- Speedometers mistakenly sent in as defective can be sold again as spare parts
- better protection would be available for **one euro** per car
- Suitable technology (Secure Hardware Extension/SHE and Hardware Secure Modules/HSM) is already installed, but is not used to protect against speedometer fraud (but only against theft and chip tuning - i.e. areas that cause direct damage to manufacturers)
- According to the police, the economic damage caused by speedometer fraud amounts to around six billion euros per year. In contrast, it would only cost around three million euros to effectively protect all new cars sold in Germany against fraud

Why speedometer fraud is not reliably recognizable (1/5)

Wear classification of

- Pedal rubbers
- Steering wheel
- Seat edges
- floor coverings

is **not** meaningful. Because today

- Almost all used cars professionally reconditioned
- Pedal rubbers replaced as standard
- Steering wheels coated with leather, seat covers upgraded

Why speedometer fraud is not reliably recognizable (2/5)

Mechanical traces

- Almost all vehicles can be manipulated via the diagnostic socket (OBD)
- In most cases, it is no longer necessary to remove speedometers or control units
- mechanical traces no longer occur in most cases

Electronic tracks

- does not exist with "professional" manipulation, not even recognizable for OBD dongles - see video at https://www.tachojustierung.org/justierung-saemtlicher-speicherstellen/ and https://www.tachoprogrammierung.de/ in the middle of the page under the heading "Speedometer adjustment at the market leader" - there **"MyCarly test"**
- cannot be detected with the means of a workshop or vehicle expert

Why speedometer fraud is not reliably recognizable (3/5)

Analysis of the control units

- the required "layers" are not accessible with standard workshop diagnostic equipment (only from the manufacturer/supplier)

- Odometer readings are recorded by current manipulation devices in "up to 87 control units" (advertising from www.bayern-tacho.de) overwritten

- Fault memory entries, particulate filter regeneration data, operating hours counter, etc. are also manipulated

Why speedometer fraud is not reliably recognizable (4/5)

Ultrasonic analysis ("speedometer spy")

- Ultrasonic emission of the engine is to provide information about the mileage by comparison with a reference database
- ADAC cannot recommend the method in its current form. This is because there is as yet no evidence of the validity of the mileage readings for the reference vehicles. Furthermore, there is no information on whether the reference vehicles were measured at defined mileage intervals
  or how large the distances between the measured values are.
- Furthermore, the effects of different engine, body and equipment variants on the ultrasound image of a car have not yet been systematically taken into account

Why speedometer fraud is not reliably recognizable (5/5)

Odometer readings from

- Workshop invoices
- Service booklet
- Test reports from main investigations
- Fuel receipts (for leased vehicles)
- History entries in manufacturer workshops
- Mileage databases (e.g. car pass)

are not necessarily correct. This is because if the manipulation takes place before the first long-life service (after two years) and before the first main inspection, the incorrect values are also entered in the above-mentioned places

Goals of the ADAC initiative against speedometer fraud (1/4)

Up-to-date technical protection of the entire route

The cost of manipulation must be so high that it is no longer worthwhile in relation to the price increase of the used car.

This is to be achieved through EU type approval for each new vehicle model.

For example, through existing IT technology such as Hardware Secure Modules (HSM)

Photos: Freescale, Infineon

Goals of the ADAC initiative against speedometer fraud (2/4)

neutral proof of the effectiveness of this protection

In other safety-critical electronics sectors, this is successfully achieved through certification, for example, with the cooperation of the German Federal Office for Information Security (BSI)

The number of vehicle thefts shows that adequate electronic protection is possible: Thanks to modern electronics (immobilizer), the number has fallen over many years to just under 20,000 per year in Germany today. In contrast, there are a hundred times as many cases of speedometer fraud.

Goals of the ADAC initiative against speedometer fraud (3/4)

No safety gaps when replacing defective speedometers

In replacement speedometers, the actual mileage of the car may no longer be adjustable. They should start counting from zero. The speedometer replacement must be noted in the vehicle documents together with the mileage of the car at the time of replacement.

The installation of a new speedometer is rarely necessary nowadays, as speedometer defects are extremely rare and there are repair offers for many types of damage that are in line with the current value of the vehicle, which can save the consumer money compared to a new speedometer.

Goals of the ADAC initiative against speedometer fraud (4/4)

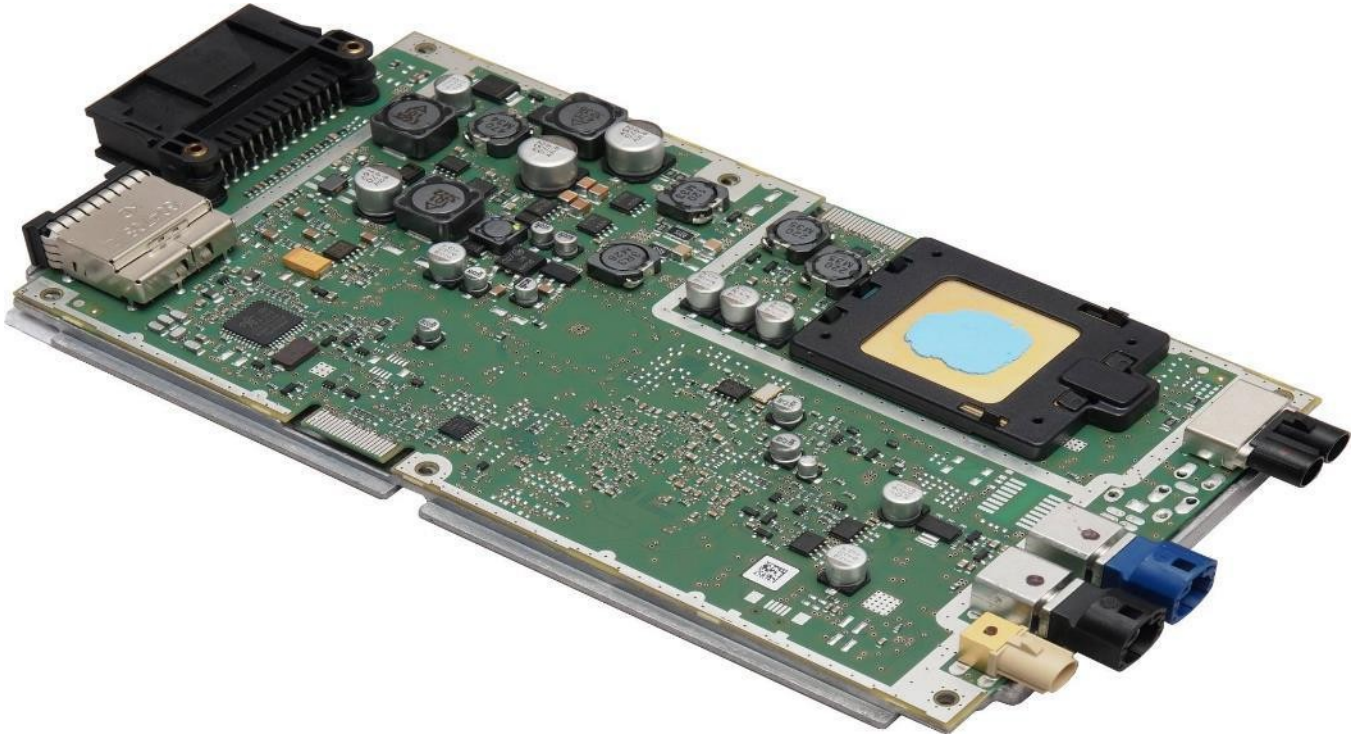
No hidden "back doors" in the control unit software

Some suppliers use these so-called "backdoors" to recondition speedometers and sell them as spare parts. Vehicle manufacturers are also suspected of using this method to carry out more detailed test drives at the factory.
to "push away".

Data in the car

2.11.2023 Arnulf Volkmar Thiemel, ADAC

Data in the car



Today, even a Golf-class car can have up to 70 control units.

These collect, process, store and send information (data).

Below are the different layers and who has access to them and how.
Photo: ADAC/Thiemel

Where can data be read out? - ADAC layer model (1/6)

1. Shift:

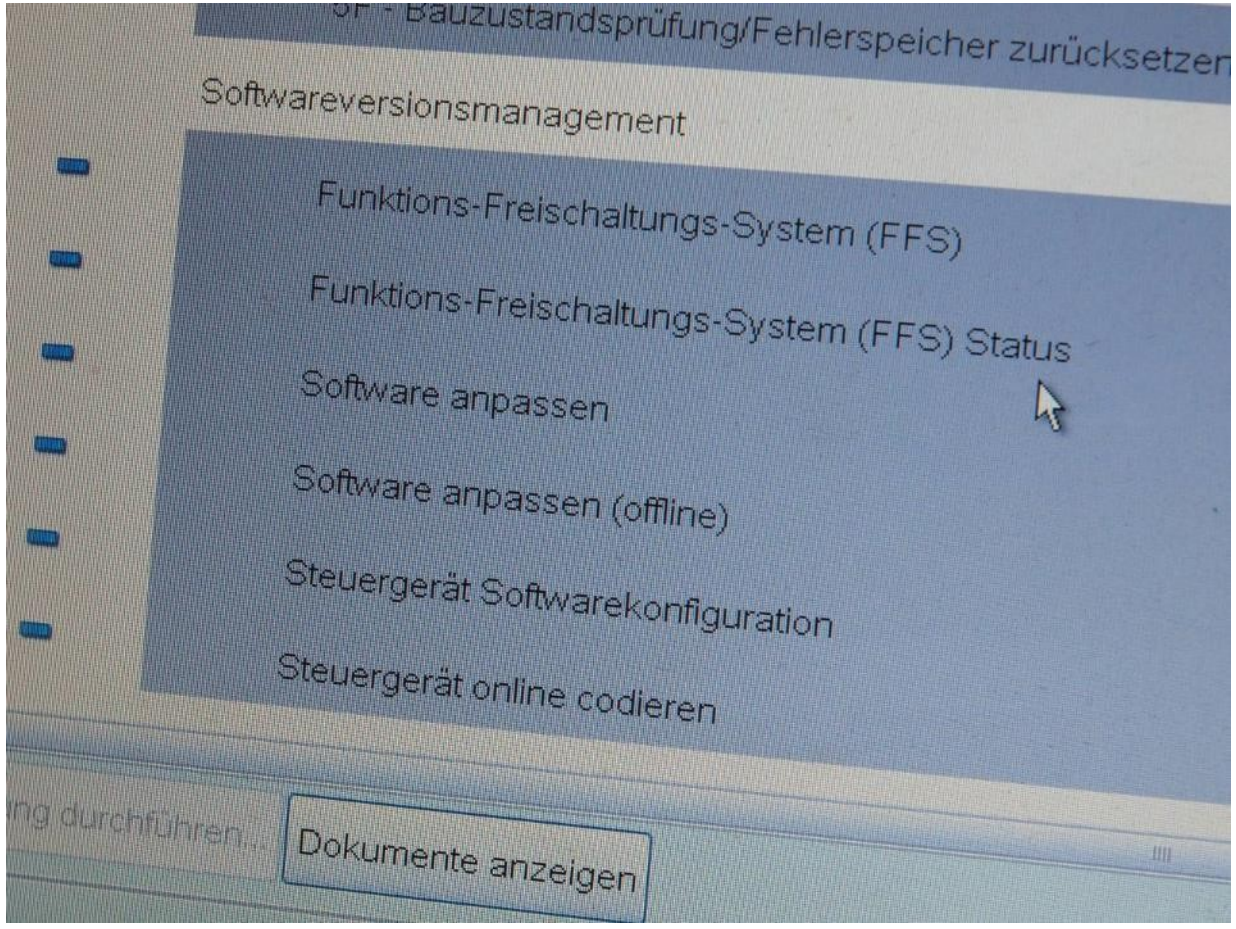
OBD standard since 2001 (diesel from 2004; only emissions-related information; standardized codes across manufacturers), readout with simple
"Aldi appliances"
Photos: ADAC/Thiemel

Where can data be read out? - ADAC layer model (2/6)

2. Shift:

Accessible for free multi-brand diagnostic devices (more control units accessible, in some cases configuration of control units also possible - number of brands and models dependent
from the knowledge of the diagnostic manufacturer) *Photos: ADAC/Thiemel*

Where can data be read out? - ADAC layer model (3/6)



3. Shift:

accessible for diagnostic devices in manufacturer workshops (with Online connection to the manufacturer - e.g. for key duplication or for programming control units that are specially protected against theft)

Photos: ADAC/ Thiemel

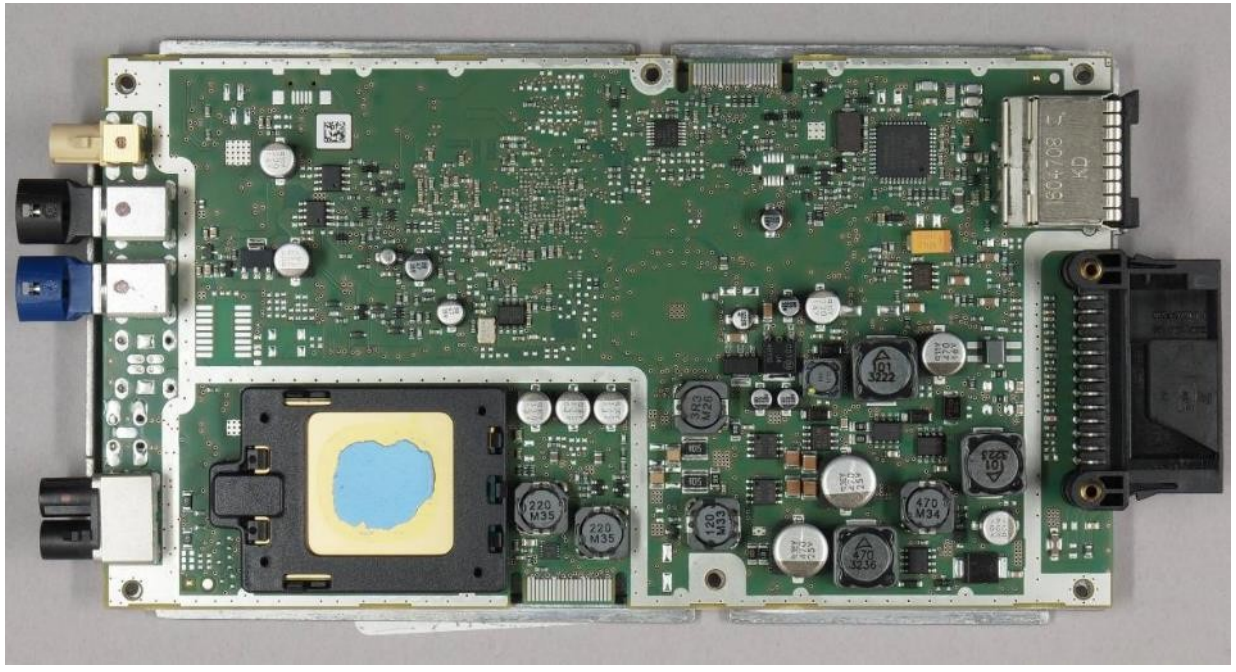
Where can data be read out? - ADAC layer model (4/6)

4. Layer

Accessible to the manufacturer's development department (e.g. storage of environmental conditions - e.g. for findings in the event of warranty or recourse claims against suppliers)

Photos: ADAC/ Thiemel

Where can data be read out? - ADAC layer model (5/6)



5. Layer

Suppliers (e.g. to defend against recourse claims by the vehicle manufacturer or for accident reconstruction)

Photos: ADAC/

Thiemel

Where can data be read out?
ADAC shift model (6/6) Summary

OBD standard (only emissions-related information; cross-manufacturer codes)

Free multi-brand diagnostic devices (more control units accessible, configuration possible - number of brands and models depends on the diagnostic device manufacturer)

Diagnostic devices in manufacturer workshops (with online functions - e.g. for replacing control units with Theft protection or key reordering)

Manufacturer development department (e.g. with memories for certain events, e.g. environmental conditions for airbag deployment)

Suppliers (e.g. to provide evidence of improper use of the control unit by the manufacturer)

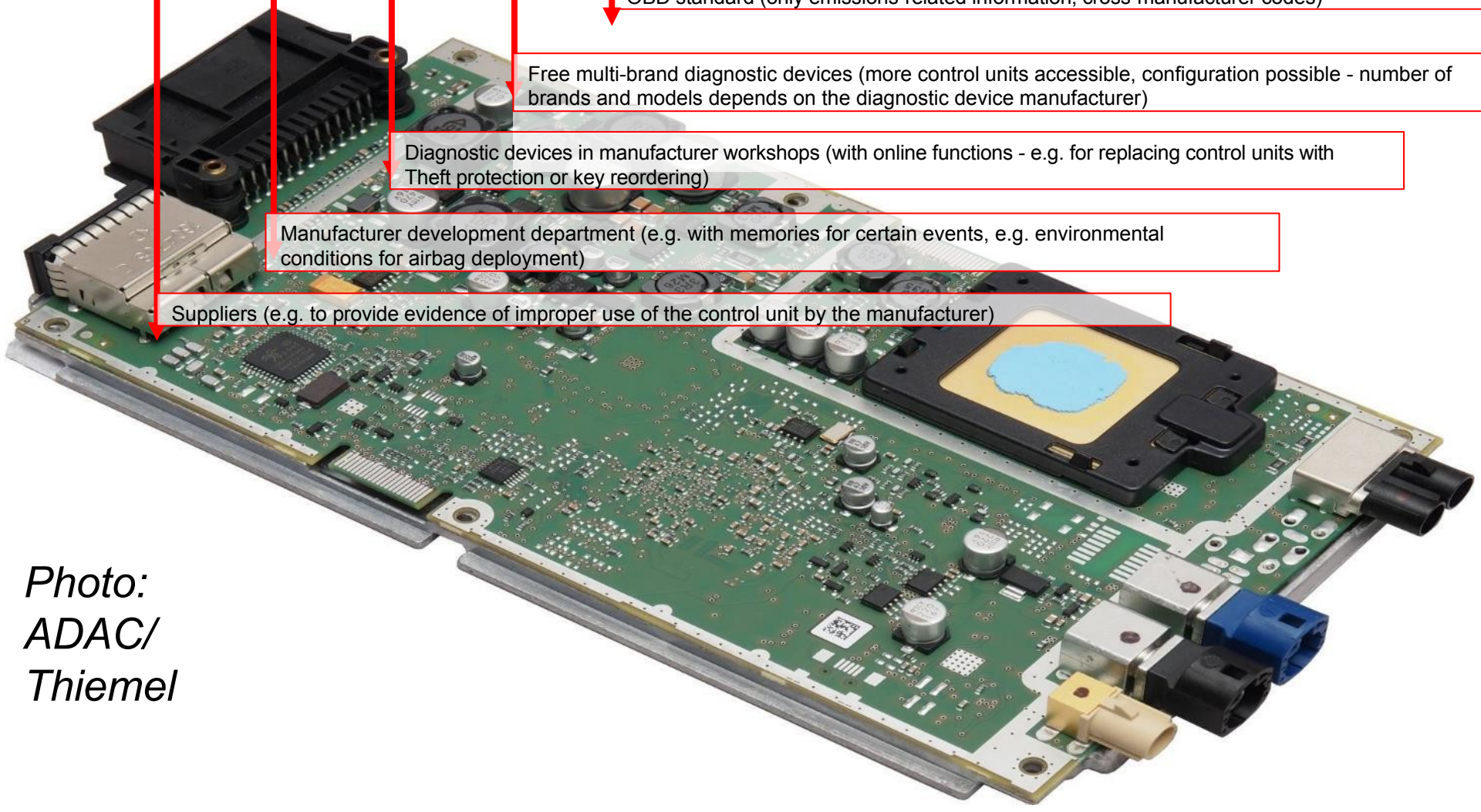


Photo: ADAC/ Thiemel

Data in the car

- many media inquiries on the subject for years
  "What data does a car generate, store and send?"

- hardly any proven information available in the public domain

- only manufacturers and suppliers know, but do not provide any information

Backgrounds

- Each car manufacturer uses its own "data language" in the electronics, for which there are
  but there is no "dictionary" or similar

- "Data language" has to be "learned" at great expense through reverse engineering; previously

This is too expensive even for investigative publications such as "Der Spiegel" and "Stern"

750 billion dollars ...

can be realized with data from vehicles by 2030 - says a recent McKinsey study.

This data is the "gold of the present". Even renowned car manufacturers are well aware that only in the past were they indispensable thanks to their engine lines and body pressing plants. Today they are no longer.

A company like Apple has now had over a billion high-tech iPhones built in China - a once developing country.
If Apple or Google also want to manufacture cars in the future, they don't necessarily need the renowned manufacturers. They will either set up their own production facilities (see Tesla) or commission suppliers (e.g. Magna) or use existing (Asian) suppliers.

Only with the "gold of the present" ...

the existing car manufacturers can survive in the future. That is why they are doing everything they can to retain sole control over all the data from their cars. Even if they don't yet know in detail what they want to do with it.

Otherwise they will become interchangeable and sink into insignificance. The race has long since begun - without consumers really noticing it yet. There is a method to it.

It is no coincidence that the Volkswagen Group has set up its own software division, CARIAD, with thousands of IT engineers to develop its own operating system for the Group brands' cars.

ADAC survey "Data in the car" 2016 (1/5)

To gain an overview of the data generated, an expert needs around six months full time on a vehicle that was previously unknown to him. This is because he has to learn the manufacturer-specific protocol language - without manufacturer support. It's like learning a foreign language without a teacher and without a dictionary. The following have been examined so far:

- BMW 320d
- BMW i3 (partial)
- Mercedes B
- Renault Zoe

(Photos: ADAC)

ADAC survey "Data in the car" 2016 (2/5)

Five particularly illustrative examples of data from the **BMW 320d** under investigation:

- Maximum engine speed reached with the respective mileage (permitted conclusions about the driving style)
- Number of journeys between zero and five, five and 20, 20 and 100 and over 100 kilometers (allows conclusions to be drawn about the usage profile)
- Duration, how long the driver was driving in different modes of the automatic transmission (continuous/manual/sport) (allows conclusions to be drawn about the driving style)
- Number of adjustments of the electric driver's seat
- Number of electromotive belt tensions, e.g. due to heavy braking (allows

conclusions to be drawn about driving style)

ADAC study "Data in the car" (3/5)

This data is used, for example, in the **BMW i3** (electric car with range extender) **transmitted to the manufacturer via mobile radio every time the car is locked**:

- Position of the 16 previously used charging stations
- Contents of the fault memory
- Detailed traction battery data (state of charge, cell temperatures, etc.)
- Selected driving mode ECO/ECOPLUS/SPORT
- Application data of the gasoline-powered range extender (REX)
- How often was the charging plug plugged in, how and where was charging carried out (fast, partial, etc.), how much was the traction battery discharged beforehand?
- Odometer reading for various operations such as charging etc.
- Quality of the charging voltage, failures
- Around 100 last parking positions of the vehicle (only stored in the control unit)

ADAC survey "Data in the car" 2016 (4/5)

Examples of data found in a **Mercedes B-Class** with me-connect:

- The vehicle's GPS position and status data are transmitted to the Mercedes backend approximately every two minutes (e.g. mileage, fuel consumption, fuel level, tire pressure and levels of coolant, wiper fluid or brake fluid)
- The number of electromotive belt tightenings is saved, for example due to strong Braking (allows conclusions to be drawn about the driving style)
- Fault memory entries are sometimes stored with information about excessive engine speed or temperature (allows conclusions to be drawn about the driving style)
- kilometers driven on freeways, country roads and in the city ("highway-conditions", "road-conditions" and "urban-conditions") are stored separately
- Operating hours of the vehicle lighting are saved
- 100 charging and discharging cycles of the starter battery are stored with time and

date as well as mileage, resulting in driving and standing times

ADAC survey "Data in the car" 2016 (5/5)

Examples of data found on a **Renault Zoe** (electric car):

- Renault can prevent the traction battery from being charged via a mobile phone connection
  (e.g. if the leasing invoice for the traction battery has not been paid)
- Renault can use RemDiag to read any information from the vehicle's CAN data bus via a mobile phone connection. This remote diagnosis is switched off by default, but can be activated by the manufacturer at any time
- A data packet is sent to Renault every time the vehicle is driven, but at least every 30 minutes: VIN, various serial numbers, date, time, GPS position, temperature, charge and cell voltage of the high-voltage traction battery; this information can also be requested by Renault at any time
- In addition to the pre-programmed functions for communication between the Renault server and the Renault Zoe, these functions can be extended as

required via a mobile phone connection

Next steps

- A great deal of additional information has been discovered, the usefulness/necessity of which still needs to be discussed with the manufacturers, as neither experts nor the ADAC have any idea what it is intended for.

- Investigations by the ADAC and the FIA (umbrella organization of European automobile clubs) are continuing on cars from other manufacturers - including on remote apps that can be used to control vehicle functions remotely

- Here, too, the "language" of the respective manufacturer must first be learned each time - without a dictionary or teacher

ADAC demands on "data in the car"

- **Transparency:** Car manufacturers must publicly provide a list of all data collected, processed, stored and externally transmitted for each model ("car data list").

- **Free access:** The vehicle owner, independent workshops and roadside assistance personnel must have free read access to all data in the vehicle. Write operations must be reliably secured.

- **Data security:** Car manufacturers must be obliged to ensure data security. Neutral proof of this must be provided, for example in accordance with Common Criteria ISO/IEC 15408 - e.g. via the German Federal Office for Information Security (BSI).

- **Opt out:** With the exception of the legally prescribed use of data (e.g. eCall, exhaust gas control), the car owner must
can be
  easily switched off, unless absolutely necessary for operation.

Security gaps in 2.5 million BMW models

- At the beginning of 2015, the ADAC discovered security vulnerabilities that affected 2.2 million BMW, Mini and Rolls Royce vehicles.
- This meant that the cars could be opened from the outside in a matter of minutes by mobile phone after a one-off preparation, without leaving any traces. The ADAC emphasizes that it did not carry out a complete security check of BMW vehicles or even the entire company. There was no order for this and this is the responsibility of the respective manufacturer.
- Specifically, the most important security vulnerability was that the same electronic key was used for all vehicles to authorize remote opening; in addition, no encryption was used for data communication with the BMW server.
- In addition, the vehicle location was not anonymized when transmitted to the manufacturer and the data traffic could simply be redirected to a third-party server.

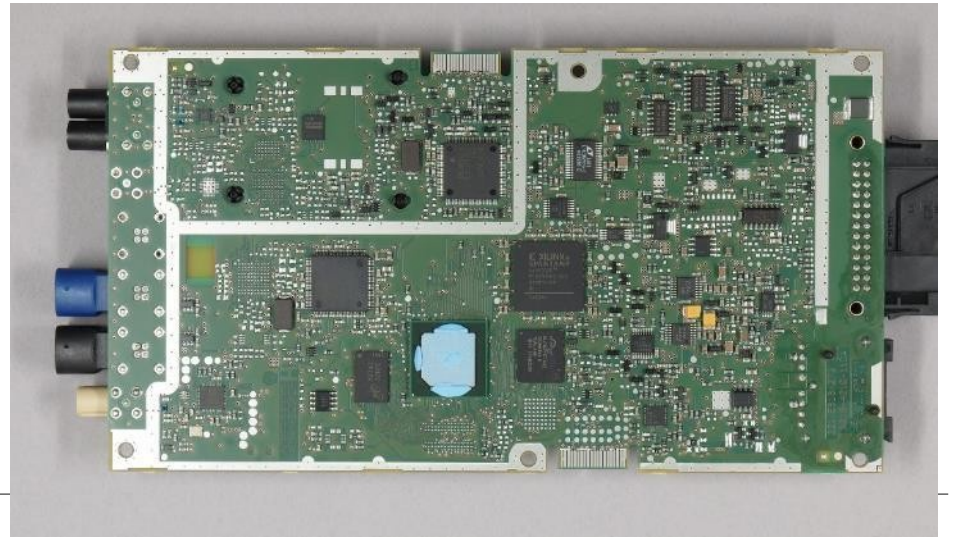


Photo: ADAC/Arnulf Thiemel

Cars with keyless locking systems are particularly easy to steal

2.11.2023 Arnulf Volkmar Thiemel, ADAC

How a keyless locking system works

- Car owner only needs to carry the key with them, no need to press a button
- As soon as he approaches his car, it recognizes the key by radio
- touching the door handle (or pressing a button) opens the central locking system
- Can usually also be started without an ignition key by pressing a button
- Keyless locking systems (called comfort keys at BMW) are widely used today

A whole series of thefts

- Series of over 100 car thefts in the Rhine-Main region in mid-2015
- Without exception, cars with keyless-go locking system affected
- Police find devices for the first time with which the car thieves have extended the radio connection between the key and the vehicle using simple technical means

How it works

Photo: ADAC/Thiemel

- Thief brings small device close to the original key (a few meters away; also works through walls)
- This "extends" the key radio signal and sends it to the second device (up to several hundred meters away) near the car
- The thief's helper can open the car and drive away

Video of a REAL keyless entry theft

The surveillance camera of an ADAC member recorded this **REAL** theft of a car with a keyless locking system:

Photo: Surveillance camera M. Brester

How it works

- With this method, there is no "hacking" of data or even encryption
- Simple range extender, similar to the CB radio amplifiers of the past
- The car runs without the key as long as there is fuel in the tank (or until the engine stalls or is switched off)
- Usually, the cars are driven abroad immediately after the theft and "disappear" there

Procedure of the ADAC

- ADAC has carried out its own tests: over 600 vehicles of many brands could be illegally opened and driven away
- Device for stealing keyless vehicles has been built
- all vehicles in the ADAC car test are examined, result noted in the test report

(Photo: ADAC/Thiemel)

- Numerous press releases to warn consumers
- Requirements for manufacturers (see also www.adac.de/keyless)

Aluminum foil is not helpful

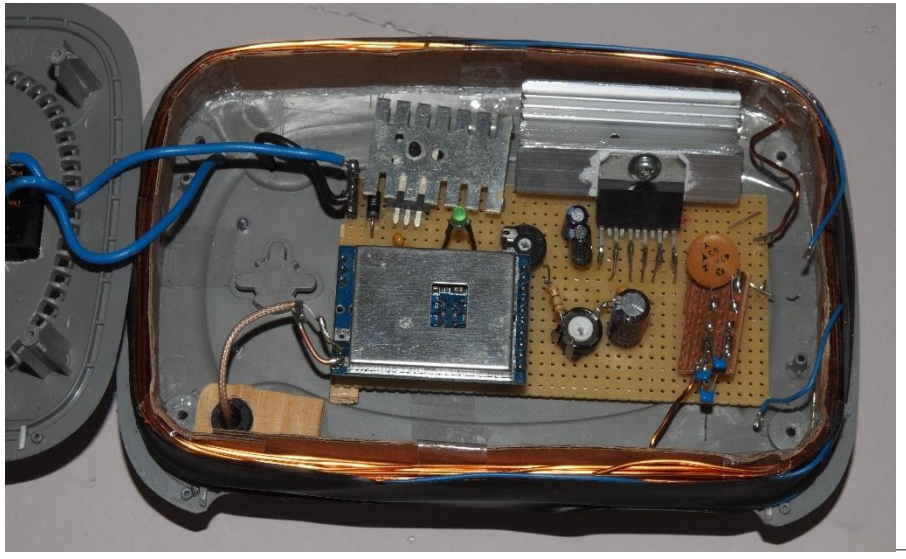
- Aluminum foil around the key or shielding key cases can prevent theft of keyless cars, but should not be recommended by the ADAC; because if a car is stolen anyway, the vehicle owner is "to blame"

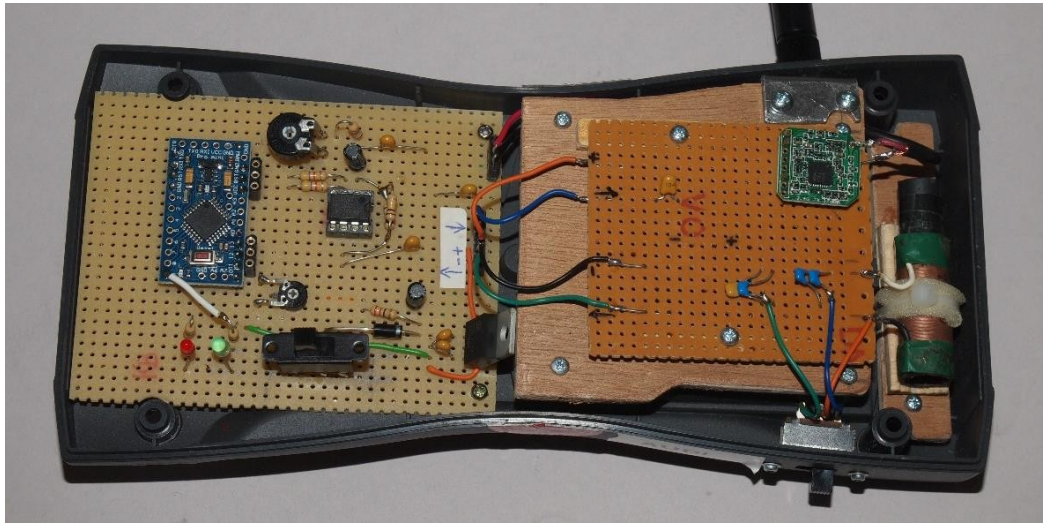
- In reality, however, car manufacturers have a duty: a more expensive locking system must not be significantly easier to crack than the standard wireless remote control

- Car owners affected by such a theft can quickly come under suspicion of committing insurance fraud - if their car is recovered and the police do not discover any classic signs of theft

Jaguar LandRover, Seat Leon and VW Golf 8 better secured (1)

Cars with keyless can be safer than before. This is demonstrated by the Jaguar and Land Rover models tested by the ADAC from model year 2018 - and now also Volkswagen Golf 8, Seat Leon and other models since 2019. They can neither be opened illegally nor driven away with the self-built radio extender that the ADAC has been using for over seven years. The ADAC devices do not contain a CPU!





Photos: ADAC/ Thiemel

Jaguar LandRover, Seat Leon and VW Golf 8 better secured (2)

These cars use computer chips with ultra-wideband (UWB) technology. These can determine the distance between the key and the car very precisely from the propagation time of the radio signals - and thus also detect a radio extension. If a radio extender is used, the car no longer responds. Other vehicle manufacturers are also called upon to make their keyless systems more secure.

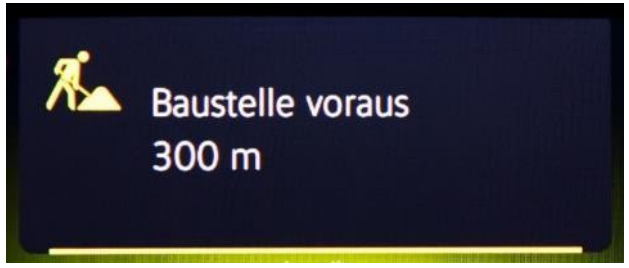
make. Ideally with a
neutral proof of the effectiveness of the
Anti-theft measures (e.g. according to Common Criteria, www.commoncriteria.org).

Photo: ADAC/Thiemel

C2X is a milestone like ABS and airbags

2.11.2023Arnulf Volkmar Thiemel, ADAC

How it works



Photos: ADAC/Ralph Wagner

- Car detects nearby hazards by radio
- Early warning in the instrument cluster (right-hand image), automatic braking if necessary
- For the first time, accidents can be completely avoided instead of having to go through costly

mitigate their consequences

The advantages of C2X

- standard in the Golf 8, ID.3 and many other new Volkswagen models as well as Cupra Born

- Warning of hazards detected by a car in front (e.g. ESP intervention on slippery roads, end of traffic jam) and of hazards that warn "themselves" (breakdown vehicle, fire department, roadworks sign, etc. with C2X on board)

Photo: ADAC/Ralph Wagner

- Mature and EU-standardized: intensively used by numerous manufacturers for 15 years tried and tested

- Can be extended to pedestrians, cyclists and other road users

The advantages of C2X

- pWLAN is standardized across manufacturers
- Later expansion of suitable use cases via 5G possible
- secure: first certifications per Common Criteria by the BSI

ADAC demand: all manufacturers should use standardized communication

Thank you for your attention!

Arnulf.Thiemel@tzll.adac.de