PROVING FREEDOM FROM INTERFERENCE

PROVING MIXED-CRITICALITY ISOLATION

FRÉDÉRIC AMEYE, HEAD OF SW ARCHITECTURE

GLOBALPLATFORM CVF MUNICH · 21 OCTOBER 2026

Roleplay time.

You have to sign off a missile launcher

one internet-facing service,

one piece of software that can fire

© 2026 Renesas Electronics Corporation. All rights reserved.

Three ways to host a missile launcher

Same two workloads, three very different amounts of sharing

A Shared everything

Internet VM
web, mail, updates

Launch VM
fire control

Shared PV drivers / backends

Shared hypervisor

One server: CPUs, caches, DRAM, NIC

Cost **Low**
Isolation **Weakest**

B Separate boxes, one site

Internet server
own OS, own HW

Launch server
own OS, own HW

Shared:
network, admin console, power, building

Cost **Medium**
Isolation **Better**

C Air gap, different vendors

Site 1
vendor X hardware

air gap

Site 2
vendor Y hardware

Shared:
people and supply chain only

Cost **Very high**
Isolation **Strongest**

Nobody can afford C in a car.

© 2026 Renesas Electronics Corporation. All rights reserved.

What's shared is what's attackable

Shared element	A	B	C
Software trust base: hypervisor, PV drivers	Shared	Separate	Separate
CPU caches, interconnect, DRAM bandwidth	Shared	Separate	Separate
DMA masters (NIC, GPU) and who programs them – SMMUs configs	Shared	Separate	Separate
Network, config and update path	Shared	Shared	Separate
Power, clock, building	Shared	Partly	Separate
Hardware vendor and supply chain	Shared	Shared	Separate

High-Assurance

= what you removed
+ evidence that it stays removed
in the shipped image

© 2026 Renesas Electronics Corporation. All rights reserved.

Why most SoCs take road A

The easiest way to merge automotive needs with smartphone and cloud product lines

Cockpit / IVI

- Android, app store, browser
- LTE, Wi-Fi, Bluetooth
- Weekly OTA updates
- QM: no safety claim

ADAS / vehicle control

- Perception, planning
- Braking, steering commands
- Hard real-time deadlines
- ASIL B to ASIL D

Road A: one hypervisor

- Same silicon as the phone or server line
- Same hypervisor, two more VMs
- Isolation becomes a config file

What could go wrong?

Can a single SoC give you architecture-B isolation, and can the OEM prove it on the shipped image?

© 2026 Renesas Electronics Corporation. All rights reserved.

Are hypervisors enough?

Same with containers. But worse.

© 2026 Renesas Electronics Corporation. All rights reserved.

Why a hypervisor can't guarantee FFI

3

hypervisors escaped guest-to-host in one week at Pwn2Own Berlin 2025

>1 yr

an ESXi VM-escape chain was used in the wild before disclosure (2025)

1. **One software TCB for every domain**

   Existing vulnerabilities: ESXi (2025), Hyper-V vSwitch (CVSS 9.9), QEMU VENOM.

2. **Safety VM depends on cockpit-facing code**

   Paravirtual backends and shared drivers are in the critical path.

3. **Interference happens below the hypervisor**

   Caches, interconnect and DRAM bandwidth are not scheduled by it: temporal FFI is hard.

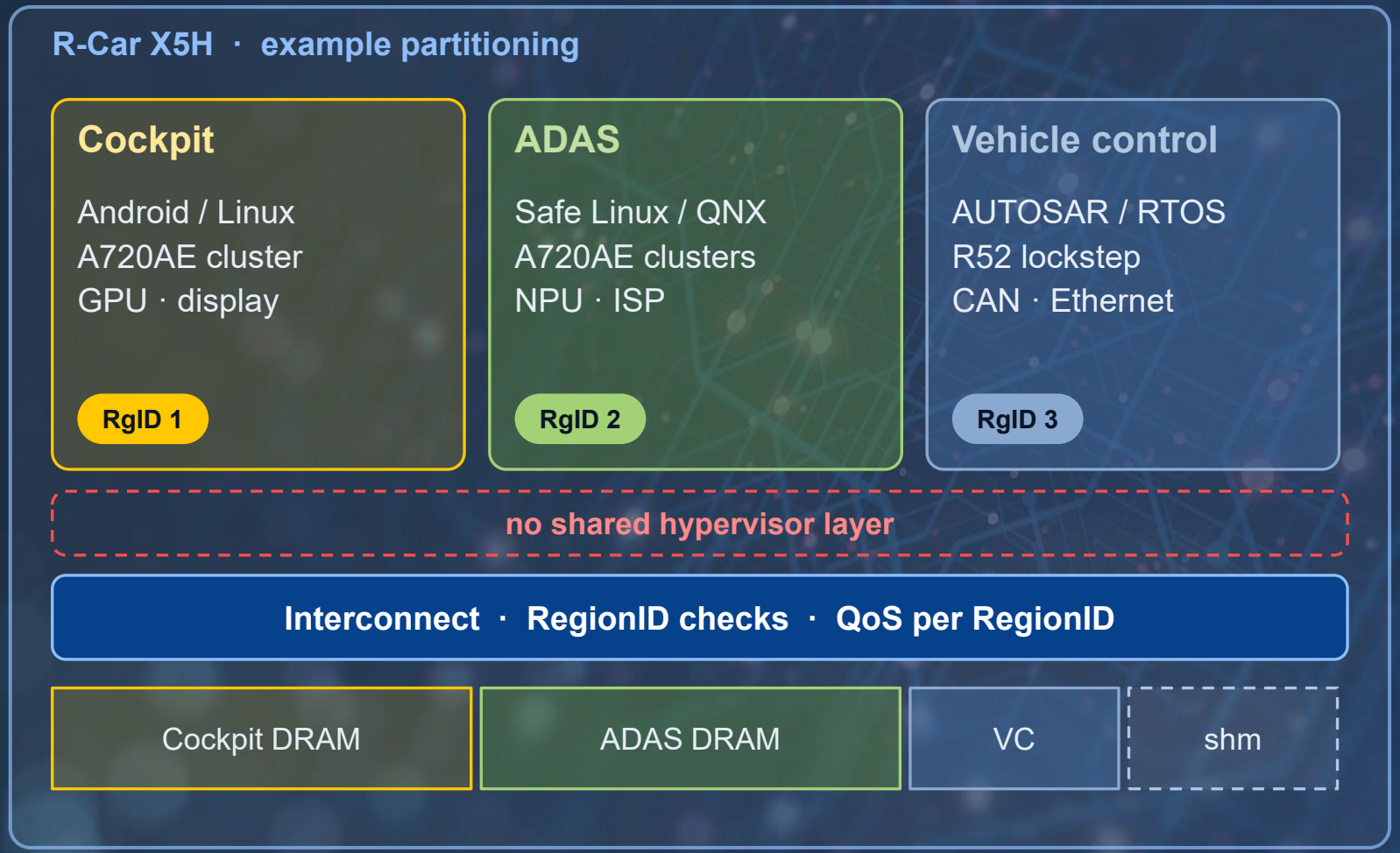
4. **DMA protection is only as good as its owner**

   The SMMU is programmed at runtime by the hypervisor. Compromise it and every DMA master can corrupt safety domain.

Sources: ZDI Pwn2Own Berlin 2025 (ESXi, Workstation, VirtualBox); CVE-2025-22224/22225/22226 (CISA KEV); CVE-2021-28476; CVE-2015-3456; M. Bechtel, H. Yun (Univ. of Kansas)

© 2026 Renesas Electronics Corporation. All rights reserved.

Hypervisorless ADAS + Cockpit fusion



1 **Least amount of shared SW**

No hypervisor or PV backend in the safety TCB.

2 **Boundaries in hardware**

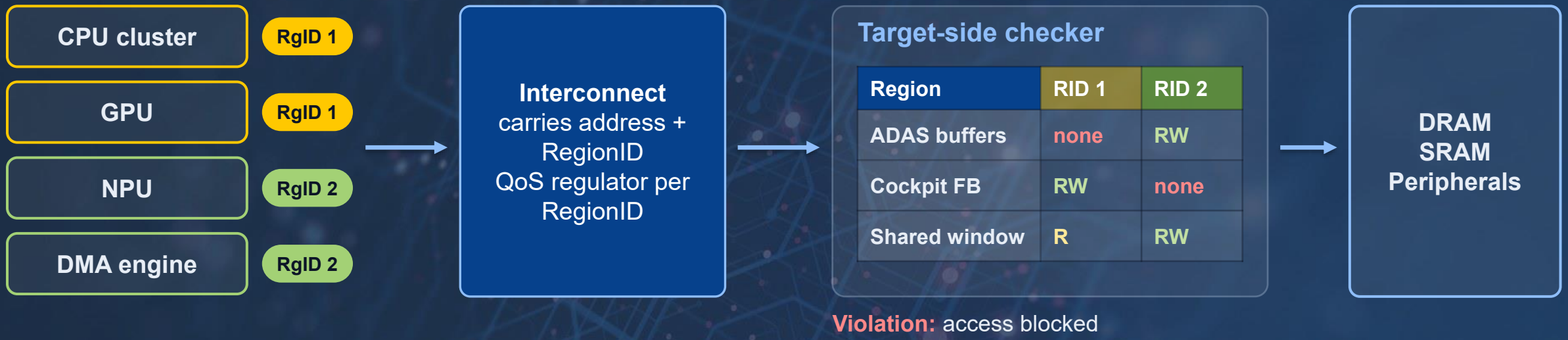
RegionID tags every access; memory, peripherals and bandwidth are checked per domain.

3 **Explicit channels only**

Domains talk through declared shared-memory windows with fixed access rights.

© 2026 Renesas Electronics Corporation. All rights reserved.

RegionID: every access carries its domain



Unforgeable

Software inside a domain cannot change the RegionID its accesses carry.

Checked at the target

Independent of the initiator's MMU or page tables: a corrupted kernel gets blocked access.

Spatial and temporal

The same tag drives memory protection and bandwidth QoS.

Across chiplets

RegionIDs mapped and carried over UCIe and PCIe SR-IOV.

© 2026 Renesas Electronics Corporation. All rights reserved.

What can the attacker do?

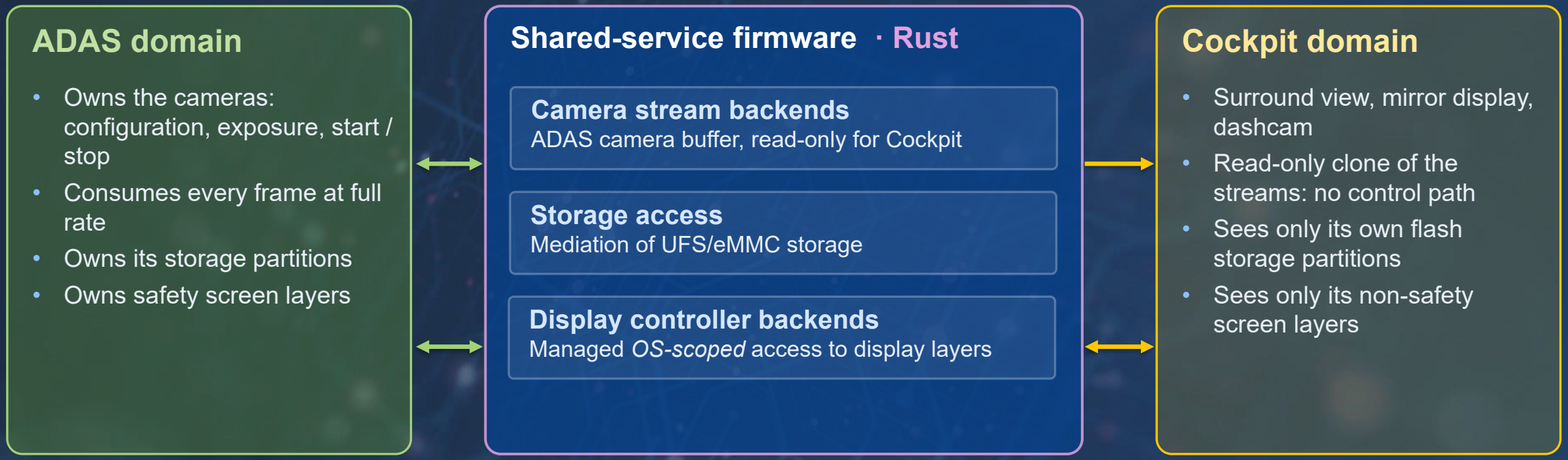
Attacker has root access in the cockpit partition. What can he do?

Attack from the cockpit	Hypervisor-based	RegionID, hypervisorless
Program GPU / DMA to overwrite ADAS memory	**Exposed** if SMMU config is wrong or rewritten	**Contained** blocked at target, no RW right
Exploit hypervisor or PV backend	**Exposed** all VMs, VENOM-class	**Contained** no shared hypervisor to exploit
Flood DRAM to make ADAS miss deadlines	**Exposed** not scheduled by the hypervisor	**Contained** bandwidth bounded per RegionID
Rewrite the isolation configuration	**Exposed** held by runtime software	**Contained** locked at early boot
Malformed messages to a shared service	**Residual** validate the protocol	**Residual** memory-safe Rust backends
Cache and DRAM timing side channels	**Residual** shared silicon	**Residual** to **Contained**

© 2026 Renesas Electronics Corporation. All rights reserved.

What still has to be shared

Sharing still happens to improve system efficiency & cost



Ownership stays with ADAS

The cockpit can watch, never steer the camera

RegionID still applies

The firmware only reaches its declared windows

Tiny trust base

No OS, no hypervisor: a few services only

Memory-safe code

Rust closes the classic RCE paths

© 2026 Renesas Electronics Corporation. All rights reserved.

From partitioning intent to proven image

One source of truth across the V-cycle: declared once by people, generated and verified by machines

1 Declare source of truth

Safety & security engineers

At project start: domains, masters, regions, rights, budgets

2 Generate

Automatically, from step 1

Injected into the build system. No hand edits, no human mistakes.

Build & integrate

Hundreds of contributors, years

Many teams change the software; one final signed image

3 Verify the image

Automatically, against step 1

Not against step 2: every master-to-target path in the image

Verified against the source of truth, never against generated output

4 Evidence

For assessors and the OEM

ISO 26262 / 21434 work product, rerun in CI on every release

A machine-enforceable contract

No human step between the platform model and the shipped image.

```
$ ffi-check fusion.img model.yml
  declared paths ...... 318 OK
  undeclared paths ..... 0 OK
  QoS budgets ........... OK
PASS: image conforms to model
```

Illustrative output

© 2026 Renesas Electronics Corporation. All rights reserved.

Don't trust. Verify.

Next: remote proof that every device in the field
still enforces the safety partitioning it was designed for.

Patent pending · mechanism not disclosed today

© 2026 Renesas Electronics Corporation. All rights reserved.

Three questions to ask chipmakers; and a GP roadmap

1. **What is shared?**
2. **Where is it enforced?**
3. **Can I prove it?**

Call to action: a certification profile

to harmonise practices and grade the security level of a shared platform, based on:

- How the hardware is shared between domains
- How the isolation mechanisms are tested by security researchers
- How the tooling prevents configuration mistakes

A natural fit for GlobalPlatform and SESIP.

thank you

frederic.ameye.vz@renesas.com

© 2026 Renesas Electronics Corporation. All rights reserved.