TAPPS

Trusted Apps for open CPSs

Secure platform for EV control systems

ENERGICA

Giovanni Gherardi and Electronic Development Team

Co-funded by the Horizon 2020 Framework Programme of the European Union under grant agreement no 645119

The Energica Project

- The Energica project started in 2010 in Modena Italy, by CRP Group.
- In 2012 CRP presented at Eicma the running prototype of Energica and in 2013 launched the first model Ego.
- Energica Motor Company SPA was officially founded in 2014 with the aim of creating high-performance sustainable motorcycles. Energica concept came from eCRP 1.4, the runner-up World Champion and European Champion electric racing motorcycle.

The Energica Project

- Power > 100Kw, Torque 195Nm
- Acceleration: 0-100Km/h <3 seconds
- Max speed: Self limited to 240Km/h
- PMAC oil-cooled motor
- Water Cooled Motor Drive
- No gearbox/clutch
- Straight Gear primary Transmission, Chain final.
- Bosch ABS system
- Lithium-polymer batteries (range 120-200 km)
- 3Kw 110-220V on-board battery charger plus Mode 4 DC Fast
- Charge Interface for EU and USA (CCS)
- Digital dashboard (4.3 inches TFT color display)
- Bluetooth 2.1 + 4.0 (Bluetooth Low Energy)
- Advanced Battery Management System

Power Management

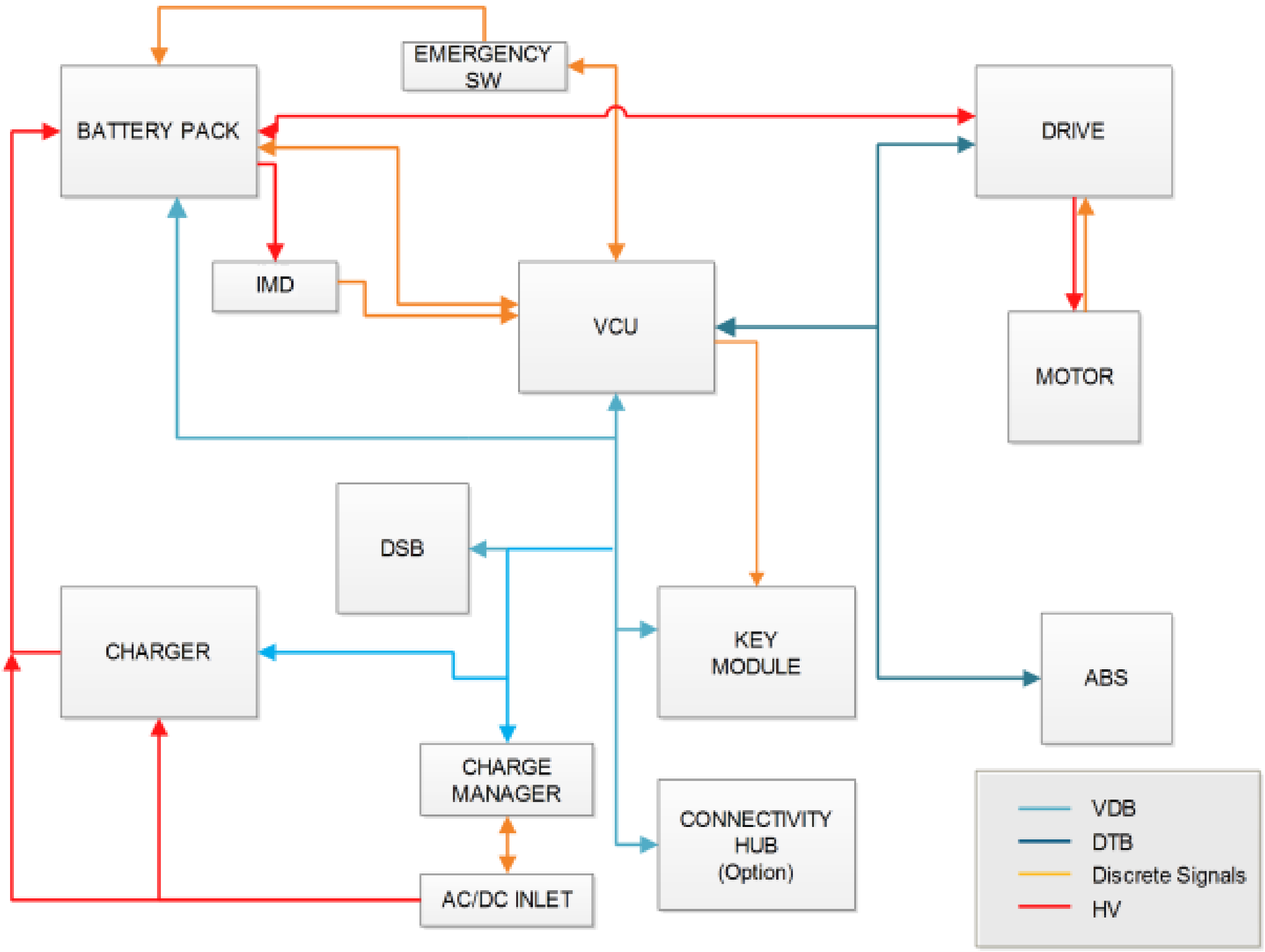
Energica has no 12V Lead Acid Battery. All 12V loads are driven by a Military Grade 600W 12V isolated DC-DC Converter (PSU). Energica PSU integrates a secondary 12V Low Power Always On DC-DC that powers wake up circutry.

- Weight and Space Saving
- Enhanced Energy Efficiency
- Possibility to extend storage time and keep monitoring RESS

Special care needed for Vehicle Power Management:

- Wake on CAN!!!!
- No ECU are allowed to drive stand-by power except for those responsible of waking up the vehicle
- Not directly compatible with ready available automotive electronics

Vehicle Electronic System Architecture



Intrinsic Security Risc

The system is completely automated and procedures and devices like:

- Power On/Power Off sequence
- High Voltage Supply routing
- Brakes and electric braking
- DriveByWire system for torque control
- Front beams

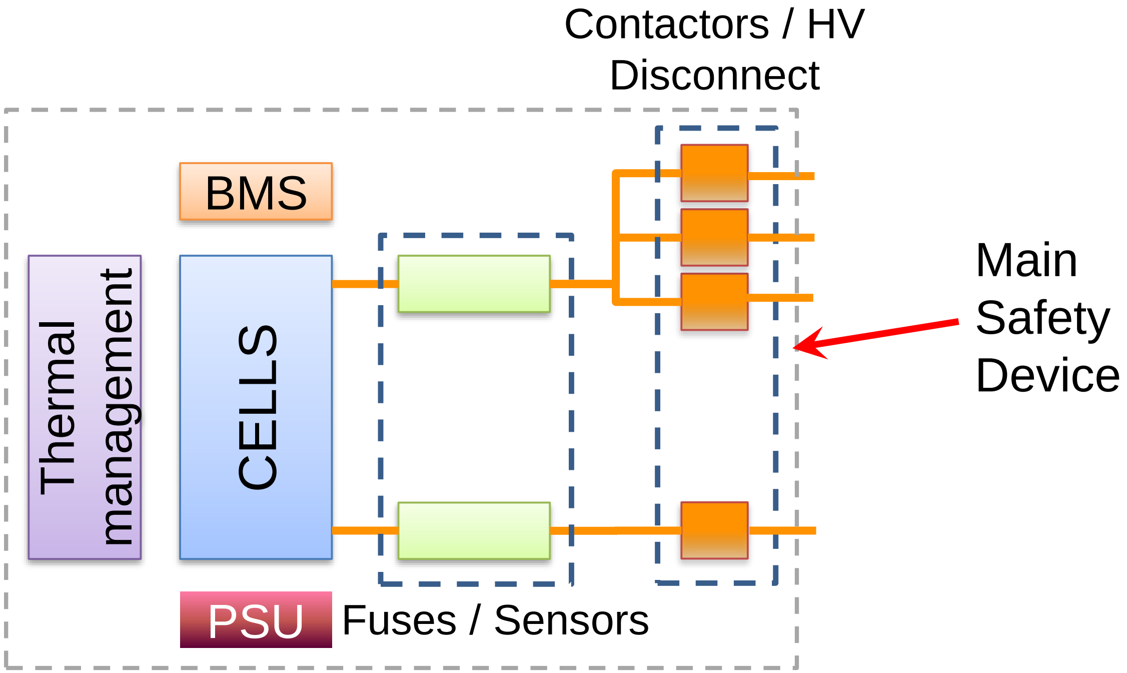
are controlled by software, accordingly, is the perfect CPS for a potential attack. Powertrain has a fixed gear with no clutch (no meccanical disconnection possible).

Malicious software could potentially take the complete control of the vehicle.

SECURITY ENFORCEMENT IS THEREFORE MANDATORY FOR USER SAFETY!!!!

Safe State

Simplified RESS Block Diagram



VCU

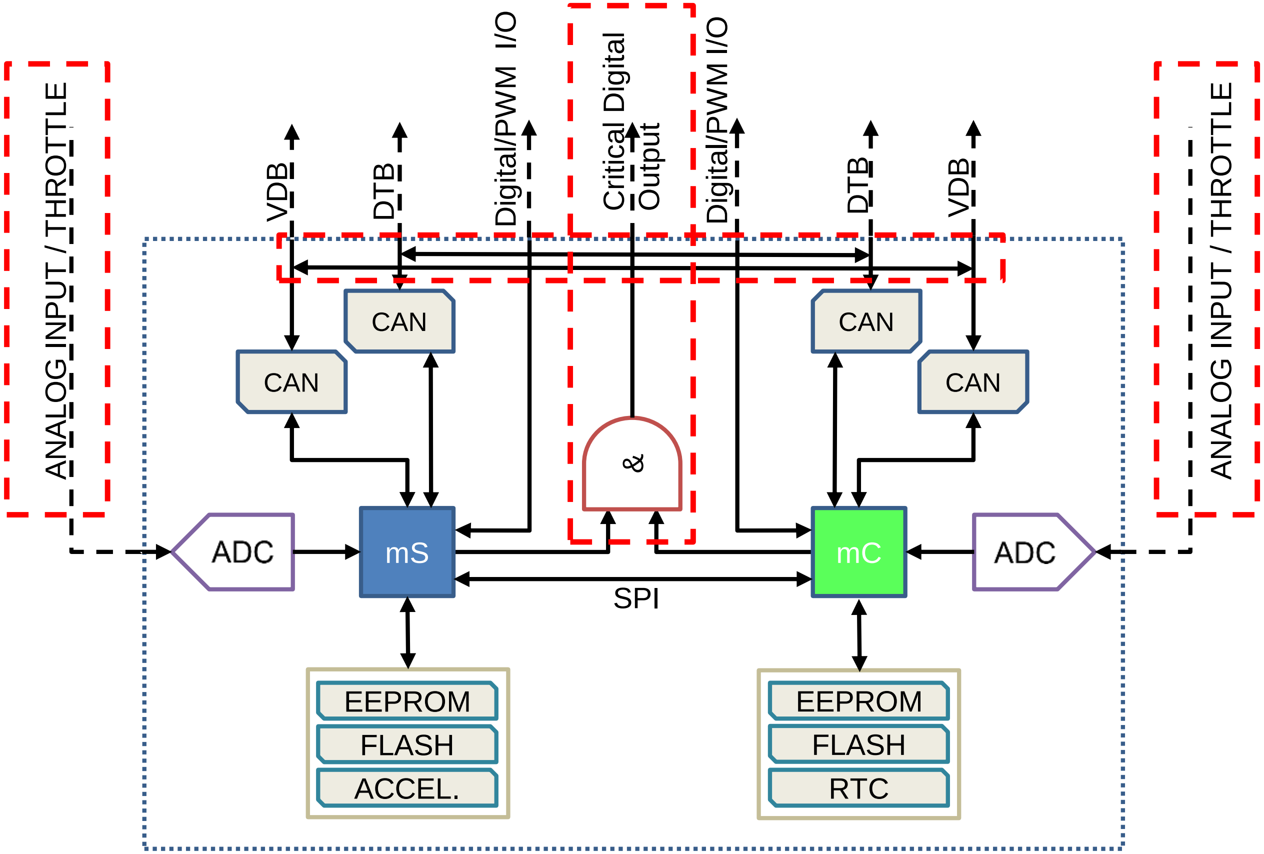
Energica Vehicle Control Unit: role and capabilities

- Responsible for Energy Storage Management and Supervision (Including Charge Control)
- Implements DriveByWire functionalities and algorithms
- Implements System Safety and Functional Safety (Hardware and Software Redundancy)
- Implements Extended On Board Diagnostic (for Vehicle and sub-systems)
- Implements User interface
- Capable of data logging

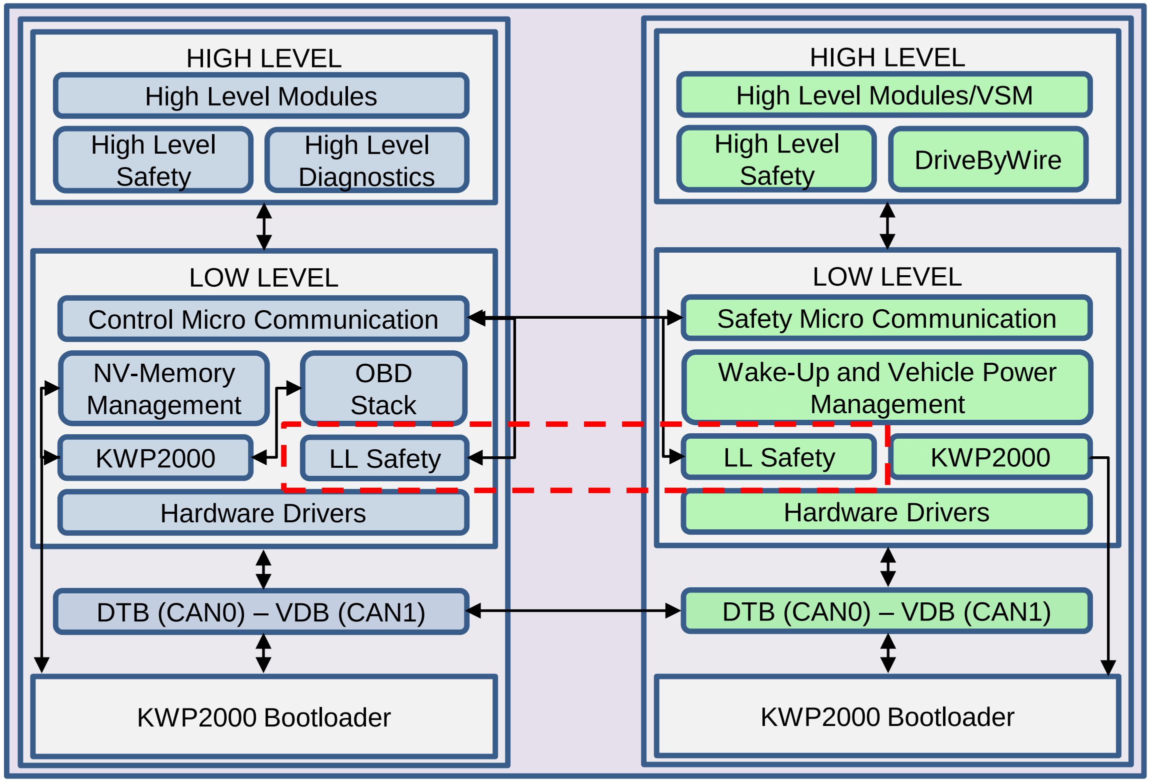
First look: Performances and Architecture

- Based on two ARM Cortex M3 (Safety Micro and Control Micro)
- Equipped with RTC, 3-Axis Accelerometer, 128Mb of Flash Memory
- Capable of handling a big CAN Dictionary (about 2100 symbols)
- Equipped with four 500Kbit/s CAN transceivers to drive VDB and DTB Buses (acting also as gateway between two Buses).
- Twelve dedicated ADC (6 on uS and 6 on uC) for throttle control for hardware and software redundancy and fault detection

VCU Hardware Architecture



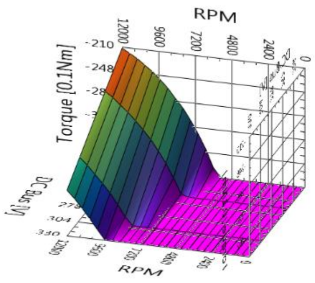
VCU Firmware Architecture

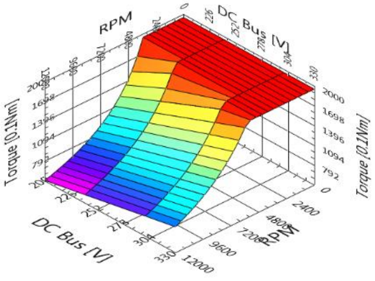


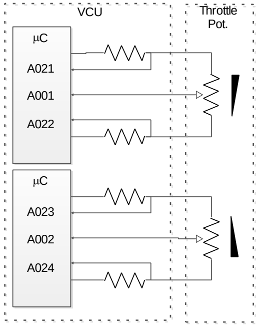
DriveByWire Safety

Energica DriveByWire:

- Complex and redundant ADC Hardware (2 ADC, 12 ADC Channels on two different microcontrollers).
- Two different micro executing different code to process analog readings
- Direct connection with low level safety module -> Fast HV Disconnect
- Fast control loop (less than 10ms time response)
- Connection with ABS system for optimal electrical braking







Upcoming Security Devices

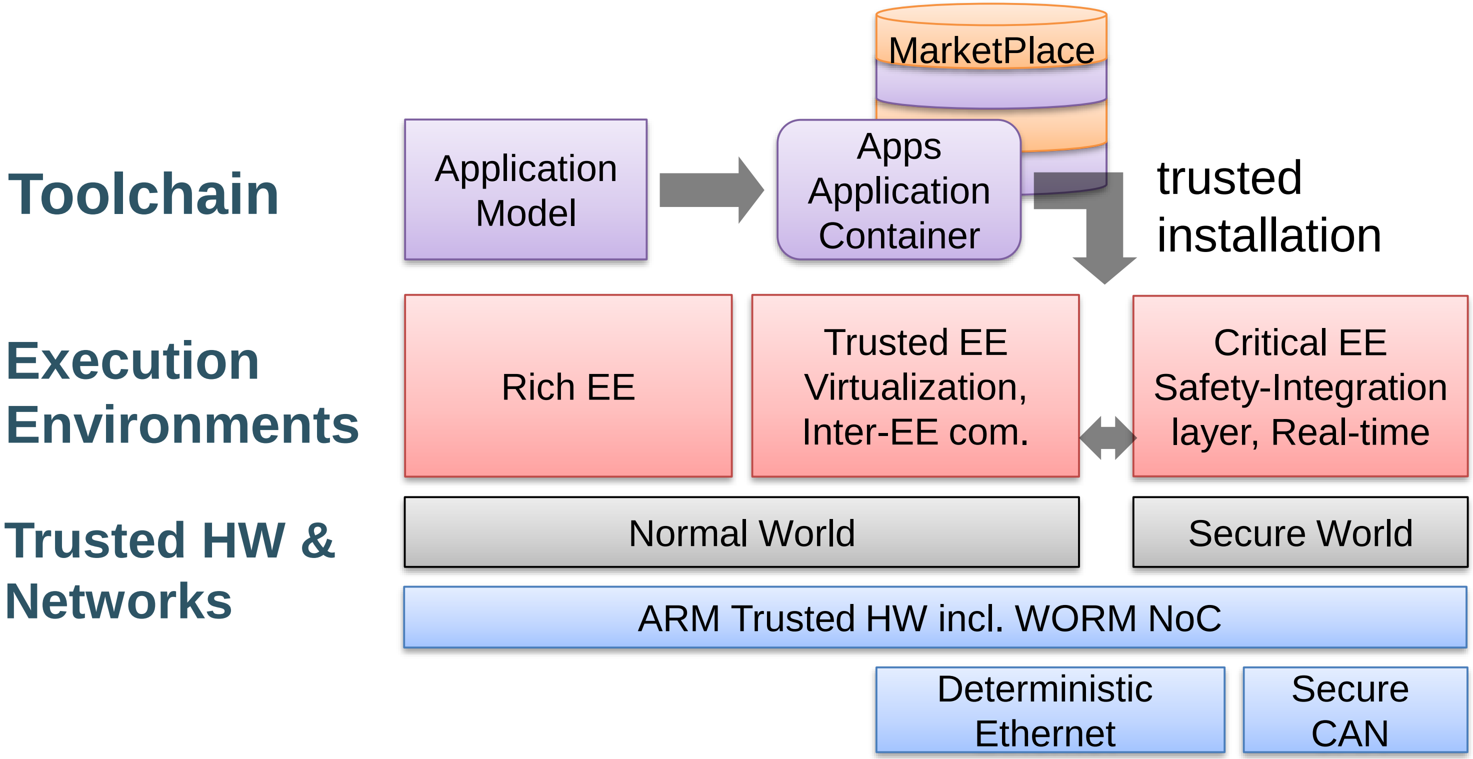
Preventative measure adopted are quite effective to prevent unwanted behaviour of the system and protect it from a physical attack in a closed environment but they are not enough to expose the system to the outside world.

In order to implement advanced connectivity and infotainment functions, Energica needs to allow execution of “feature rich applications” coming from an untrusted domain.

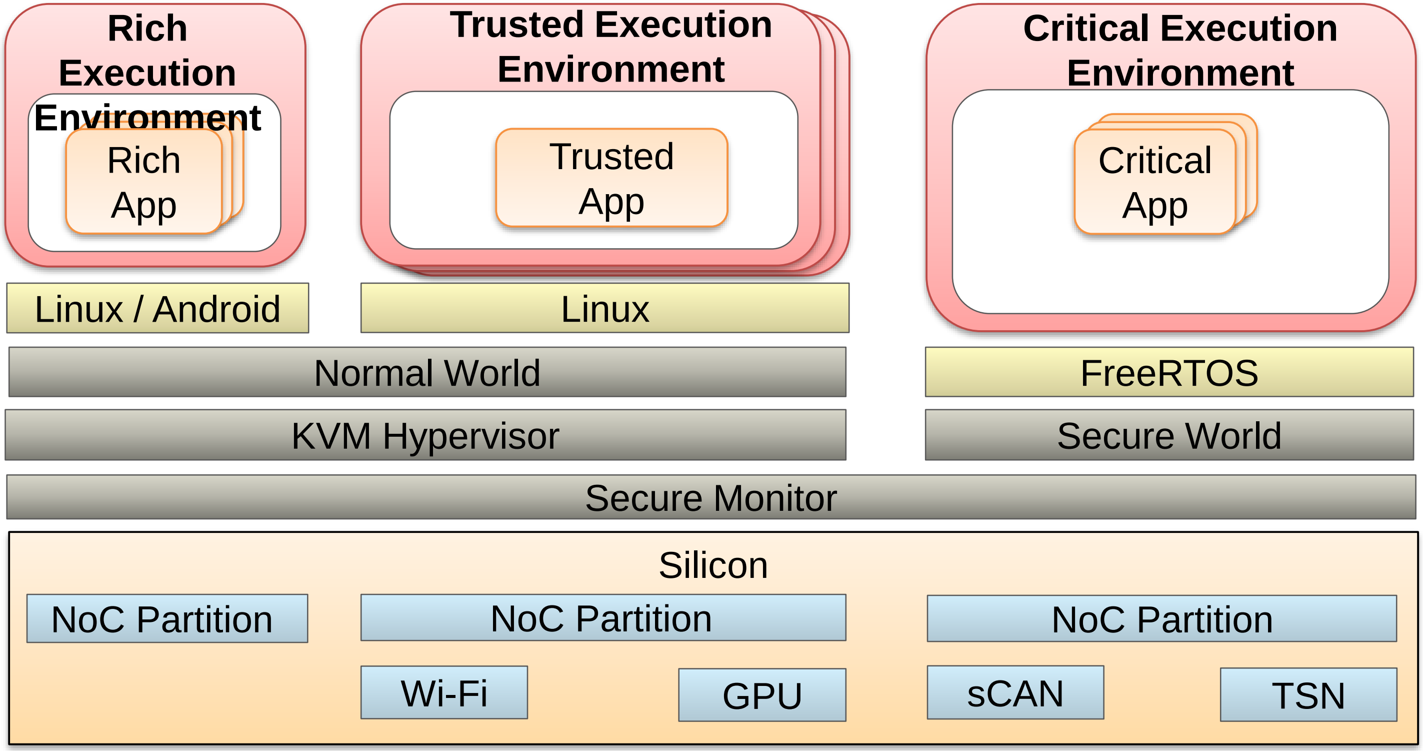
These two direction are normally in contrast with enforcing System Security. Energica is doing both by:

- Adoption of TAPPS architecture
- Replacing standard CAN Bus with sCAN (Secure CAN)

TAPPS Architecture

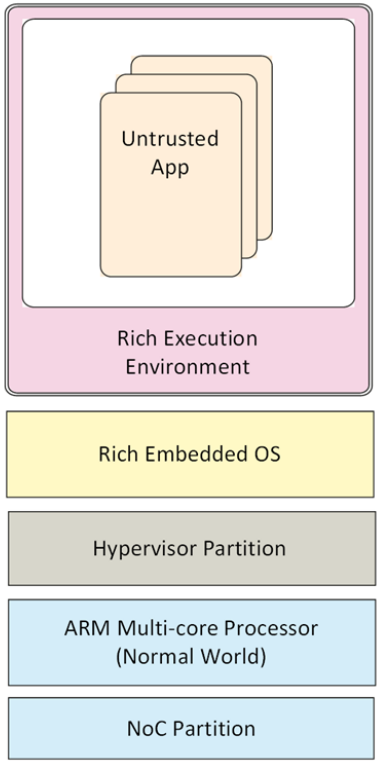


TAPPS Architecture



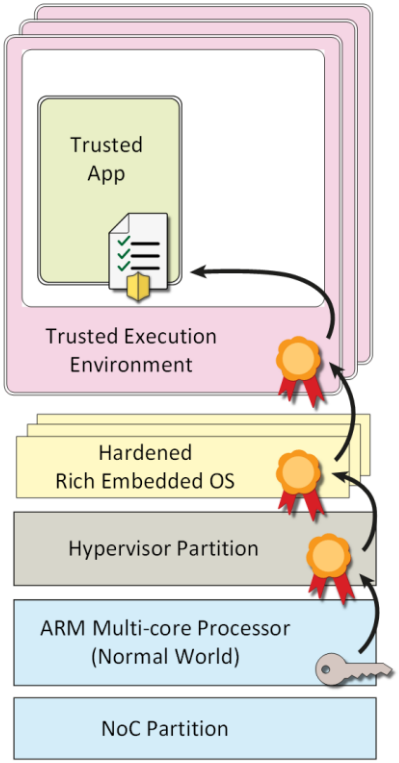
TAPPS Architecture Untrusted Applications

- Standard Application like those known from todays Smartphones
- No special means of protection on the application layer
- Separated in a Network on Chip (NoC) and Hypervisor partition


Untrusted App
Rich Execution Environment
Rich Embedded OS
Hypervisor Partition
ARM Multi-core Processor (Normal World)
NoC Partition

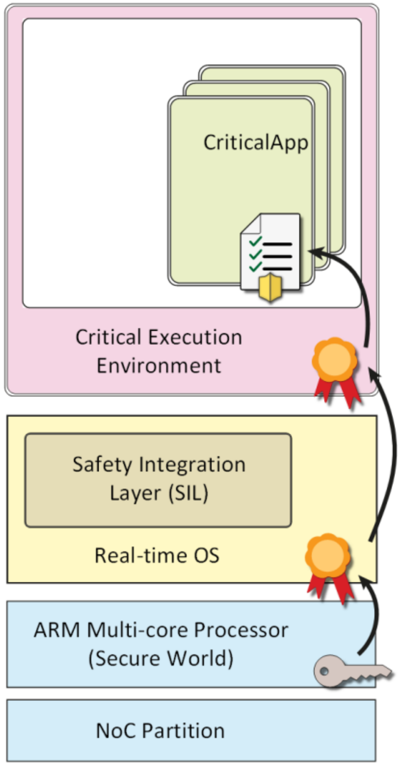
TAPPS Architecture Trusted Applications

- More trustworthy applications
- Capable to interact with critical functions of the system
- Each T-App is separated in its own execution environment in its own Hypervisor partition
- Additional hardware security through NoC partition


Trusted App
Trusted Execution Environment
Hardened Rich Embedded OS
Hypervisor Partition
ARM Multi-core Processor (Normal World)
NoC Partition

TAPPS Architecture Critical Applications

- Most trustworthy Apps with critical or real-time requirements
- Separated in the NoC and the ARM TrustZone (secure world)
- Running on top of a real-time operating system

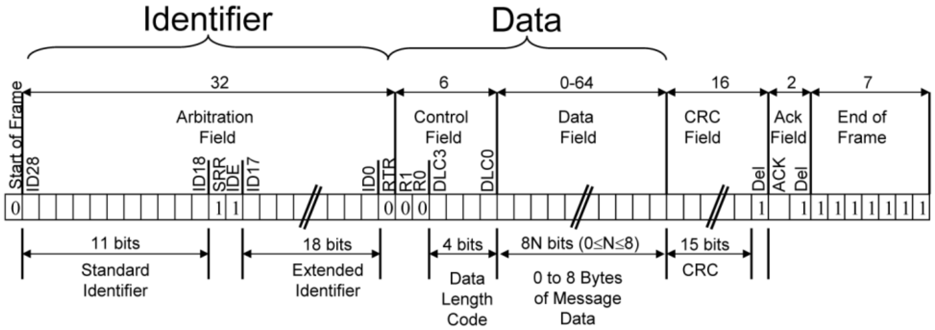

CriticalApp
Critical Execution Environment
Safety Integration Layer (SIL)
Real-time OS
ARM Multi-core Processor (Secure World)
NoC Partition

sCAN (secure CAN)

Standard CAN Bus:

- Standard CAN is “data centric”
- Frame ID represents just the “Key” to decode the message
- In standard CAN sender is unknown

- Once malicious software is running in one ECU, the malicious software “trusted” by all the other ECUs.



sCAN (secure CAN)

- Secure CAN is based on the encryption of part of the Frame ID and Payload of a standard CAN frame
- The encrypted Cyphertext generated is transmitted on standard CAN BUS
- Secure and Standard Frames can coexist on the same bus
- Ultra-light weight, sCAN can encrypt CAN (and LIN) messages in real time (less than 1ms)
- Standard CAN Frames Priorities granted.
- Implementable as software or directly on-chip inside transceiver.

Conclusions

- Energica Electronic System was designed taking into account safety first
- Following customers needs and opening the vehicle to external world creates Security issues
- Security enforcement requires a multi level approach, form interface layer to computation layer through transport layer
- Energica is pursuing market needs opening de facto side business opportunities in product customization and aftersales.

Partners of TAPPS

fortiss

ST life.augmented

TTTech

Virtual Open Systems

actility Making Things Smart

FCSR Fondazione Centro San Raffaele

T.E.I. of Crete

eNeRGICA

crit SCOUTING YOUR NEXT TECHNOLOGY

OSPEDALE SAN RAFFAELE

Third parties

Contact

Giovanni Gherardi - Eleonora Montanari

Giampiero Testoni - Gabriele Volpi

TAPPS

Trusted Apps for open CPSs

Co-funded by the Horizon 2020 Framework Programme of the European Union under grant agreement no 645119