Trusted Execution Environment in Automotive Critical ECUs

The rise of connected vehicles has significantly increased the exposition of vehicles to remote attacks and then the need to strengthen the security level of connected systems. While this security issue for cyber-physical systems is shared with other industries, the automotive industry has to meet a very high level of security with a very strong constraints on costs in order to maintain its competitivity. One way of reaching this goal is to use all the potential of existing hardware.

This path has already been followed through the use of built-in hardware root-of-trust features (such as fuses, authenticity verification of the bootloader, hardware coprocessors) of the System-on-Chip (SoC) deployed in the ECUs and the use of hypervisors, which virtualize processors and allow to execute several systems on the same ECU. However, ECUs currently lack software root-of-trust features, that cannot be brought by the Operating Systems executed on top of the hypervisor nor by the hypervisor itself, which are too complex to be certifiable at the expected level of security.

The solution proposed in the CTI project is to rely on the ARM® TrustZone® feature available on most of modern SoC. TrustZone® provides a hardware-based isolation between a Normal Word, where the current automotive software stack will continue to reside, and a Secure World for a software root-of-trust where a secure OS will execute applications. This software root-of-trust concept is also known in the mobile industry as a Trusted Execution Environment (TEE) and is massively deployed. The key difference with the mobile industry is that in the automotive case, the TEE needs to

be able to resist to sophisticated remote attacks to protect critical properties such as the car's safety: the TEE for the automotive industry needs therefore to be as close as possible to zero defects and in as much as possible certified at a high level of robustness.

This approach has been illustrated in the CTI project with the use of ProvenCore, an ultra-secure OS (TEE) developed at ProvenRun that is available for ARM® Cortex®-A, Cortex®-M and RISC-V processors. ProvenCore is a micro-kernel OS that ensure strong and proven isolation properties between the Normal World and the Secure World as well as between applications in the Secure World. Hence the execution and data from ProvenCore and each application in the Secure World cannot be tampered and are fully protected.

In the context of the CTI project, ProvenCore has been deployed on the ECUs that are critical for the security on the vehicle reference architecture, as illustrated in Figure 1. These ECUs are:

V1.0 15/03/2021

En partenariat avec :

En collaboration avec :

- The Communication Unit and Electric Vehicle Charger Controller (EVCC) as they offer direct communication interfaces accessible from outside the vehicle.
- The Bastion, or central gateway, as it is the hotspot for internal car communications within the vehicle and also acts as a firewall between the subnetwork with external communication interfaces and subnetworks with safety-critical ECUs.
- The Multimedia and Navigation system, or infotainment system, as it supports a very large codebase prone to many vulnerabilities.

deployed as ProvenCore applications, could be offered on-demand:

- Secure boot, to extend HW authenticity verification of the bootloader to any other executable code on the ECU.
- Secure firmware update, to support secure update of any executable code of the ECU even if an OS from the Normal World is corrupted.
- Secure storage of credentials, configuration files, logs or any other sensitive data, to protect this data from tampering attempts from any other application or OS.

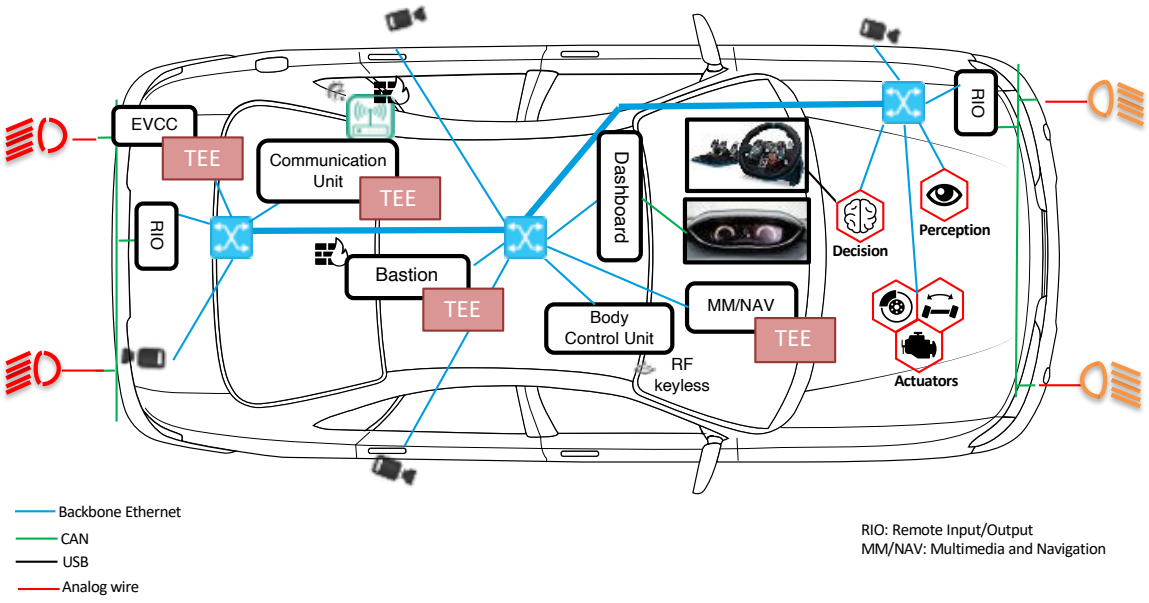

Figure 1: CTI reference architecture for connected car

ProvenCore has shown to be highly portable, as it could be executed on the six hardware platforms and the two Normal World OS used in the CTI project.

Leveraging on this robust software root-of-trust, a wide-range of security services,

- Cryptographic services, or virtual HSM, to any application of the ECU, based on credentials on the secure storage.
- Network firewall and network filter, with the ability to have exclusive access to network peripheral, to ensure that the network security policy

cannot be circumvented from the Normal World.

- Network authentication, to authenticate the ECU, other vehicle ECUs or remote systems based on credentials on the secure storage.
- Network IDS, to detect abnormal network activities and trigger reaction, such as reporting them to a Security Operational Centre (SOC).
- Host IDS, to detect abnormal activities or events from the OSes in the Normal World and trigger reaction, such as reporting them to a SOC.
- Secure communication (VPN), to establish a trusted channel between ECUs or with external systems, based on credentials on the secure storage.
- Recovery OS, to ensure continued access to the ECU and provide a fail-safe mode, even if the OSes in the Normal World are no longer responsive.

This list is not limitative, as other services could benefit from a software root-of-trust, such as payment services for the EVCC or tolls, or DRM for the infotainment system.

The CTI project has shown the potential for security services supported by a TEE, in terms of security, flexibility, portability and compliance to the automotive constraints. The approach is now mature enough to be industrialised in modern connected vehicle ECUs and answer to the security needs of the automotive industry.

QorIQ LS1021A, LS1043A, i.MX6
XILINX UltraScale+ MPSoC
RENESAS R-Car H3
Rockchip RockPro64

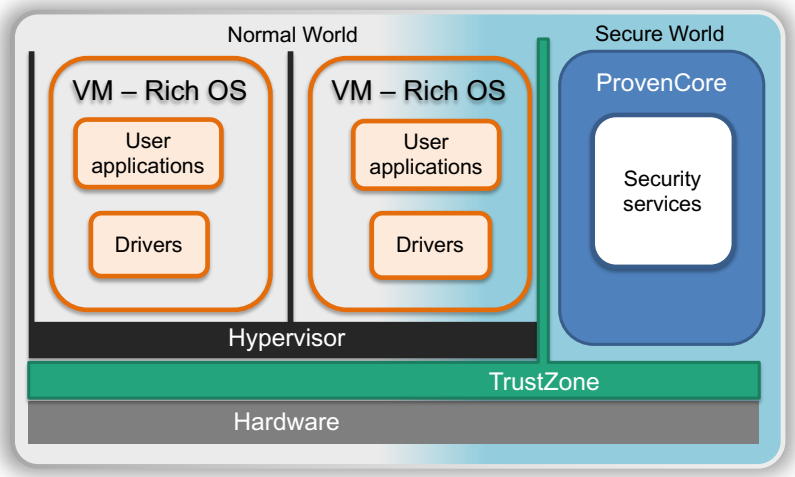

Figure 2: ECU software architecture with TEE with supported platforms for CTI project