Securing hardware components and connection enablers in the VCU

Securing hardware components & the connection enablers in the VCU

Your speakers

Tobias Klein

Manager Onboard Security

- Electrical engineering and IT security background
- > 15 years experience in product management and engineering
- > 20 Patents and publications in cybersecurity, radar and UAV systems
- empowering you to protect your vehicles

Dr. Max Hoffmann

Security Manager
Onboard Security

- M.Sc. in Information Security (2017), Ph.D. in Hardware Security (2020)
- Experienced in the security software development lifecycle, from threat modeling, over secure design, to vulnerability management
- External lecturer @ Ruhr University Bochum

Christian Schleiffer

Sales Director

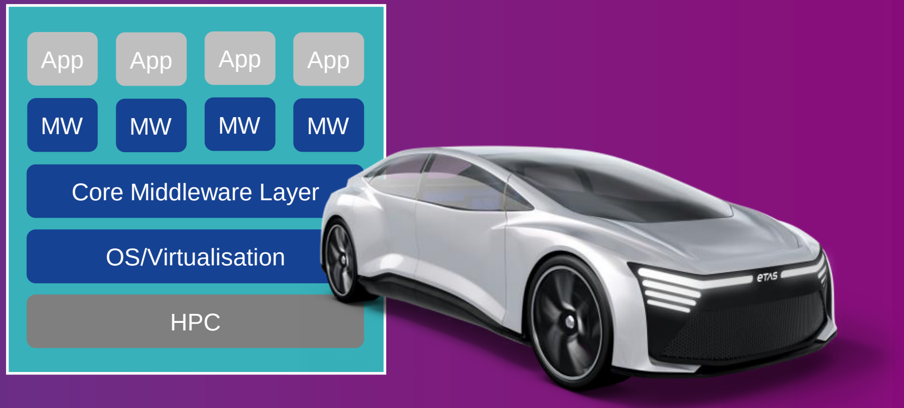
- IT & Cybersecurity engineering background
- >15 years automotive industry experience in project management, acquisitions and sales management
- Always striving to find fitting and sustainable solutions for our customers

Motivation: Why do we need new security concepts?

Shifting features, shifting threats: navigating the evolving attack landscape of feature-on-demand

Today E/E architecture
is evolving…

... and we desire to
bring more functionality to VCUs.



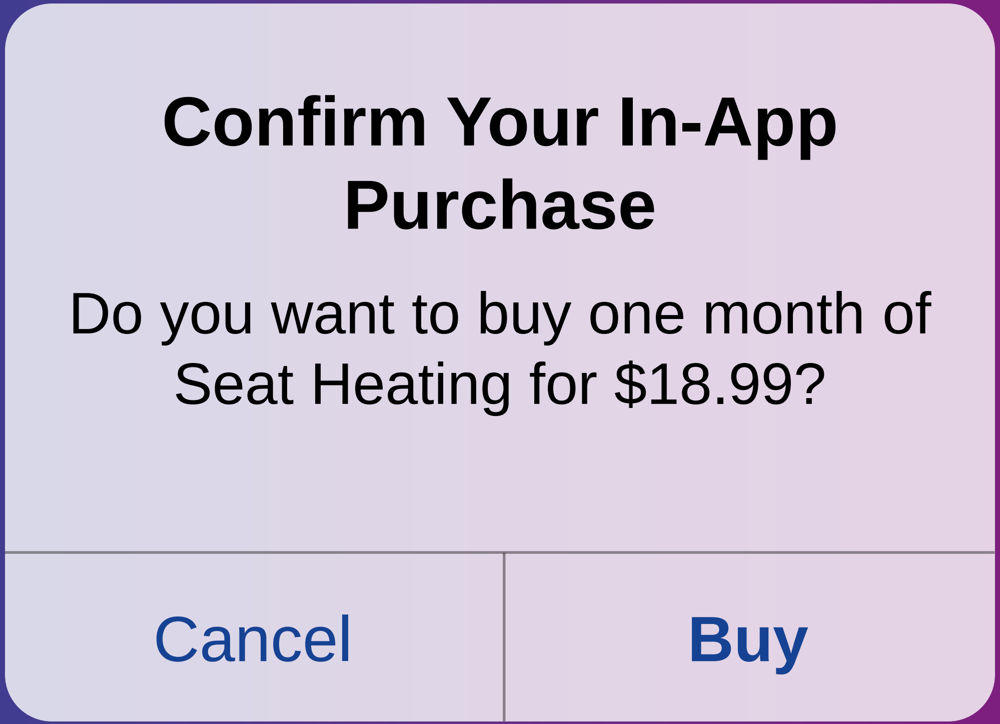
App App App App

MW MW MW MW

Core Middleware Layer

OS/Virtualisation

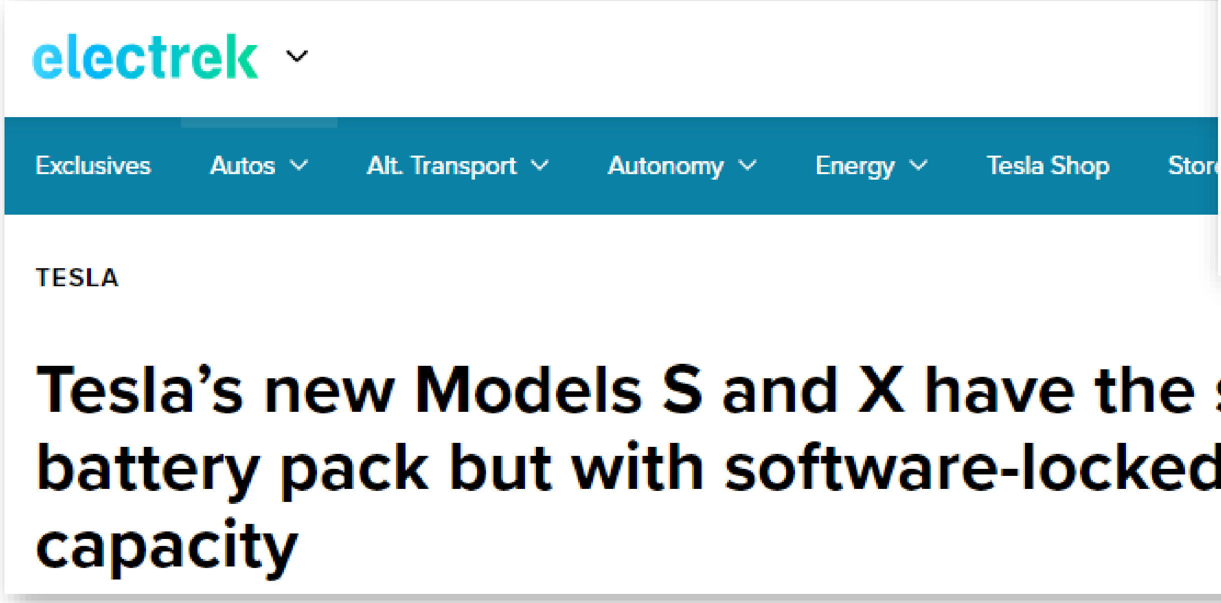
HPC



Confirm Your In-App Purchase

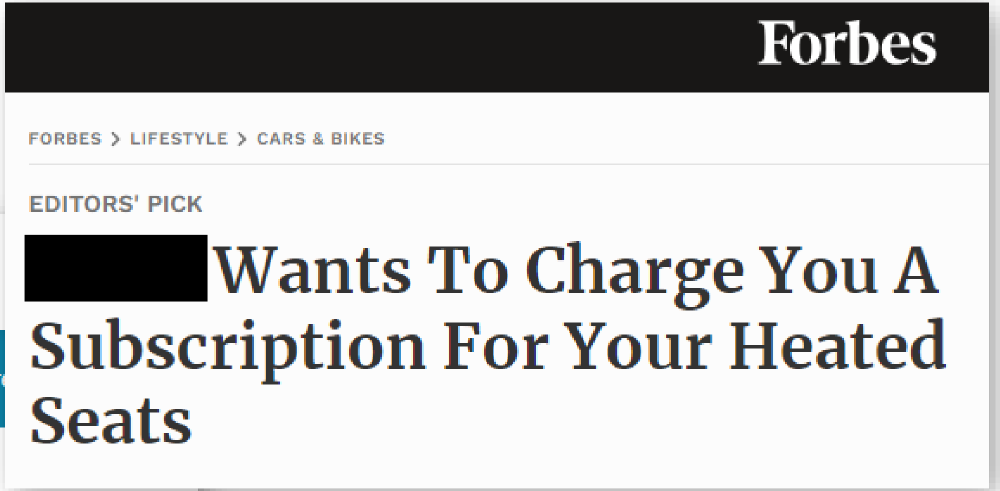
Do you want to buy one month of Seat Heating for $18.99?

Software-defined features …



TESLA

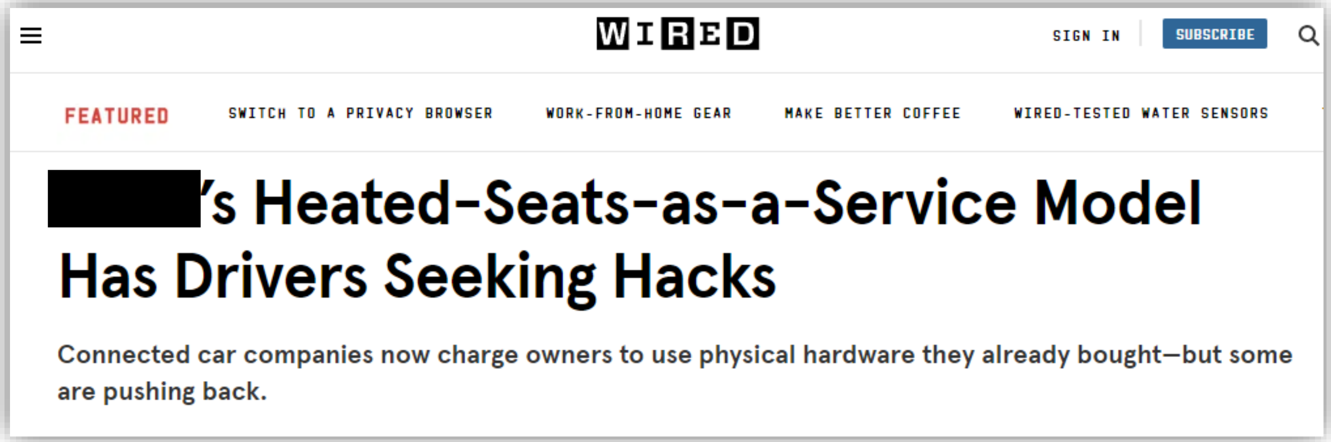
Tesla’s new Models S and X have the same battery pack but with software-locked capacity



EDITORS' PICK

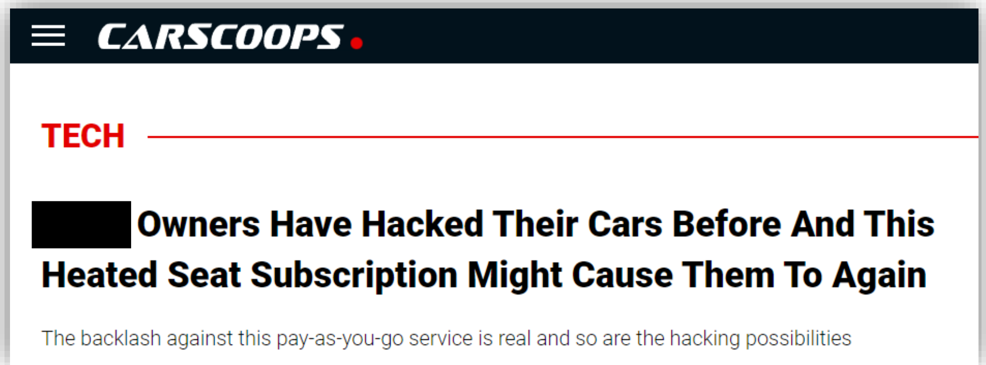
[redacted] Wants To Charge You A Subscription For Your Heated Seats

… invite hackers



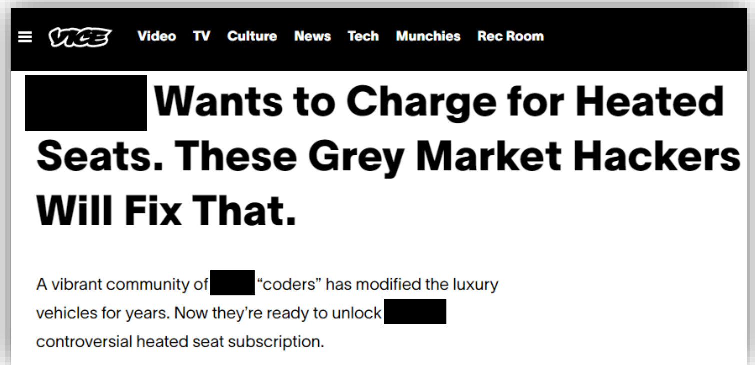
[redacted]'s Heated-Seats-as-a-Service Model Has Drivers Seeking Hacks

Connected car companies now charge owners to use physical hardware they already bought—but some are pushing back.



[redacted] Owners Have Hacked Their Cars Before And This Heated Seat Subscription Might Cause Them To Again

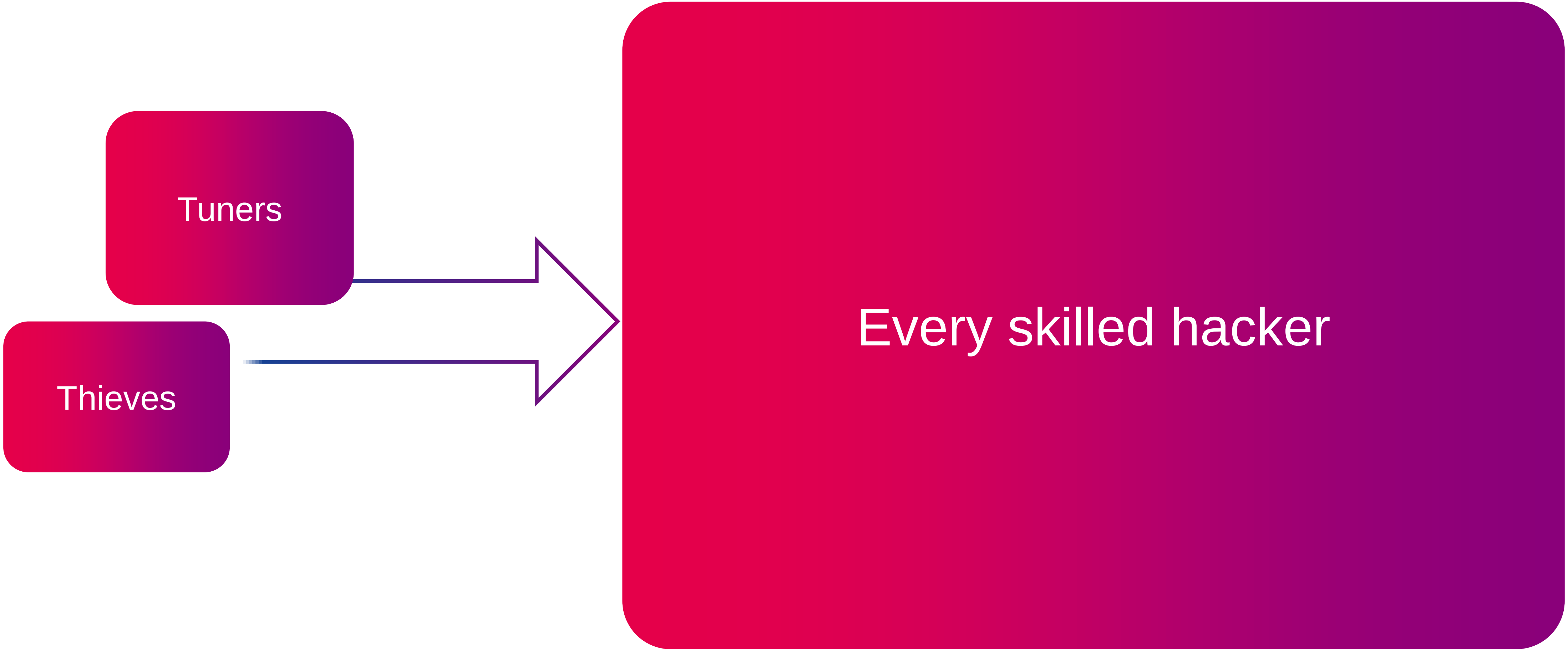
The backlash against this pay-as-you-go service is real and so are the hacking possibilities



[redacted] Wants to Charge for Heated Seats. These Grey Market Hackers Will Fix That.

A vibrant community of [redacted] "coders" has modified the luxury vehicles for years. Now they're ready to unlock [redacted] controversial heated seat subscription.

A disruptive change in threat actors

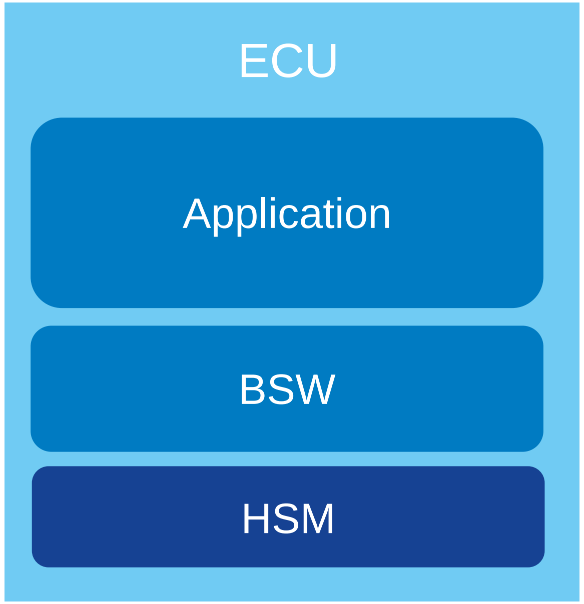


Tuners

Thieves

Every skilled hacker

Challenges in a Multi-VM environment



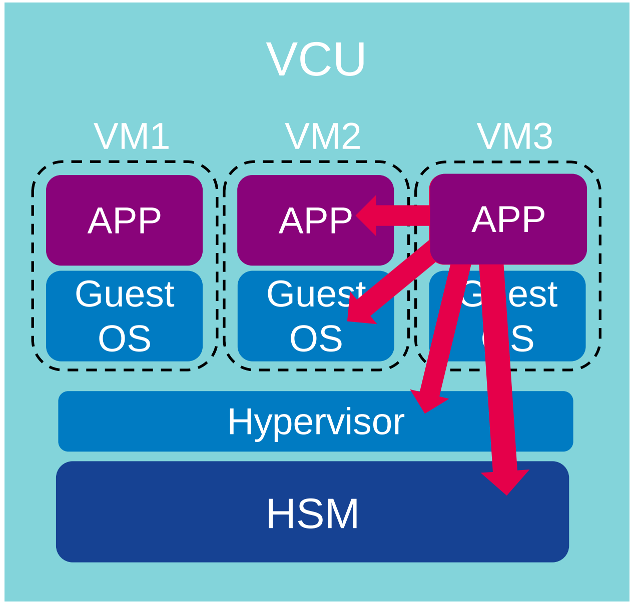
ECU

Application

BSW

HSM

Single application,
single attack target



VCU

VM1

VM2

VM3

APP

APP

APP

Guest OS

Guest OS

Guest OS

Hypervisor

HSM

Multiple applications,
different domains/priorities,
multiple attack targets

Automotive Cross-Domain Security: the concept

ETAS

Layered Defense

- Be able to react on different levels: adequate local response
- Avoid single points of failure

Strong Isolation as Base

- Segment the system into specialized domains
- Restricted and secure inter-domain communications

Local Security Response

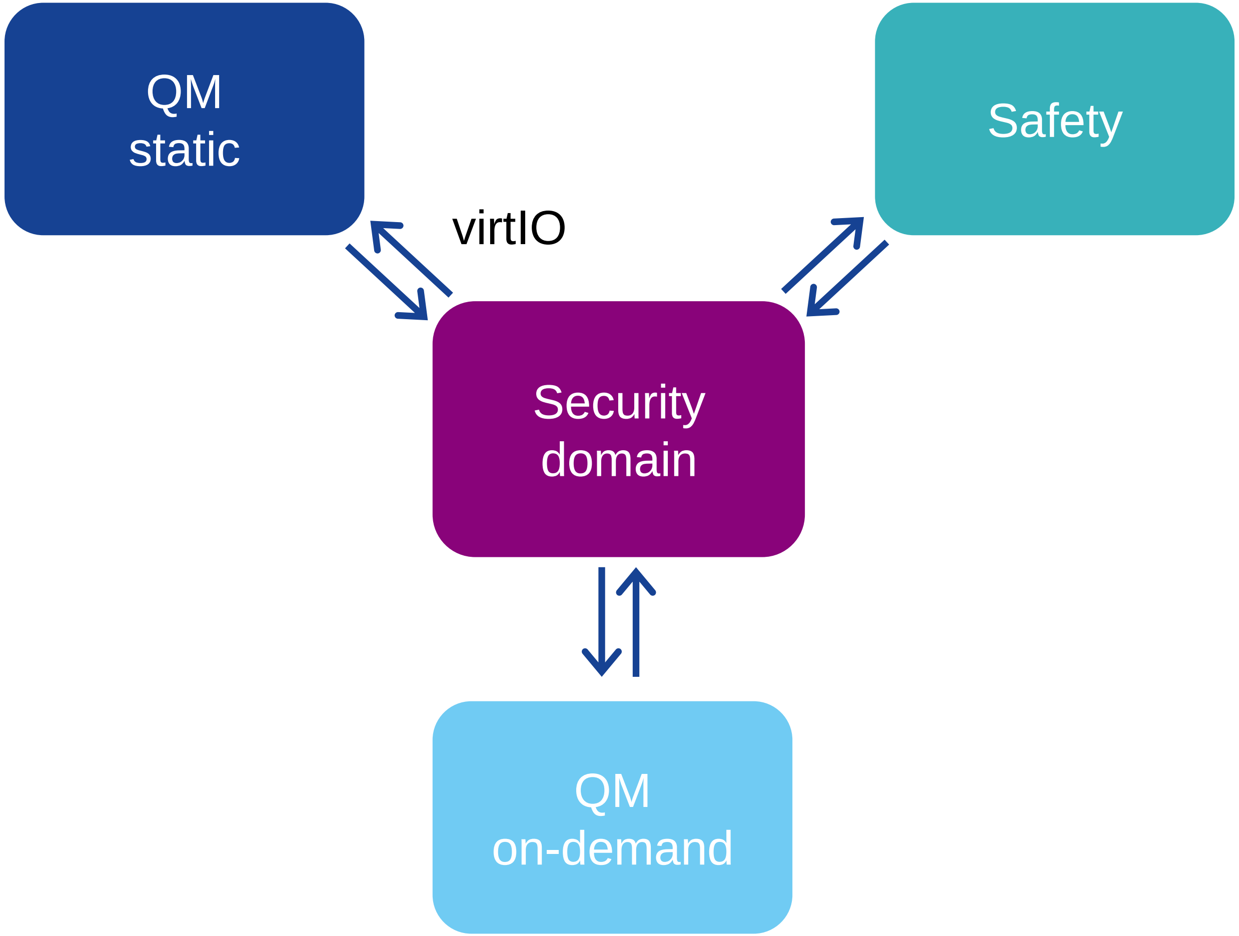
- Automatic security response on the device
- Essential functions stay operational during incidents

Centralized Monitoring and Dynamic Prevention

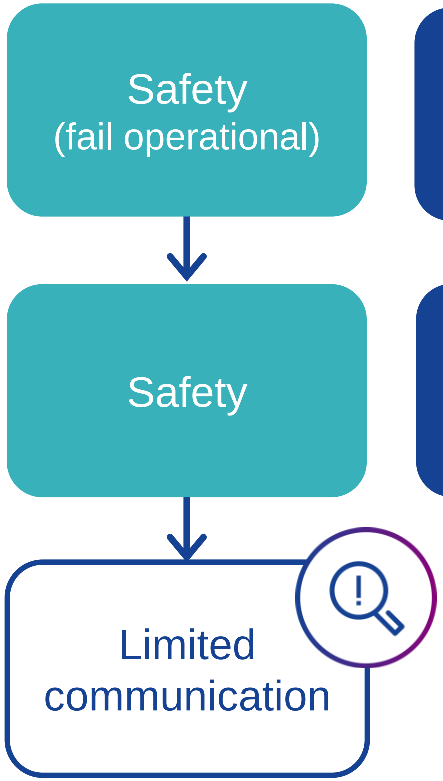
- Utilize a core security domain
- Detect anomalies and activate adaptive countermeasures across domains in real time

Automotive Cross-Domain Security: the concept

Domains are segmented by desired security response



Domains are segmented by desired security response



Safety (fail operational)

QM static

QM on-demand

Safety

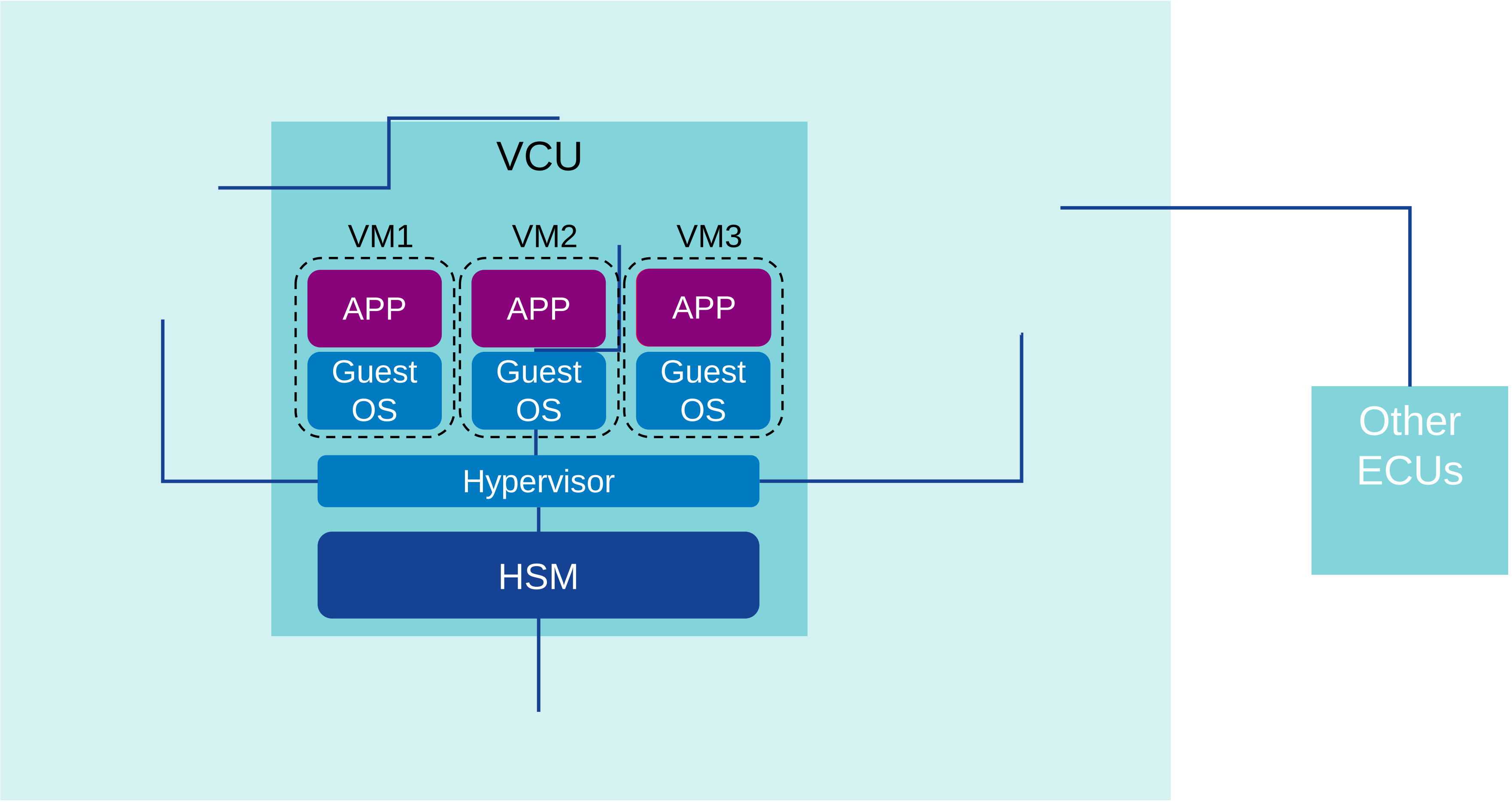
Fallback VM

STOP!

Limited communication

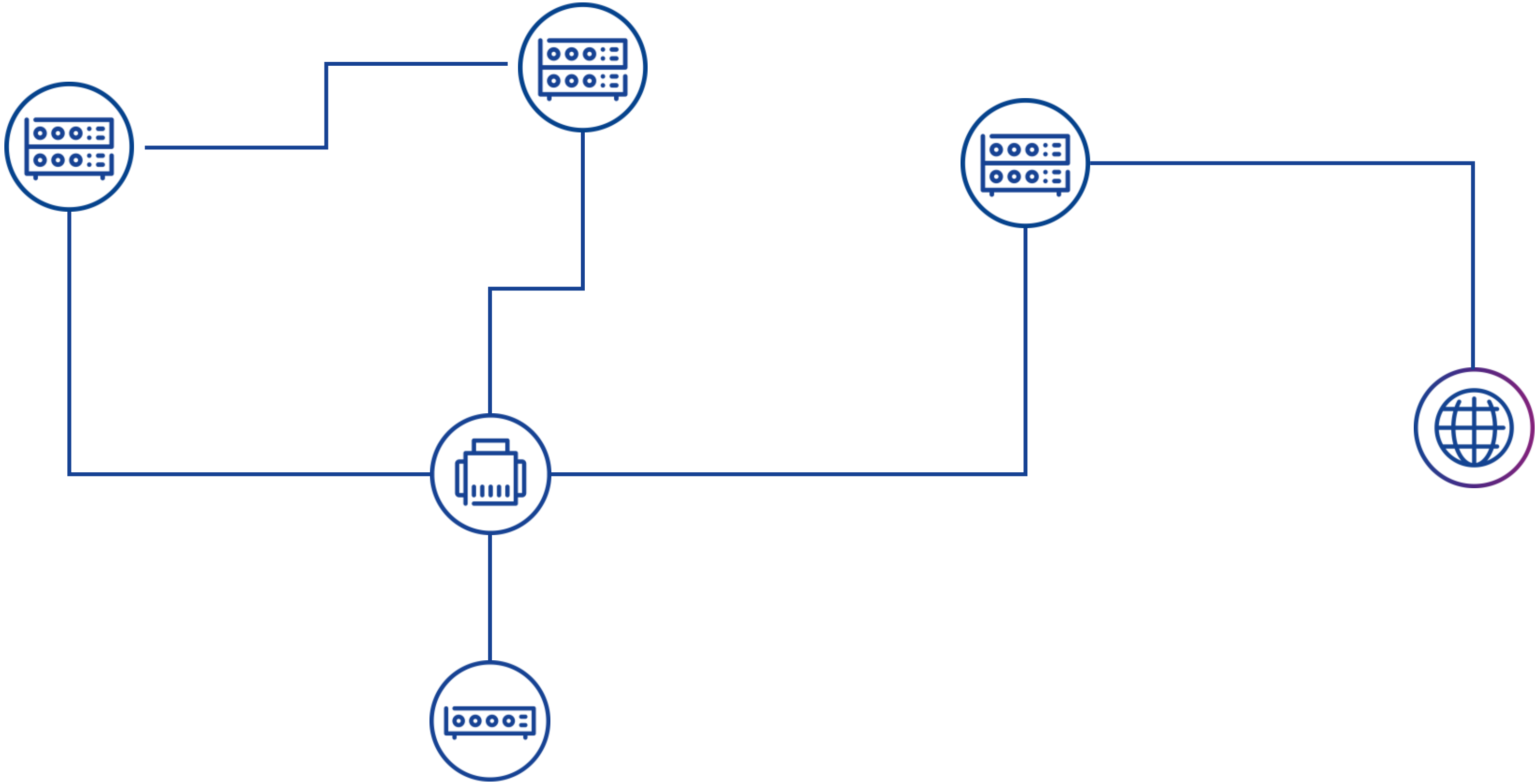
Practical application

VCU software Stack

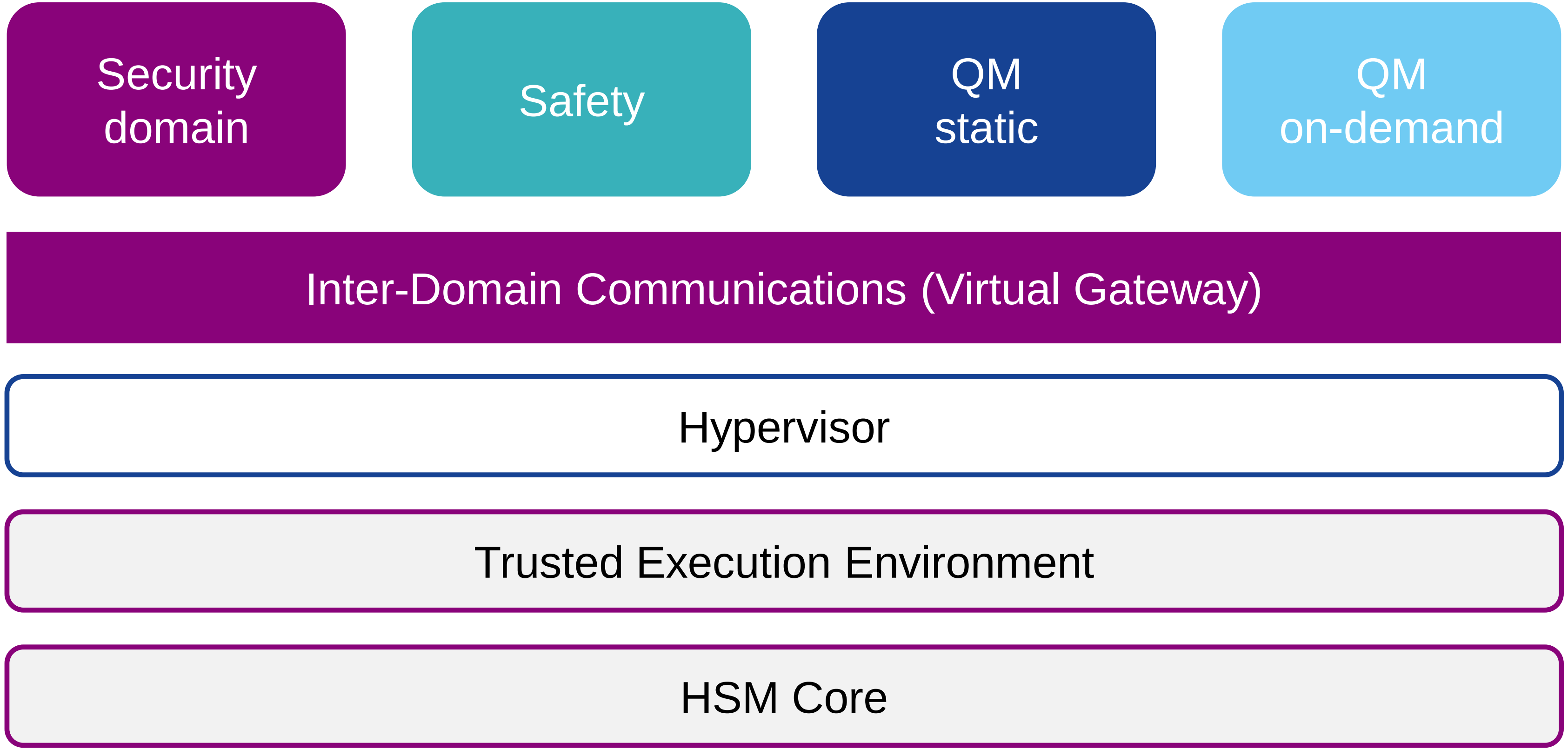


Comparison with Enterprise IT

VCU software Stack



Leveraging TEEs, HSMs, and Virtualization



Security domain

Safety

QM static

QM on-demand

Inter-Domain Communications (Virtual Gateway)

Hypervisor

Trusted Execution Environment

HSM Core

Leveraging TEEs, HSMs, and Virtualization

Trusted Execution Environment (TEE)

- Identify requesting service within a VM (IDS)
- Policy enforcement
- Authentication
- Data integrity
- Confidentiality
- Strong multi-user capability

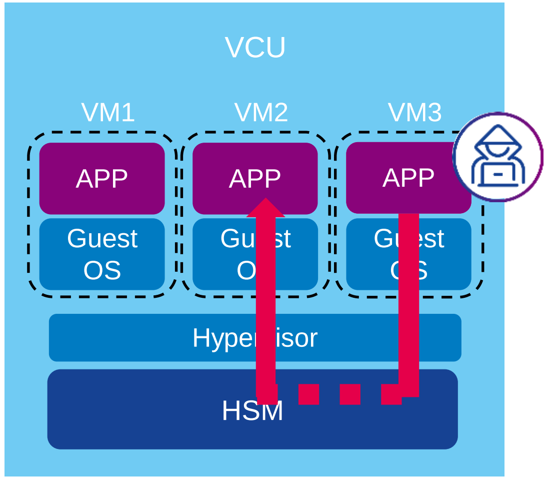
Hardware Security Module (HSM)

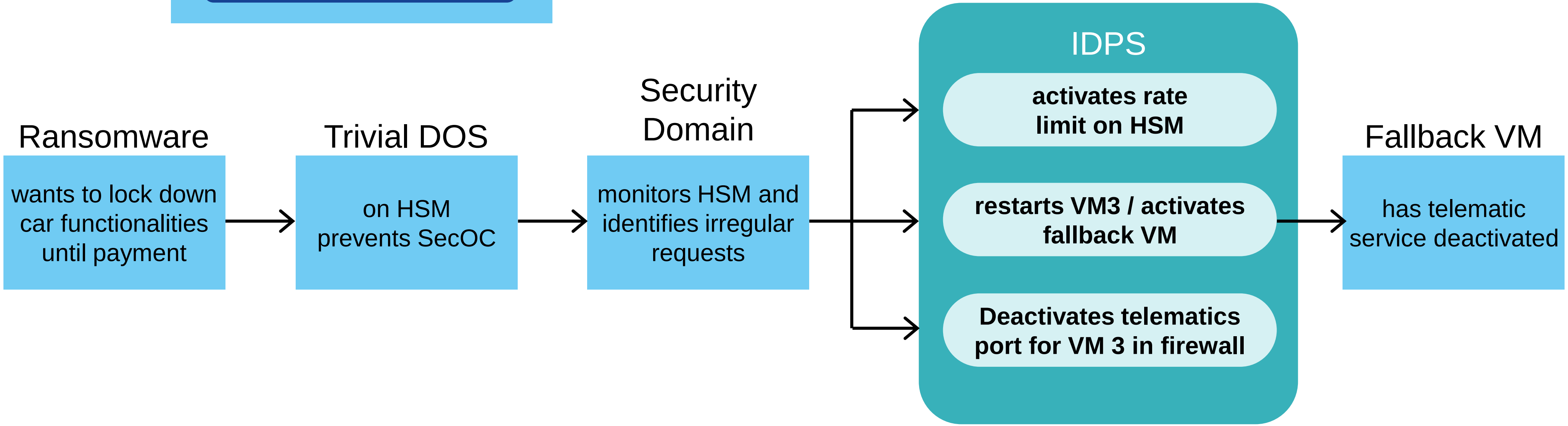
- Tamper-resistant
- RTMD
- Key storage and encryption, securing critical assets
- Low latency, but fewer users
- Full parallel operation

Virtual Network Channels

- Well-defined data flow
- Control over comm. matrix
- Flexible SW positioning

Example: mitigating a ransomware attack





Ransomware
wants to lock down car functionalities until payment

Trivial DOS
on HSM prevents SecOC

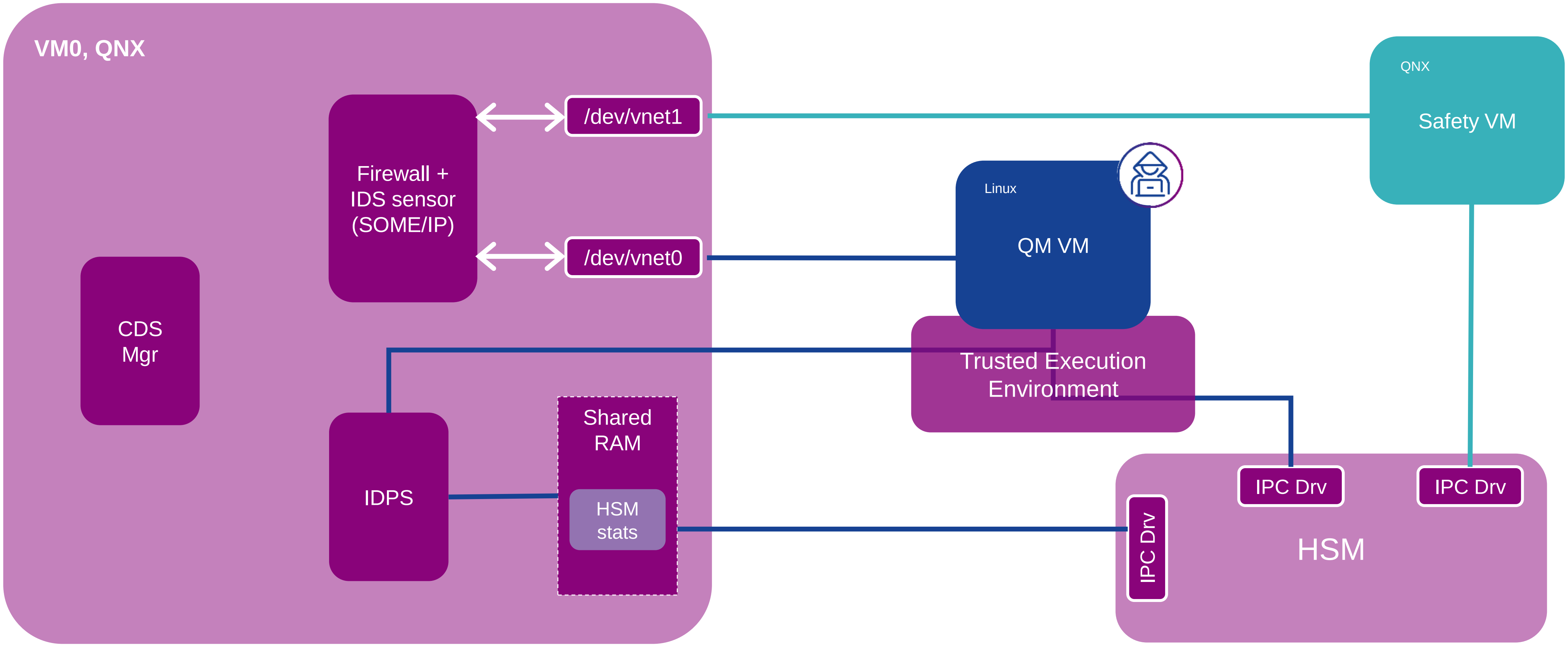
Security Domain
monitors HSM and identifies irregular requests

IDPS
- **activates rate limit on HSM**
- **restarts VM3 / activates fallback VM**
- **Deactivates telematics port for VM 3 in firewall**

Fallback VM
has telematic service deactivated

Deep dive into the security domain

Example mitigating a ransomware attack

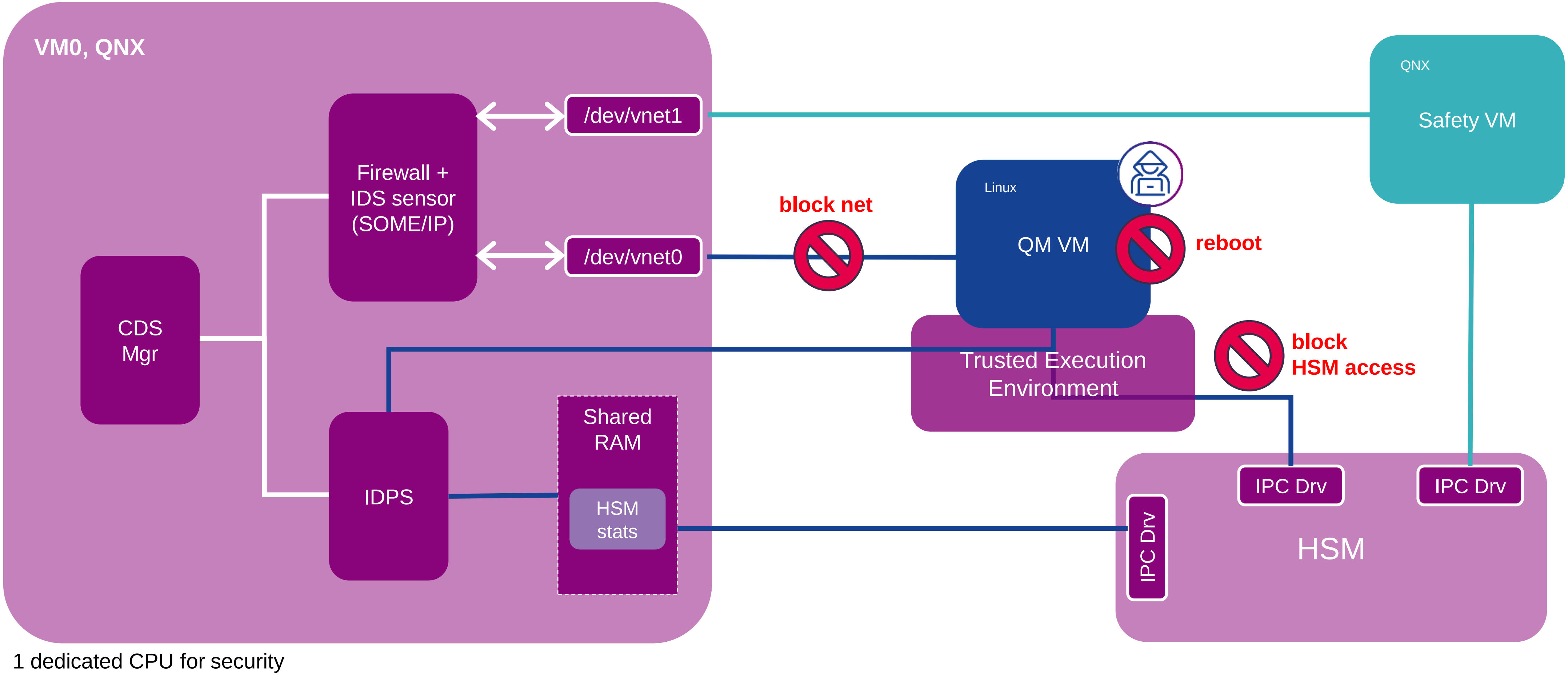


1 dedicated CPU for security

🟪 Security domain 🟦 QM domain 🟩 Safety domain

Deep dive into the security domain

Example mitigating a ransomware attack

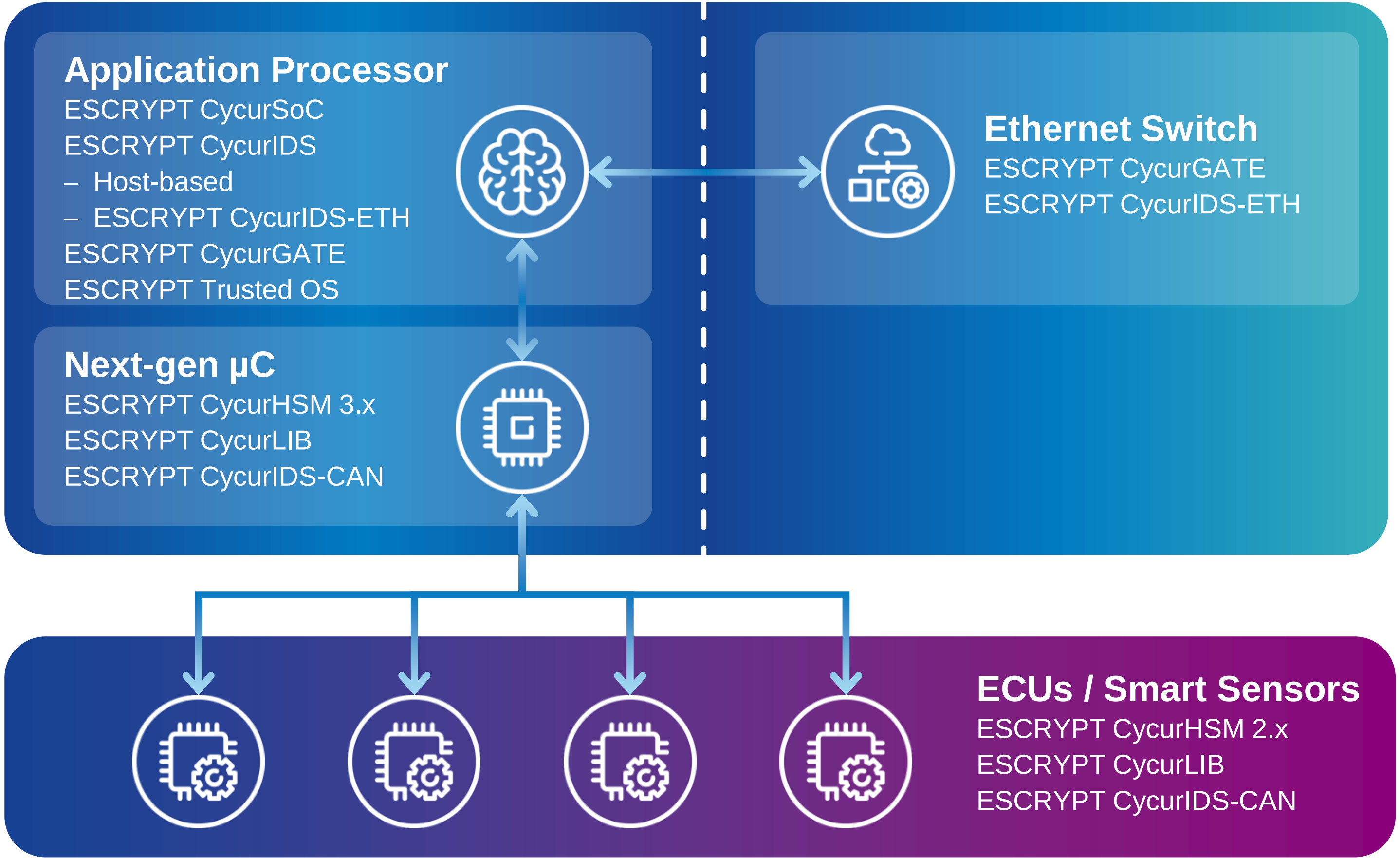


🟪 Security domain 🟦 QM domain 🟩 Safety domain

Vehicle Computer Security Suite

ETAS product portfolio

Vehicle Computer Unit (VCU)



Application Processor

ESCRYPT CycurSoC

ESCRYPT CycurIDS

- Host-based
- ESCRYPT CycurIDS-ETH

ESCRYPT CycurGATE

ESCRYPT Trusted OS

Ethernet Switch

ESCRYPT CycurGATE

ESCRYPT CycurIDS-ETH

Next-gen µC

ESCRYPT CycurHSM 3.x

ESCRYPT CycurLIB

ESCRYPT CycurIDS-CAN

ECUs / Smart Sensors

ESCRYPT CycurHSM 2.x

ESCRYPT CycurLIB

ESCRYPT CycurIDS-CAN

Automotive Cross Domain Security

Summary

Layered defense

Flexibility

Proactive threat management

Strong isolation

Ensure flexibility without compromising on safety or security.

Stay tuned!
Our new whitepaper will be released in the next days

Follow ETAS on LinkedIN to be informed about the release!

Automotive cross-domain security framework

Ensuring safety, security, and flexibility
in next-gen vehicle computers

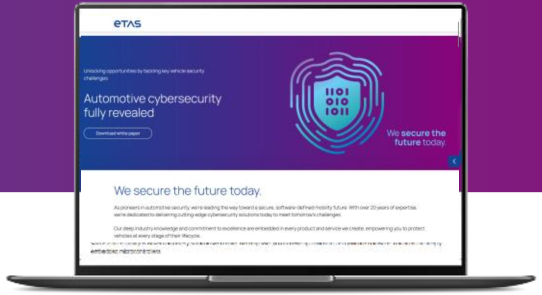
Empowering Tomorrow's Automotive Software
www.etas.com

Contact

Christian Schleiffer

Sales Director

Contact



Unlocking opportunities by tackling key vehicle security challenges

Automotive cybersecurity fully revealed

We secure the future today.

As pioneers in automotive security, we're leading the way toward a secure, software-defined mobility future. With over 20 years of expertise, we're dedicated to delivering cutting-edge cybersecurity solutions today to meet tomorrow's challenges.

Our deep industry knowledge and commitment to excellence are embedded in every product and service we create, empowering you to protect vehicles at every stage of their lifecycle.

Visit our website www.etas.com/we-secure-the-future

Or follow us on social media

Best practice: Enhancing automotive cybersecurity with effective vulnerability management

Register now:

March 11th, 10-11 AM CET
March 12th, 04-05 PM CET

#ETASwebinar
Best practice: Enhancing automotive cybersecurity with effective vulnerability management

Q&A

Thank you!