Open Source Based Safe and Secure Platform for Cost-Efficient V2X Implementations

Key requirements:
* Respond to new digital threads created by connectivity with special attention to privacy, public acceptance
* Control access to most critical assets: CAN and V2X radios
* Ensure that system is operational even in case of security breaches and critical information is displayed correctly
* Create new kind of connected car applications that integrate information across displays and inputs
* Provide developer friendly and attractive platform

Solution:
* Layered security model relying on ARM TrustZone and Fiasco.OC contains threats
* Small TCB allows rigorous verification of the secure environment. Even formal verification is possible.
* Real-time capable Core Operating System for creation of mission critical applications, such as instrument clusters or vehicle controls
* Mainstream Mer/Nemo based Linux as Rich OS for infotainment applications

V2X radio and CAN controller access:
* Connectivity offered as service that prohibits arbitrary messages
* Protocol stacks implemented in the Secure OS
* Similar design used in cellular modems of the smart phones

Example Applications:
* V2X information: Critical message delivery can be ensured through the instrument cluster. Additional information can be provided for applications in the Rich OS.
* Cruise control with multimodal output: Implementation in the Core OS and handling of controls. Information available for applications in the Rich OS.
* 3rd party road toll payment application: V2X communication frontend in Secure OS and payment frontend in Rich OS.