MIXED CRITICALITY CHALLENGES
HOW TO ENSURE SECURITY OF HYPERCONVERGED PLATFORMS?

GLOBAL PLATFORM MUNICH – OCTOBER 21, 2026

REDOUANE SOUM

Redouane SOUM

- 18y experience in HW/SW Architecture
  - System Architect at Intel
- 8y experience in Cybersecurity
  - Cybersecurity Expert at Ampere

Achievements

- Cybersecurity lead for onboard/offboard communication – Megane e-Tech (2022)
- Cybersecurity lead for latest gateway – Scenic (2024)
- 2 cybersecurity patents

AMPERE

SUMMARY

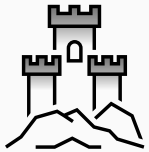
1. CYBERSECURITY CHALLENGES
   WHAT ARE THE NEW CHALLENGES?
2. FEW EXAMPLES
   IS IT JUST SCI-FI ?
3. ENABLERS
   HOW COULD WE SOLVE THEM ?
4. CONCLUSION

1

CYBERSECURITY CHALLENGES

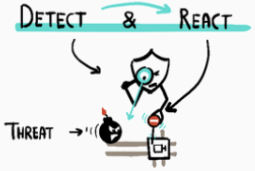
WHAT ARE THE NEW CHALLENGES?

Safe and Secure Product – Main Principles



#1 – SECURED BY DESIGN

System must be built to be strong, easy to protect and maintain



#2 - DETECT & REACT

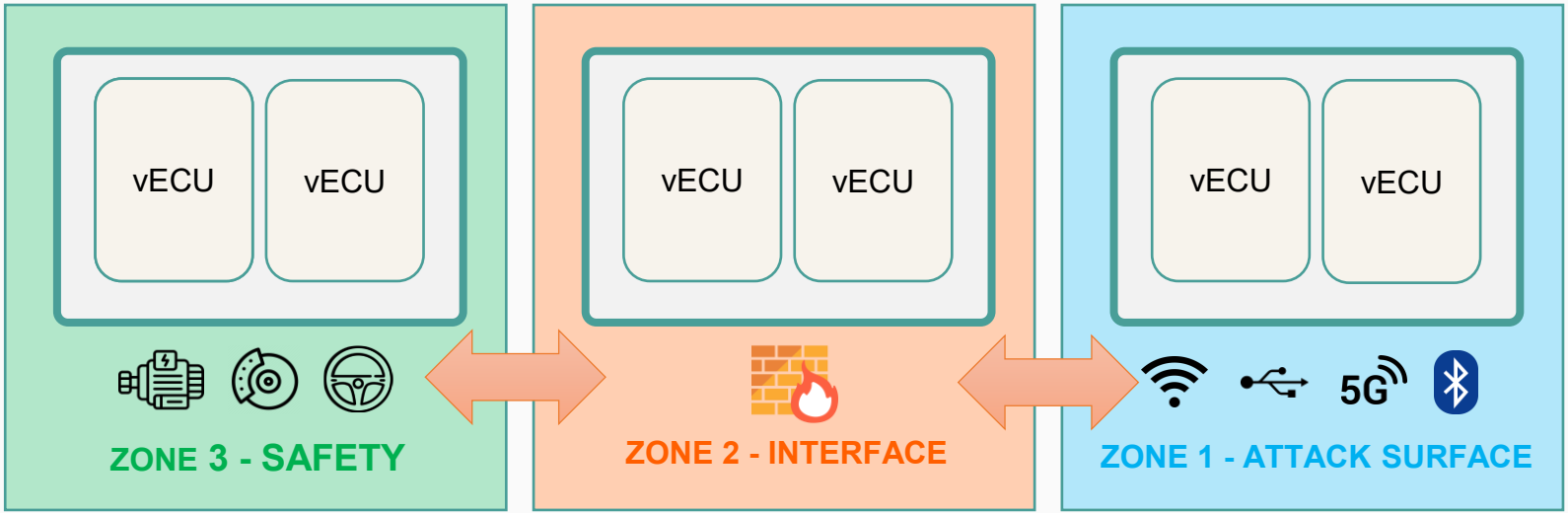
System is Monitored and the organization has Reaction capabilities to protect it.

#3 - PRESERVE & MAINTAIN

System protection must evolve with the threat and must be preserved then fixed if weakened by vulnerability.

02 –Cybersecurity challenges

SECURED BY DESIGN



Hosts safety, car dynamics and automotive functions

Safety (Autosar – Real time core)

Isolate Z1 and Z3 by attack surface reduction and access control

No Safety

Attack surface in direct contact with car external components.

No Safety
No impact on vehicle usage

vECU: virtual ECU

AMPERE

SOFTWARE-DEFINED VEHICLE SECURITY

02 –Cybersecurity challenges – Shared HW/SW

SECURED BY DESIGN

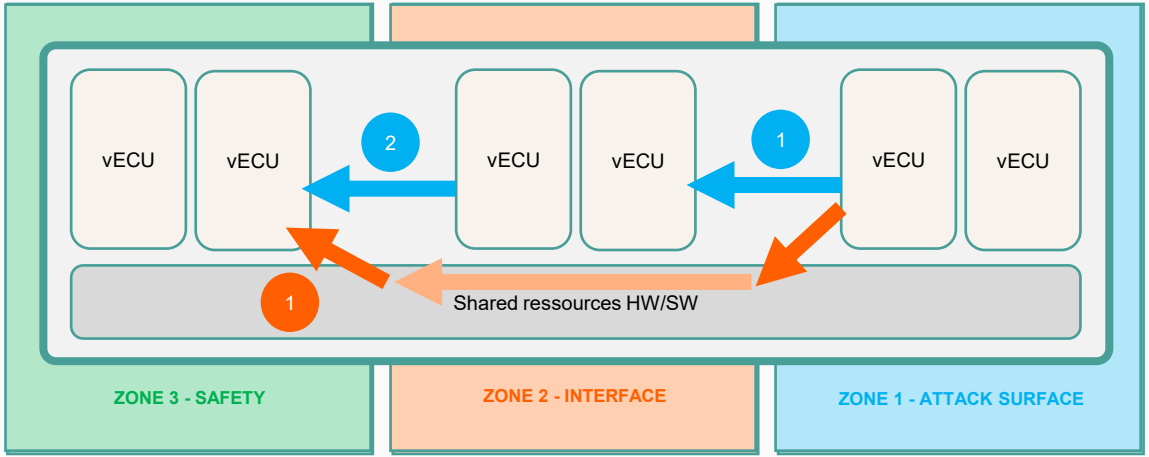
- **Before SDV** Attack path between ECU = Network communications (←)
- **SDV:** + Shared Ressources (←)

LEGACY ATTACK PATH

- Easy to identified directly linked to system fonctionnal Ucs
- Attack surface can be evaluated (network stacks and applications)

NEW ATTACK PATH

- Not linked to system functional Ucs
- Difficult to be exhaustive (meltdown?)
- How to evaluate properly the attack surface ?



How to introduce virtualisation while keeping impact on attack pathes acceptable ?

Legacy attack path

New SDV attack path

vECU: virtual ECU

SOFTWARE-DEFINED VEHICLE SECURITY

02 –Cybersecurity challenges – Shared HW/SW

SHARED HARDWARE / SOFTWARE AND SPOF*

- Virtualization : Cost reduction vs security
- Everything which is shared may be used to compromise other zones

Any of those attacks could lead to complete compromission

- List of attacks on shared components:
  - Boot rom attacks
  - Boot rom patch attacks
  - Bootloader attacks
  - HSM FW attacks
  - CPU Attacks (based on HW design) (cache attack meltdown / spectre)
  - SoC firewall (MMU, SMMU)
  - Hypervisor attacks
  - Internal IP attacks (internal ethernet switch)
  - and other vectors we don't know (yet)

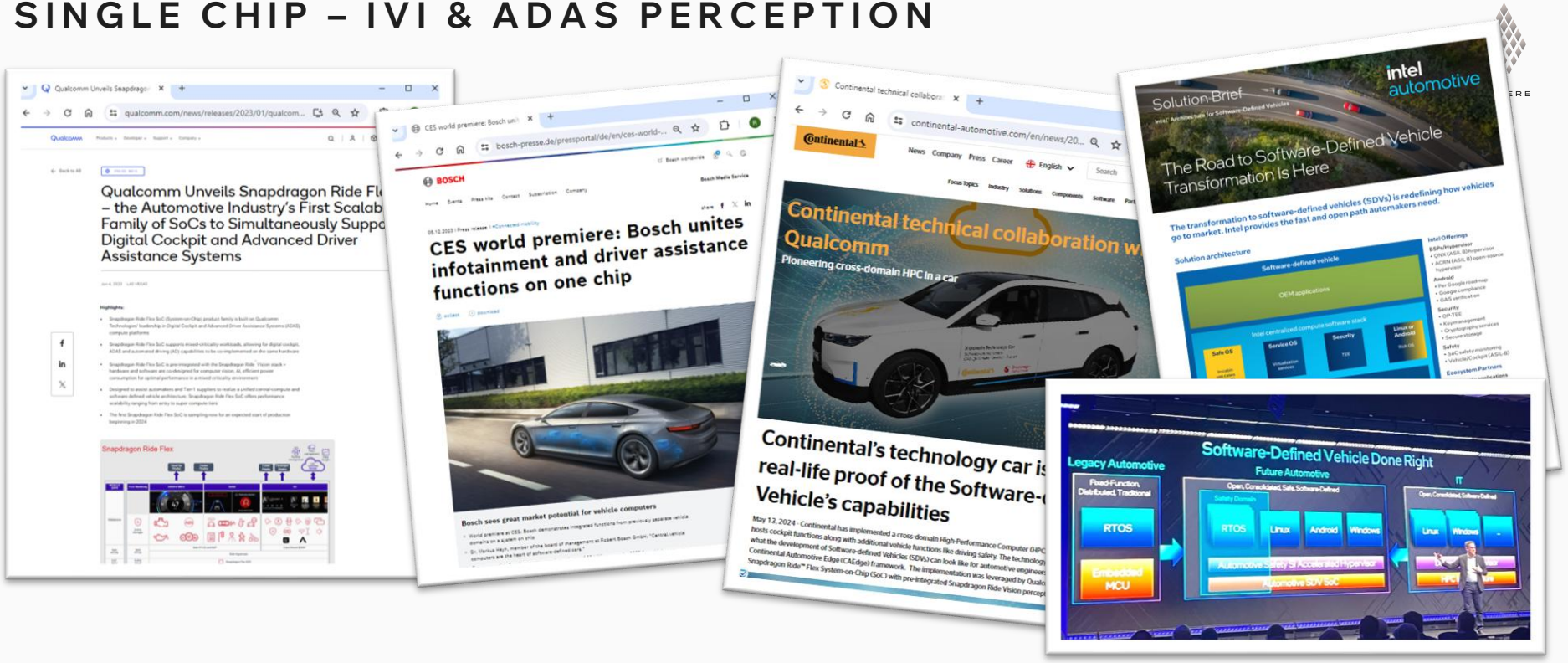
SPoF*: Single point of failure

2

FEW EXAMPLES

IS IT JUST SCI-FI ?

SDV IS NOT ENOUGH, HERE'S A NEW BUSINESS TREND SINGLE CHIP – IVI & ADAS PERCEPTION



Those are only examples of recent press releases, other suppliers than shown might be offering the same concepts. This presentation demonstrates the possible risks / impact of different approaches and does not focus on any specific product/company.

Sources:
Qualcomm Flex: https://www.qualcomm.com/news/releases/2023/01/qualcomm-unveils-snapdragon-ride-flex---the-automotive-industry-
Bosch: https://www.bosch-presse.de/pressportal/de/en/ces-world-premiere-bosch-unites-infotainment-and-driver-assistance-functions-on-one-chip-260608.html
Continental: https://www.continental-automotive.com/en/news/2024/05-13-continental-technical-collaboration-with-qualcomm.html
Intel SDV: https://www.intel.vn/content/dam/www/central-libraries/us/en/documents/2024-04/automotive-sdv-solution-brief.pdf

03 –Few examples – Step 1

PRIMITIVES USED

- memory safety vulnerability on IVI SW component exposed to WiFi

ATTACK PATH (1 STEP)

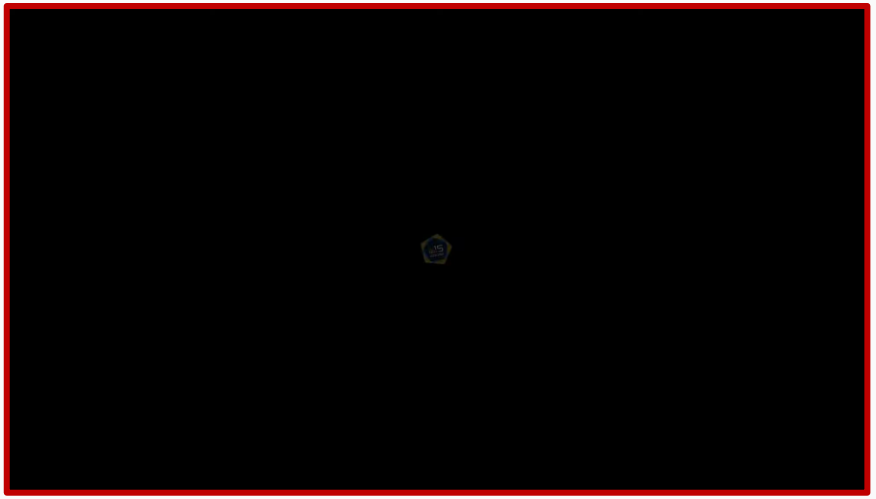
- 0-click over WIFI (HTTP Parser)
- Best Linux practices (ASLR, seccomp,...) have been bypassed using various techniques or misses in the configurations

IMPACT

- All IVI privileges

ATTACK COST

- ~200K€



AMPERE

SOFTWARE-DEFINED VEHICLE SECURITY

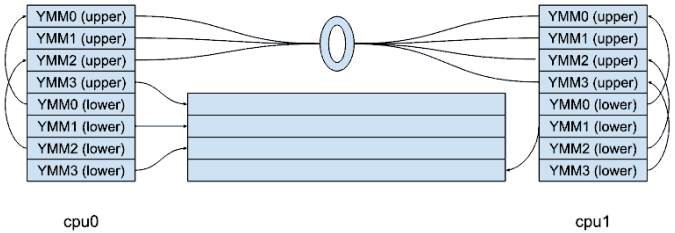
https://www.youtube.com/watch?v=k_F4wHc4h6k
https://www.synacktiv.com/sites/default/files/2022-10/tesla_hexacon.pdf

03 –Few examples – Step 2 (SPoF)

EXAMPLES

- SOC - ZENBLEED CPU core misprediction (in speculative execution) leads to register leak from process to process
  https://lock.cmpxchg8b.com/zenbleed.html
- SOC - APPLE A12–A16 BIONIC GPU By passing memory isolation using on-chip GPU
  kapersky triangulation 37C3
  https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/
- ARM Race condition in Translation Lookaside Buffer Invalidation (TLBI)
  https://support.arm.com/documentation/112137/1-0/
  (See CVE-2025-10263)
- HYPERVISOR compromising an hypervisor paravirtualized drivers (see CVE-2024-3446)
- HYPERVISOR Linux IPv4 / checksum metadata / TOCTOU / Guest→Host (see CVE-2026-99999)

Zenbleed-like



IMPACT

- Remote code execution
- Priviledge escalation

AMPERE

SOFTWARE-DEFINED VEHICLE SECURITY

03 –Few examples – System

SECURED BY DESIGN

HYPOTHESIS

- IVI and Perception are on same SoC
- Perception can break (AEB)

STEP 1 TESLA

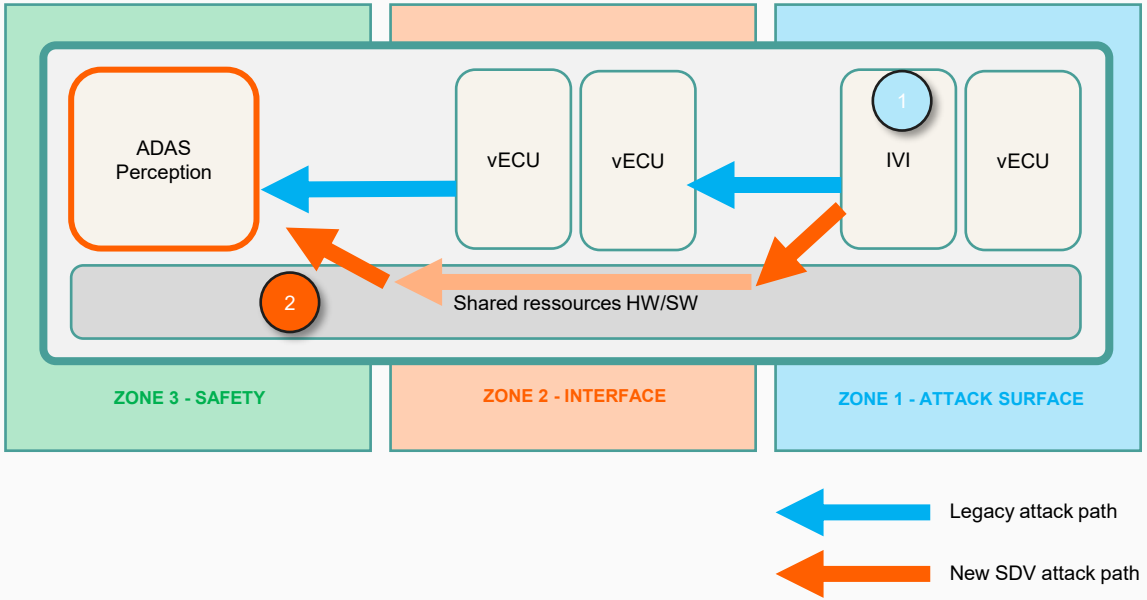
- IVI is compromised

STEP 2 ZENBLEED

- SoC is compromised

DAMAGE SCENARIO

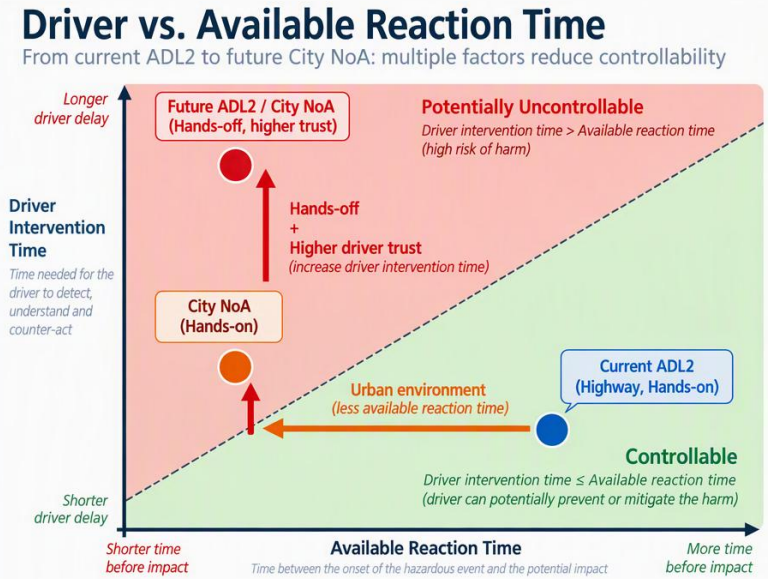
- Attacker can use ADAS functions (AEB, LKA, LCA, ELKA, ACC)



vECU: virtual ECU

SOFTWARE-DEFINED VEHICLE SECURITY

03 – E2E & NoA (navigation on autopilot)



Why does the driver take longer to intervene?

Higher trust / Overreliance
Driver initially assumes the ADAS behavior is legitimate ("Is this normal?")

Hands-off operation
Time needed to look at the road, re-engage and take control

More complex urban environments
More complex scenarios to assess (e.g. intersections, VRUs, occlusions)

Conceptual evolution of driver intervention time

Current ADL2 (Highway, Hands-on)
Baseline driver intervention time (shorter)

City NoA (Hands-on)
Longer driver intervention time than highway (due to higher trust and urban complexity)

Future ADL2 / City NoA (Hands-off, higher trust)
Significantly longer driver intervention time (due to hands-off operation and higher trust)

Current ADL2 (Highway, Hands-on)

- Limited ODD (mainly highway)
- Hands-on, attentive driver
- Longer available reaction time
- Lower driver intervention time

City NoA (Hands-on)

- Urban environment (intersections, VRUs)
- Hands-on, attentive driver
- Reduced available reaction time
- Higher scenario complexity
- Higher driver intervention time than highway

Future ADL2 / City NoA (Hands-off, higher trust)

- Extended ODD (highway + urban)
- Hands-off, higher driver trust
- Shortest available reaction time
- Highest driver intervention time
- Most challenging scenarios (VRUs, occlusions, ...)

**Urban scenarios reduce the time available, while hands-off operation and higher driver trust increase the time needed to react.
This combination decreases controllability and increases the potential impact of cyber-induced hazardous actions.**

AMPERE

SOFTWARE-DEFINED VEHICLE SECURITY

03 –Few examples – Single step

SECURED BY DESIGN

TESLA PWN2WN

- VCSec ECU is handling TPMS (tire pressure) and Key Management
- RCE with no interaction from user

STEP

- Attack VCSec sending malicious TPMS certificate

DAMAGE SCENARIO

- Attacker can open / start the car
- May have access to Safety CAN frame

VCSEC Vulnerability

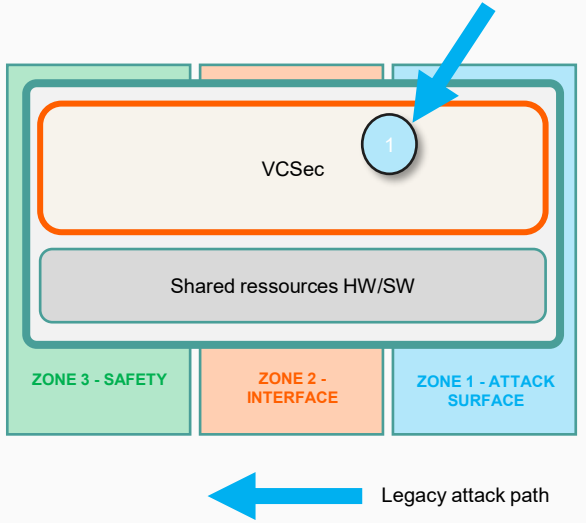
SYNACKTIV

Integer overflow in certificate reassembly

- Integer overflow in the validation of `startIndex`
- Results in Out-Of-Bounds write with a negative `startIndex`

```
char g_cert_buffer[512];

void handle_certificate_response(
    u32_t tpms_id,
    u8_t *data,                 // certificateInParts.data_.bytes
    u32_t data_size,            // certificateInParts.data_.size
    u32_t start_index,          // certificateInParts.startIndex
    u32_t certificate_size)     // certificateInParts.certificateSize
{
    // Integer overflow ex: (start_index:-8 + data_size:64) = 56
    if (data_size <= 512 && (u32_t)(start_index + data_size) <= 512)
    {
        // startIndex can be negative -> OOB write before the global
        memcpy(g_cert_buffer+start_index, data, data_size);
```



AMPERE

SOFTWARE-DEFINED VEHICLE SECURITY

https://www.synacktiv.com/sites/default/files/2024-10/hexacon_0_click_rce_on_tesla_model_3_through_tpms_sensors_light.pdf

3

ENABLERS

HOW COULD WE SOLVE THEM ?

04 – Enablers – Shared HW/SW

SECURED BY DESIGN

- **Before SDV** Attack path between ECU = Network communications (←)
- **SDV:** + Shared Ressources (←)

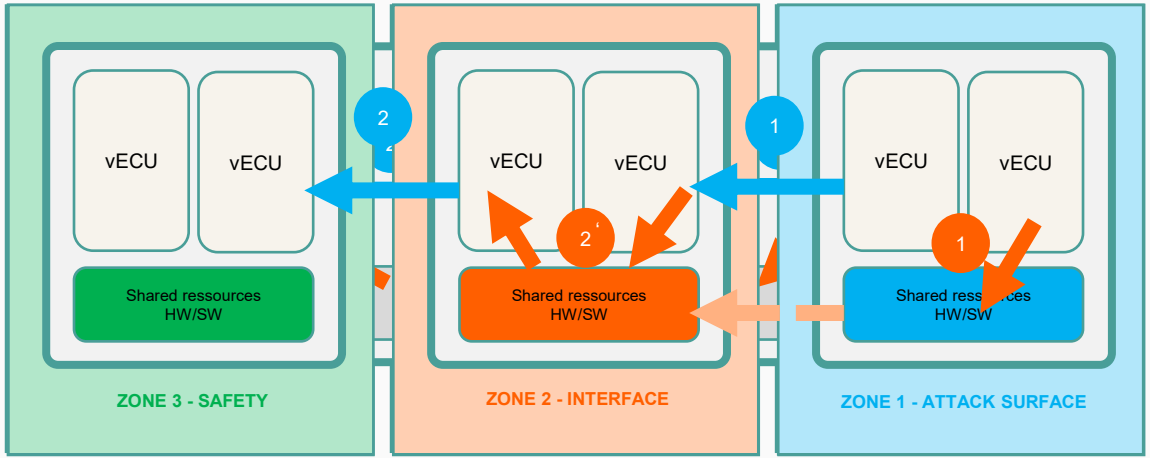
Reduce sharing at system level : dedicated HW/Zone

NO WAY TO ENSURE NO SPOF

- SoC + Hypervisor + SW

LIMIT SHARING AT SYSTEM LEVEL

- ANSSI recommendation in IT domain: no sharing between different zones
- Possible automotive policy:
  - Dedicated HW for each Zone
  - No more than two contiguous Zone on the same HW



SOFTWARE-DEFINED VEHICLE SECURITY

04 – ENABLERS – SHARED HW/SW

REDUCE SINGLE POINT OF FAILURE PROBABILITY

- Main contributors:
  1. SoC HW & BSP
  2. Hypervisor SW
  3. Hypervisor configuration
  4. Shared components (Boot rom, HSM, ect, paravirtualized drivers)
  5. Applications with cross VM communication

CROSS VM COMMUNICATION

- Isolation is important
- But useless if VMs exposed unprotected backdoors or high vulnerabilities
- Demonstrated in Blackhat UK 22*

*https://i.blackhat.com/EU-22/Wednesday-Briefings/EU-22-Serdyuk-Back-connect-to-the-connected-car.pdf

ENSURE ENABLER SECURITY LEVEL

- Request SESIP4 for hypervisor SW (2)
- Request SESIP4 for paravirtualized drivers (4)
- Request SESIP4 for SoC+BSP (1,4)

Ensure enabler security level including pentest

Responsibility T2s

ENSURE STRONG ISOLATION

- Request SESIP4 for ECU specific configuration(1,2,3,4)

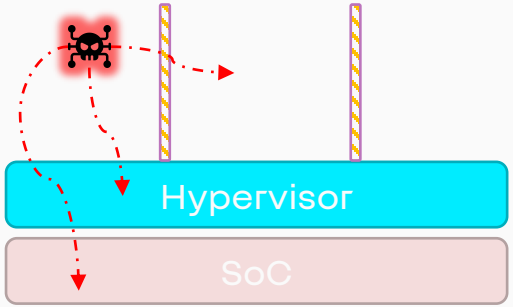
Verify isolation in final product/configuration

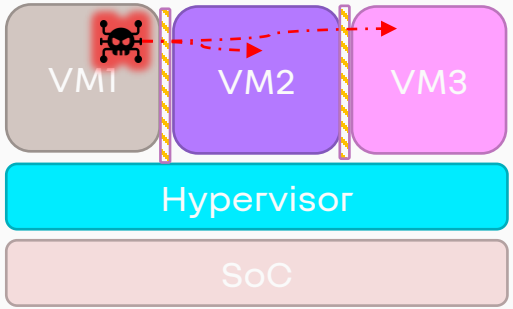
Responsibility T1

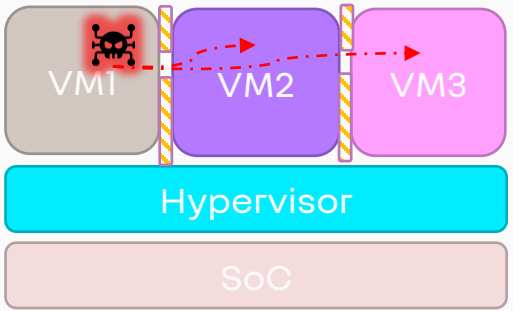
ATTACK SURFACE REDUCTION

- Review privilege allocation (which API)
- Coding guidelines (ie input sanitization, rust)
- Pentests for Application with cross VM communication (5)

Responsibility OEM







04 – Certification Scheme

We are developing a **SESIP-based certification model.**

We are ready to share this work within a GP WP to help standardize a **Protection Profile.**

SOFTWARE-DEFINED VEHICLE SECURITY

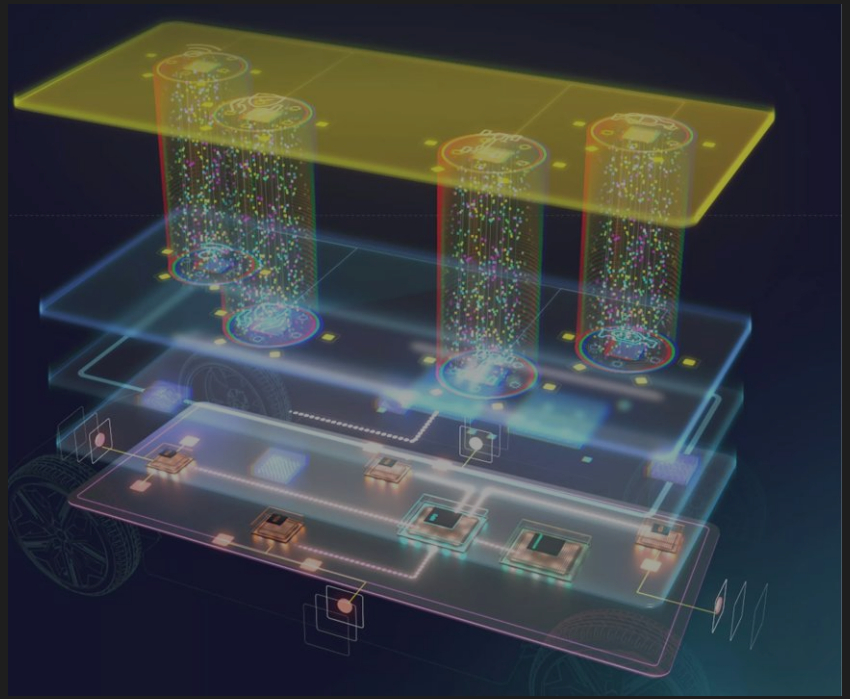
4

CONCLUSION

WHAT IS NEXT?

05-CONCLUSION
WHAT IS NEXT

- Risks are important
- Needs for a standardization
- What about a converged protection profile ?



AMPERE

THANK **YOU**

AMPERE.CARS