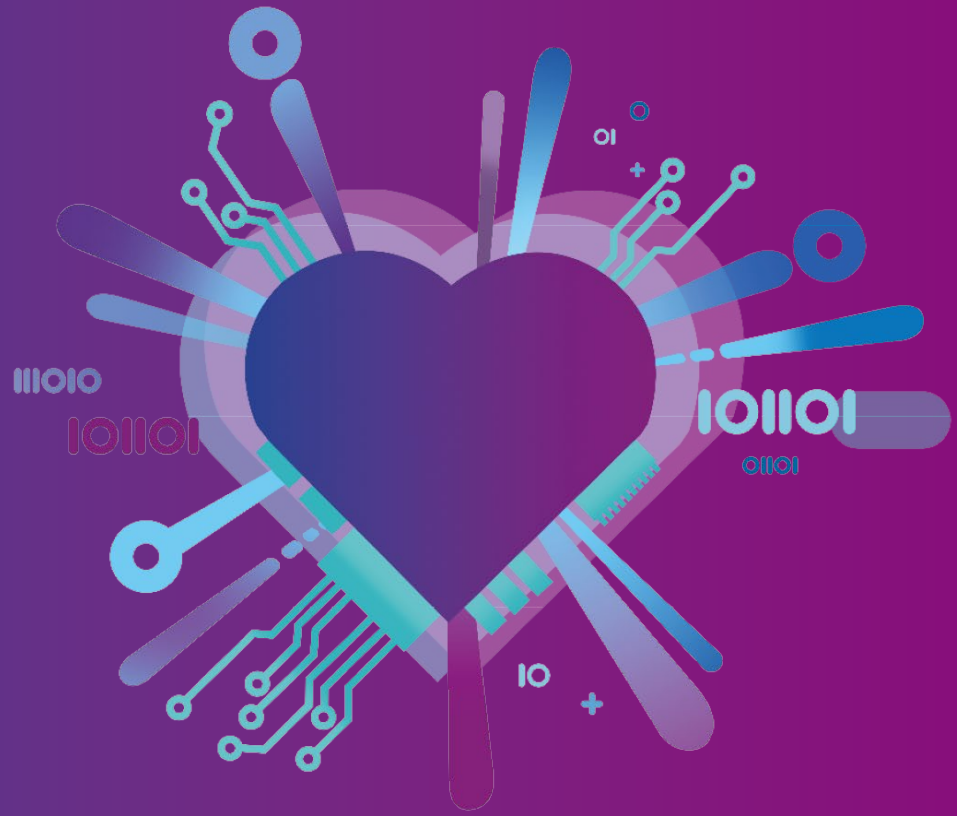
Securing your software on micro-controllers with **AUTOSAR** and beyond



Our heart beats **embedded.**

Securing your software on micro-controllers with AUTOSAR and beyond
Your speakers

George Bray

Product Manager for RTA-OS and
RTA-HVR – RTA Solutions
ETAS Ltd

- M.Eng. in Computer Science
- Joined ETAS in 2018
- Working with AUTOSAR Classic since 2020

Michael Schneider

Lead Technical Officer AUTOSAR Security
ETAS GmbH

- 8 years of experience in automotive cybersecurity
- Speaker of AUTOSAR WG-SEC, member of AUTOSAR since 2018
- Supporting our customers securing their products (ECUs, vehicles, applications, …)

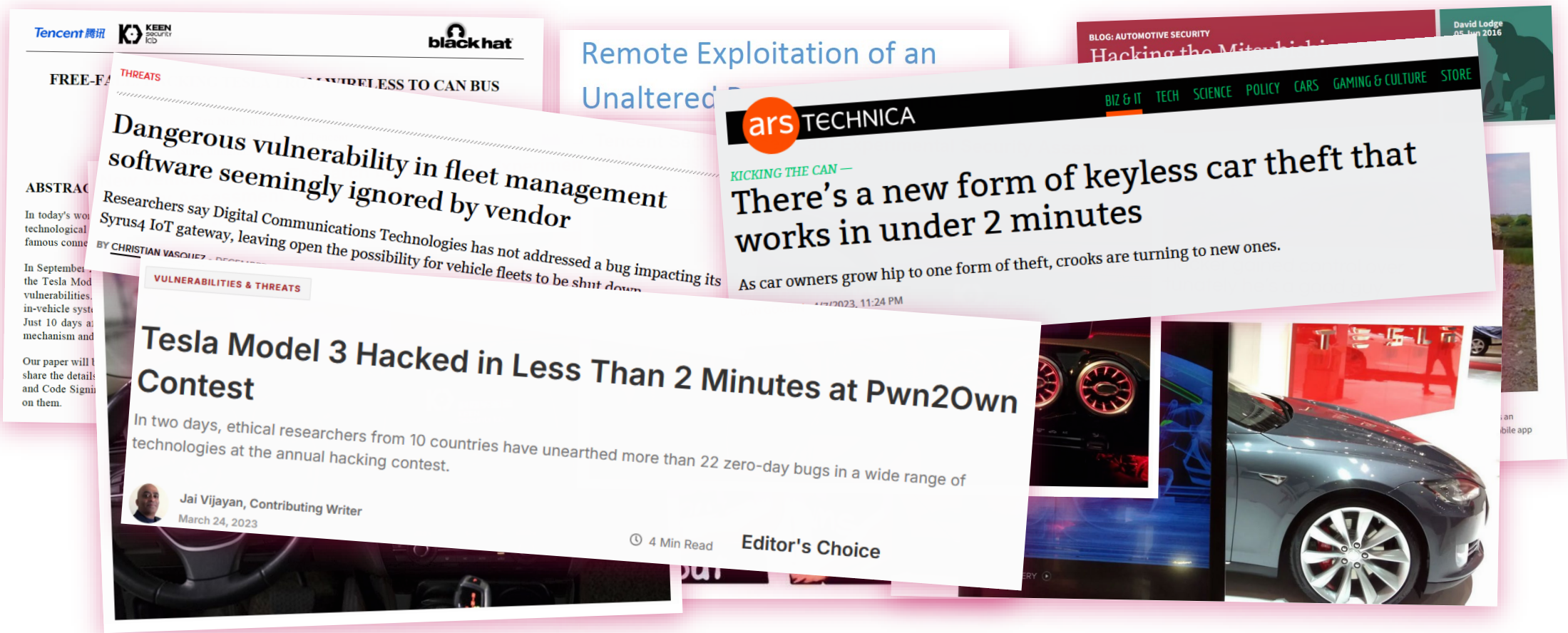
Security in automotive

Cybersecurity challenges

Cybersecurity risks: The evil is always there and everywhere

High complexity and connectivity are increasing the attack surface.
All connected endpoints and critical infrastructure of the ecosystem need to be protected.

Security in automotive

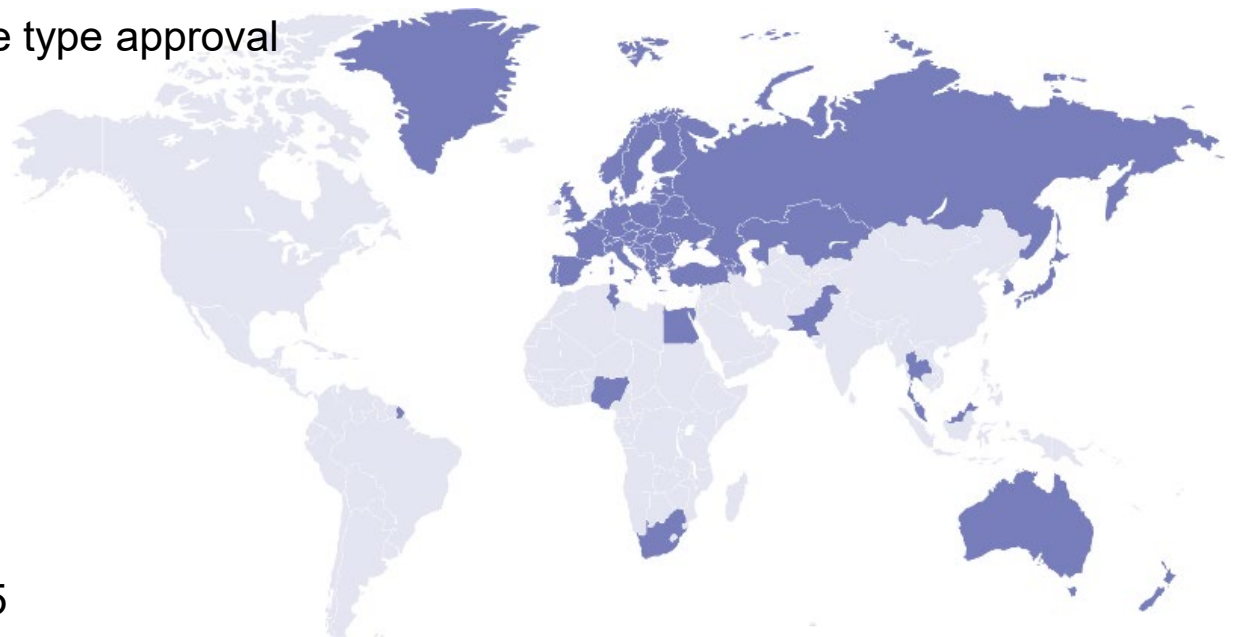


Security in automotive

Regulatory landscape

Cybersecurity **mandated by regulation** to get vehicle type approval
– UNECE R155: Europe, Japan, …
– GB 44495: China

Other regions rely on **cybersecurity guidelines**
– NHTSA Cybersecurity best practices: USA



Upcoming regulation:
EU Cybersecurity Resilience Act (CRA)

- Covers vehicles that are out-of-scope of UN R 155
- Applicable to two-wheelers, agricultural machines, off-road vehicles, …

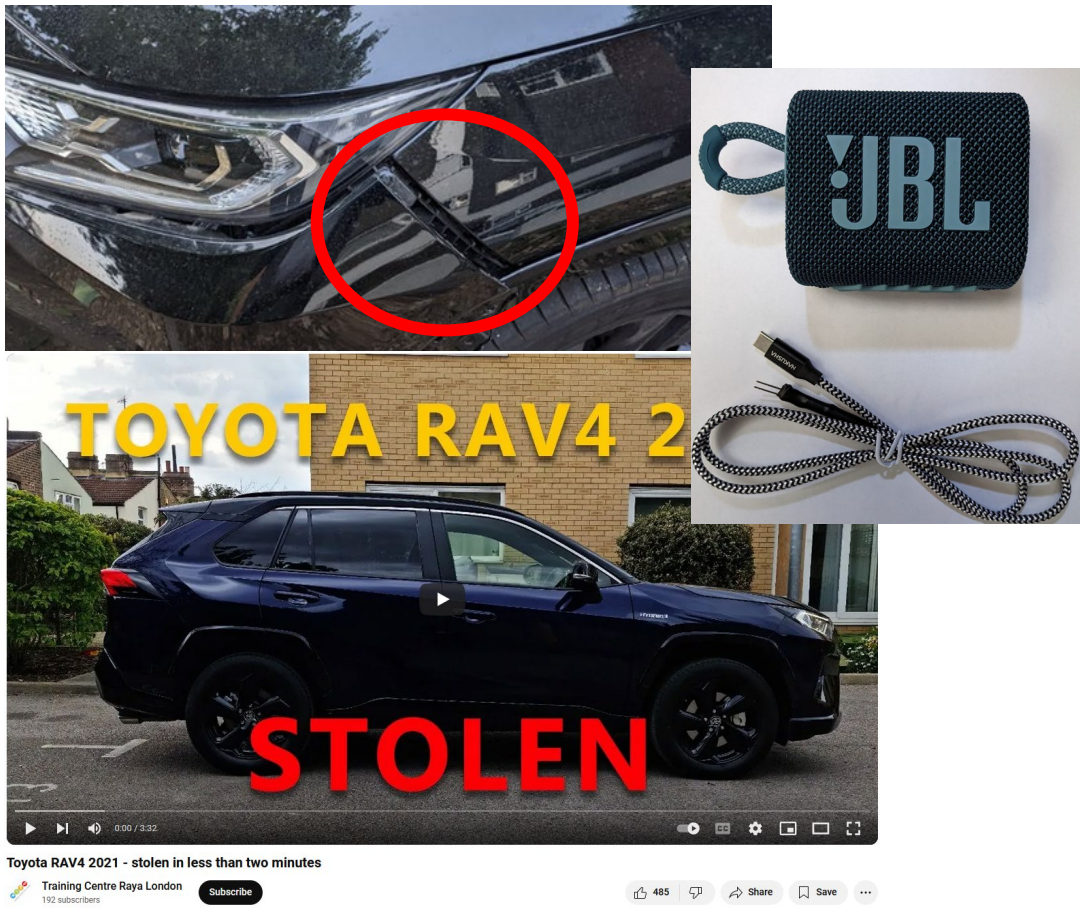
UNECE

Security in automotive

Example attack: Toyota headlights attack

Take away #1

Secure your critical in-vehicle communication



Toyota Rav 4 can be **stolen in less than two minutes**

1. Pull back bumper to access headlight
2. Connect CAN injection device to CAN bus
3. Activate CAN injection device to unlock vehicle

How does the attack work?

– CAN injection device impersonates smart key receiver
– CAN injection device sends message „Key validated, unlock immobilizer“ on CAN bus

Why does the attack work?

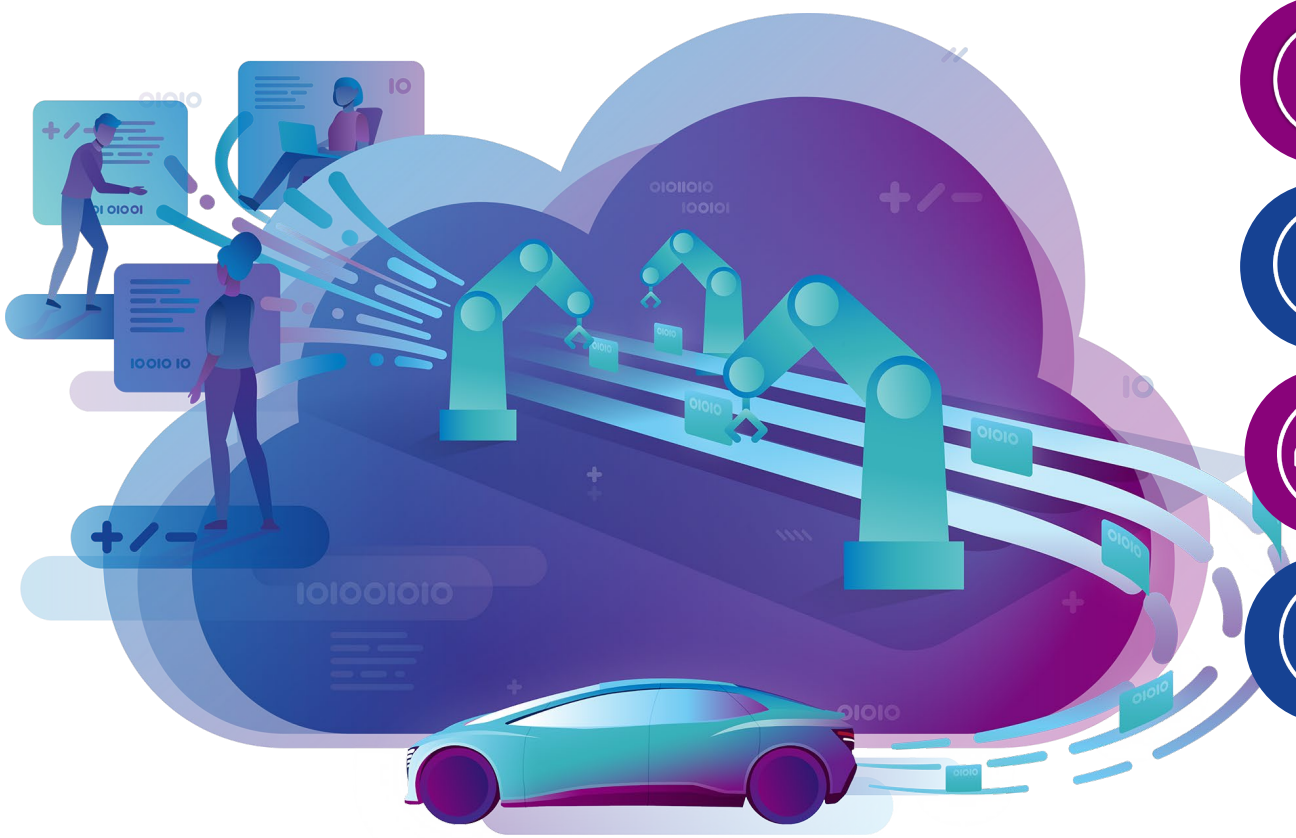
– Critical messages not authenticated
– Very little effort to impersonate smart key receiver

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

AUTOSAR can help!

Security in automotive

AUTOSAR

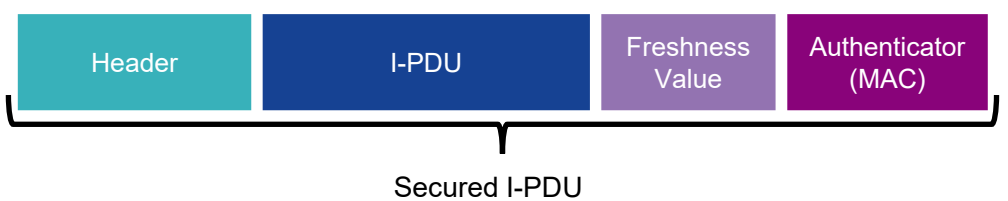


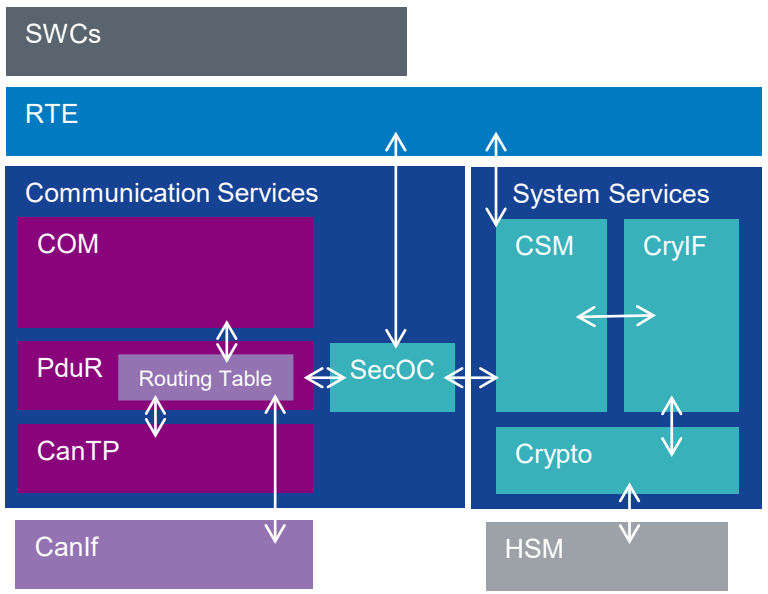
- Contains several security building blocks
- A mature architecture, developed since 2003
- Widely used and accepted in the automotive industry
- You’re likely already familiar with it

Security in automotive

SecOC – Secure Onboard Communication

- **SecOC** provides security through authentication of PDUs.
- Generally, the authenticator contains a Message Authentication Code (**MAC**).
- Default AUTOSAR security profiles can select the algorithm.
- A **freshness value** is calculated in order to protect against **replay attacks**.
- The PDU Router (PduR) seamlessly routes I-PDU to and from SecOC **without any specific configuration** of the upper layer module.





Does SecOC really do the trick?

Does SecOC really do the trick?

Another real-world example

Take away #2
Secure your secret keys from unauthorized access

Security researchers manage to **extract SecOC keys** by

1. Reverse engineering of the firmware to understand it
2. Exploit flaws in UDS secure access to execute attacker code on the ECU
3. Use code execution to extract SecOC keys

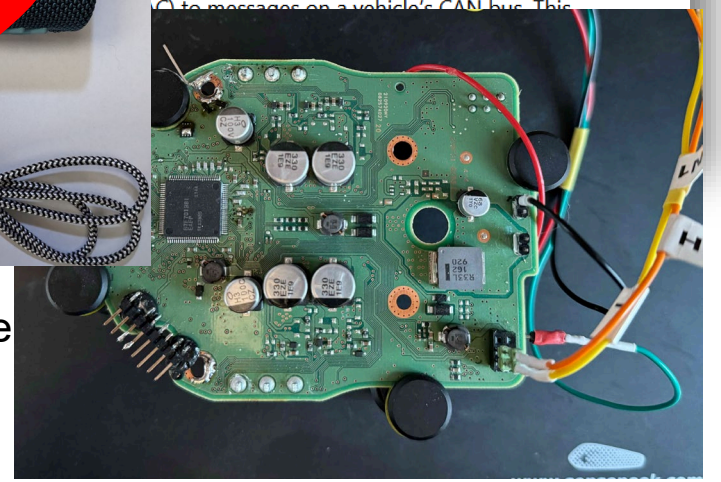
High initial effort, but attack is quick and can be repeated easily

➔**SecOC hacking device possible**

Extracting Secure Onboard Communication (SecOC) keys from a 2021 Toyota RAV4 Prime

Author: Willem Melching Mar 2, 2024

SecOC) is a new standard by AUTOSAR to add a



Why was the attack successful?

– Symmetric keys for authentication, stored in plaintext in the firmware image

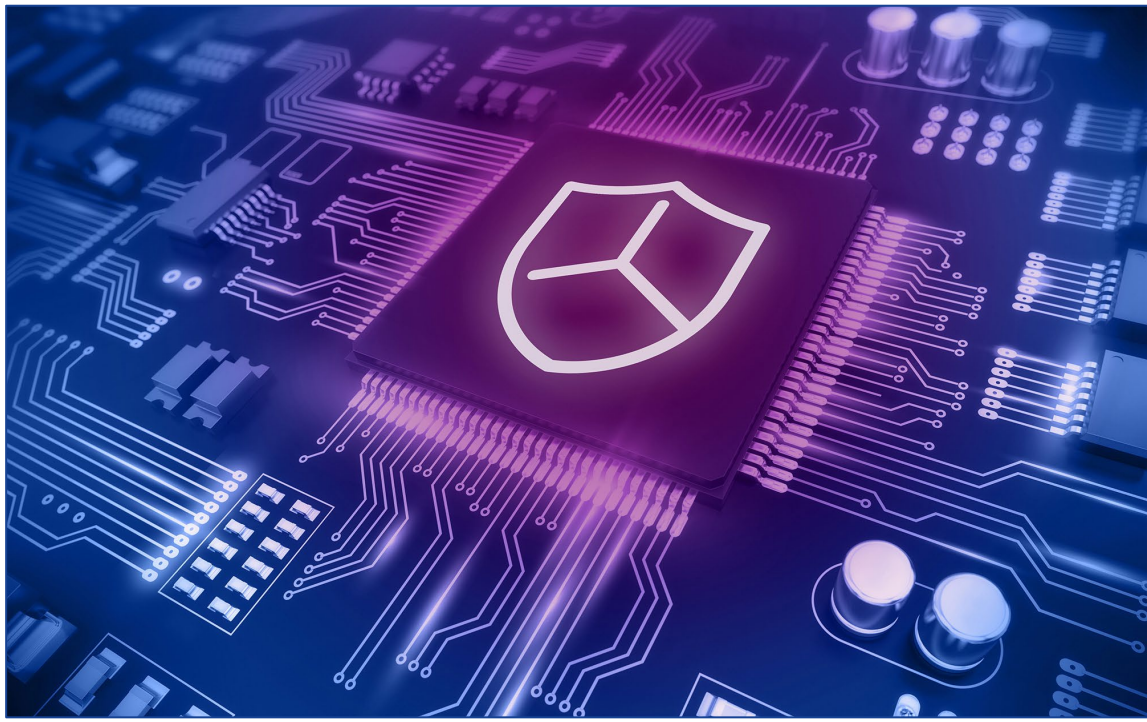
– SecOC keys are stored in plaintext on the ECU

Source: https://icanhack.nl/blog/secoc-key-extraction/

Does SecOC really do the trick?

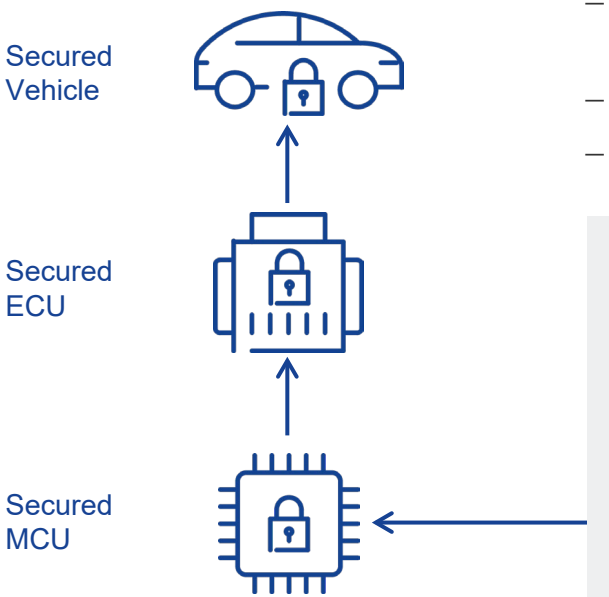
How the Hardware Security Module Enables SecOC

- Offers certificate management
- Holds keys for secure diagnostics
- Contains secure and encrypted memory

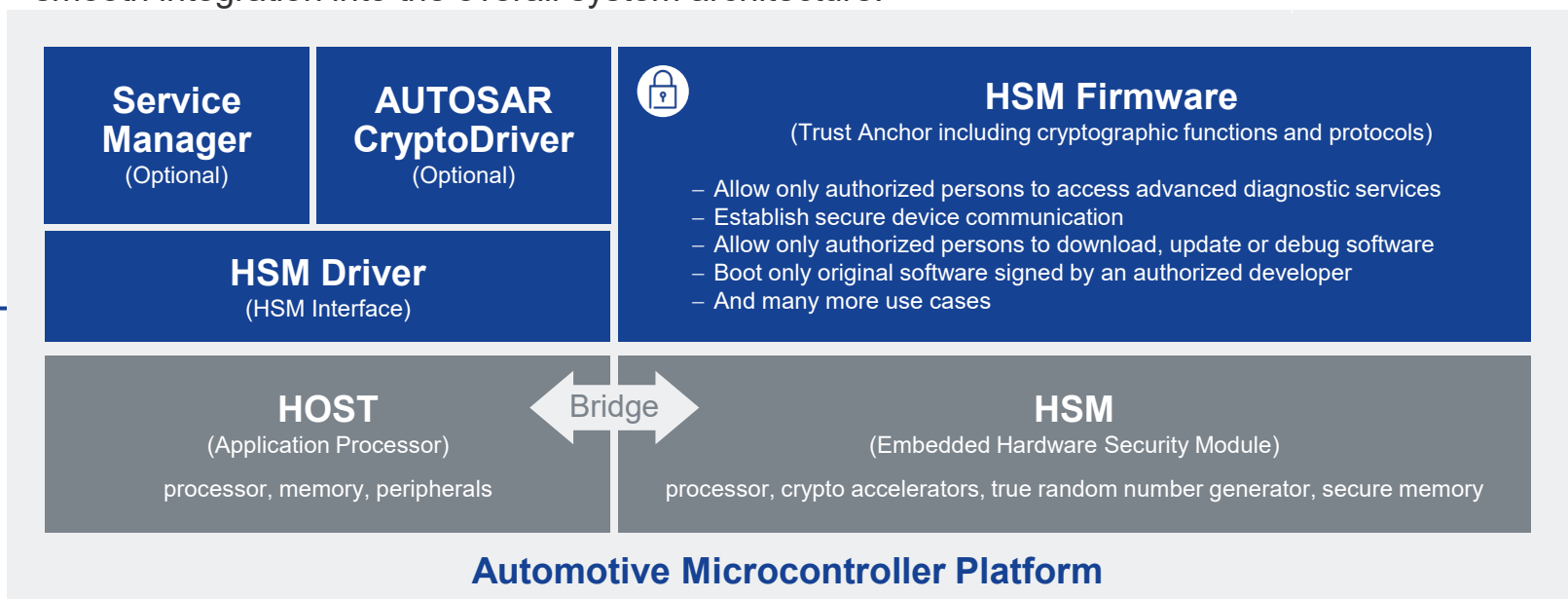


Does SecOC really do the trick?

The role of the Hardware Security Module - CycurHSM



- ESCRYPT CycurHSM is a software stack for the embedded Hardware Security Module of a Microcontroller.
- As a trust anchor it offers cryptographic protocols and algorithms to the application.
- ESCRYPT CycurHSM helps to easily fulfill complex OEM security requirements while ensuring a smooth integration into the overall system architecture.



There‘s more than that

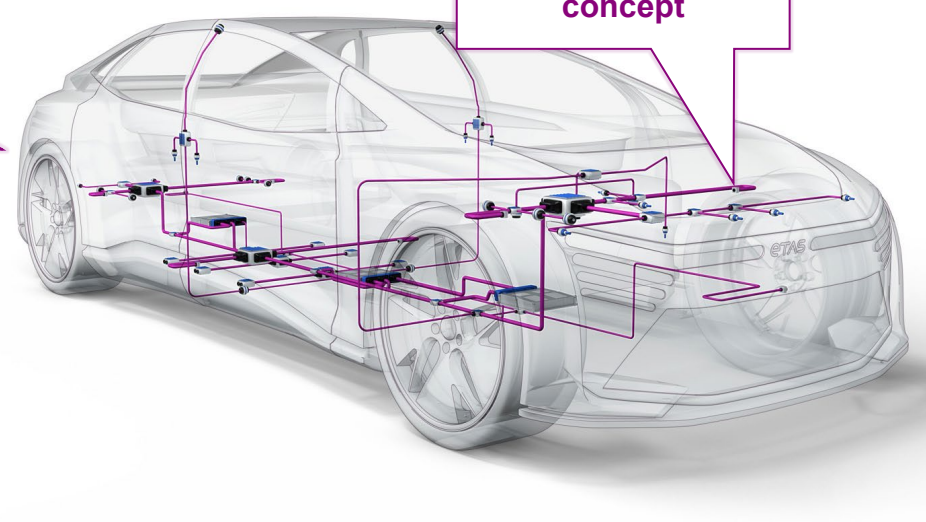
Holistic security covers more than what we can show today…

Secure Access
– Ensure that no unauthorized person can download / upload / debug software or data

Secure Operation
– Ensure that no malicious software is executed (Run Time Manipulation Detection)

Secure Startup (boot)
– Ensure that no malicious software is started

Hardware security modules are the nucleus to build complex holistic security concept



Secure Software Update
– Ensure that no malicious software is programmed into the ECU

Secure Communication
– Ensure authenticity and integrity of data received

Secure Production
– Ensure that secure data (key, certificates) cannot be accessed by a malicious person

There’s more than that

Keeping the ECU secure on the road

Security is not finished when the SOP is reached – the vehicle needs to stay secure also when it is on the road!

Intrusion Detection System

- Monitors ECU resources (e.g. communication) and raises Security Events in the case of suspicious events
- After an analysis by security experts, the OEM can decide how to react to the attack

Secure Firmware update over the air (FOTA)

- Fix bugs and security vulnerabilities by updating the ECUs firmware remotely
- A special flashbootloader verifies the signature of the update package before safely updating the ECU

Wrap-Up

What is required to build a secure ECU?

What is required to build a secure ECU?

Design phase

Security concept
– Analyse security needs: requirements, TARA, …
– Define security controls for the ECU

ETAS can support!

Hardware security
– Define requirements on secure hardware
– Select solution that fulfills the needs

ETAS can support!

Implementation phase

Leverage AUTOSAR
– Use off-the-shelf components to fix security holes
– Get support for correct configuration

ETAS can support!

Enhance expertise in team
– Trainings on AUTOSAR & Security

ETAS can support!

Test your implementation
– Code review, penetration test
– Tool-supported testing (fuzzing)

ETAS can support!

Post-production phase

Monitor the vehicle
– Detect attacks on your ECU
– AUTOSAR building blocks can support

ETAS can support!

Keep ECU up-to-date
– Fix security flaws by providing software over-the-air

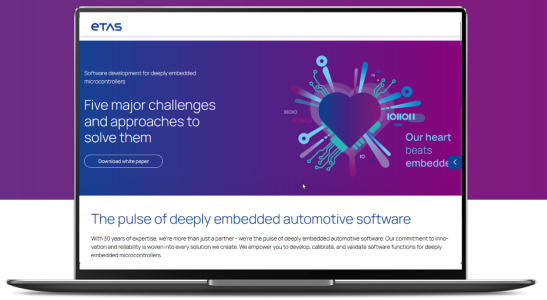
ETAS can support!

Contact us to discuss your needs

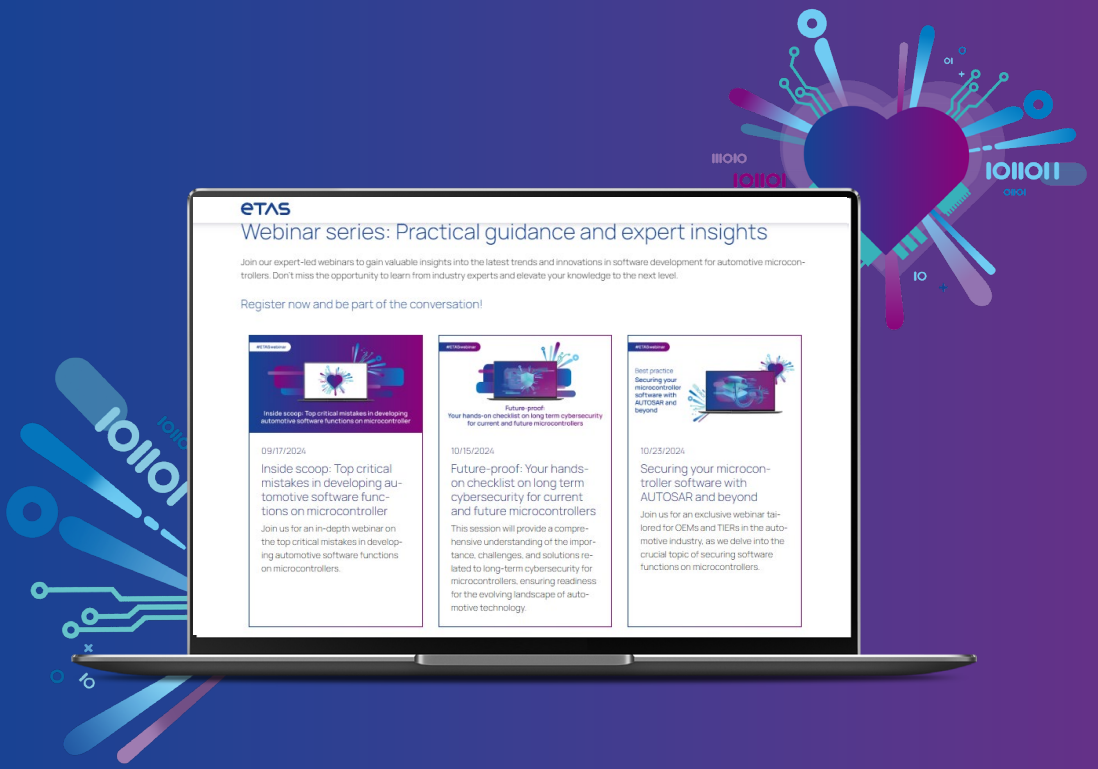
Anthony Esteban

Customer Chief Engineer

Contact



Visit our website



Upcoming webinars:

October 29
Mastering fuzz testing: How ETAS and Keysight empower the automotive industry to overcome cybersecurity challenges amid regulatory compliance – more information

November 6
Measurement, calibration & validation for any vehicle at its best – more information

November 26
Opportunities and limits of virtual testing – more information

December 10
Ask the expert: Bring your ECU software development process problem and we discuss – more information

Thank you!