mobica OPENSYNERGY NXP ACTIA®

Telematics Innovation: The Opportunities and Challenges

30th June 2020 | 1pm BST | 2pm CET

Agenda

- Requirements and challenges in the telematics industry
- How virtualisation addresses today's challenges in the industry
- How Automotive i.MX 8X Application Processors address these Telematics System requirements
- The highly specialised engineering competency that enables scalability

mobica OPENSYNERGY NXP ACTIA®

Meet the Speakers

Mark Willerton
Manager of Advanced Engineering, ACTIA

Jérôme Gueunier
Embedded System Expert, ACTIA

Tino Löffler
Cloud Connectivity Competency Center Director, OpenSynergy

Julie Duclercq
Director of i.MX Automotive Business Development, NXP

Krzysztof Walczak
Customer Delivery Manager, Mobica

Meet the Speakers

Mark Willerton

Manager of Advanced Engineering

ACTIA®

Jérôme Gueunier

Embedded System Expert

ACTIA®

Requirements and challenges in the telematics industry

- Telematics systems provide connectivity and remote functionality to automotive and mobile machine systems. Growth in functional content continually adds to the challenges and requirements to an already complex setup.

- The partnership has studied appropriate means to deal with these points. A system prototype has been created to demonstrate and validate the solutions.

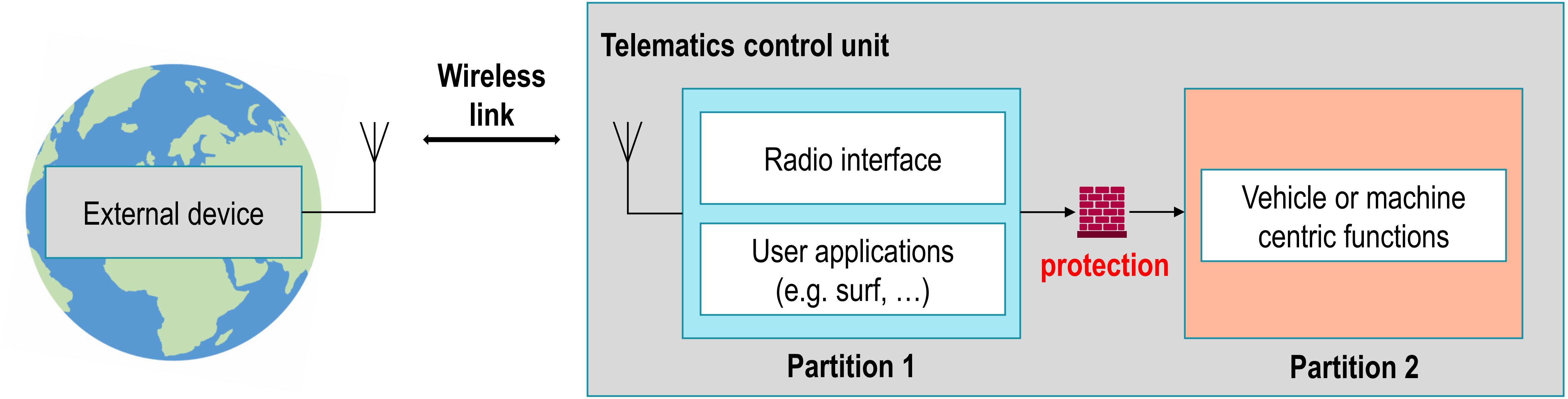
- ACTIA's latest generation telematics platform ACU6 makes these solutions available in a serial product.

- Conclusions from the study can also be seen to apply in other product areas, for example vehicle dashboards.

Cyber security

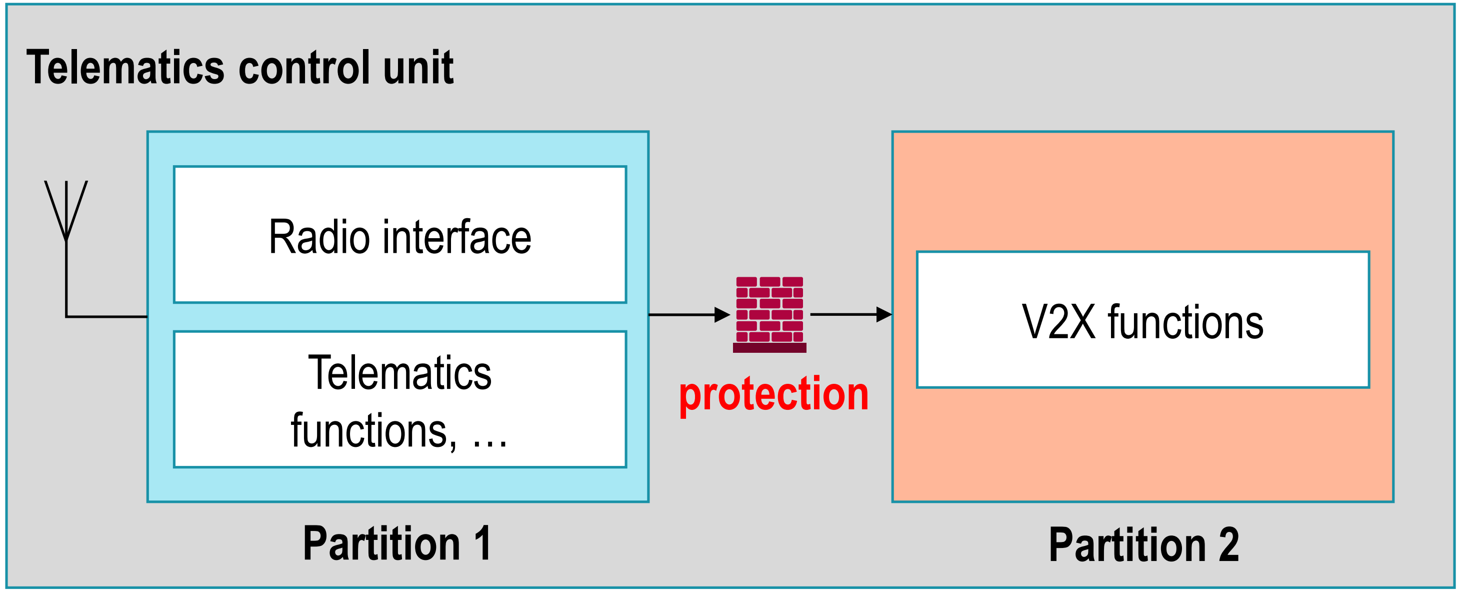
- Keeping ahead in terms of cyber security is a fundamental requirement, despite the ever increasing complexity of telematics systems. The primary objective is to **protect all vehicle/machine functions from cyber attacks** that gain access through the radio interfaces of the telematics system.

- System partitioning can be used as a means to separate sensitive functions from areas exposed to intrusion.



Functional safety

- Telematics systems are starting to host functions attributed with functional safety requirements, e.g. vehicle to vehicle/infrastructure (V2X). This places demands on key criteria such as system integrity, availability and diagnostic capability.
- To make this possible, safety systems need to be **comprehensible**. The term “less is more” often applies, in contrast to the complex telematics implementations.
- **Freedom of interference** must be ensured between the safety applications and neighbouring functions.
- System partitioning can be used as a means to:
  - Manage CPU and memory
  - Ensure critical VM availability

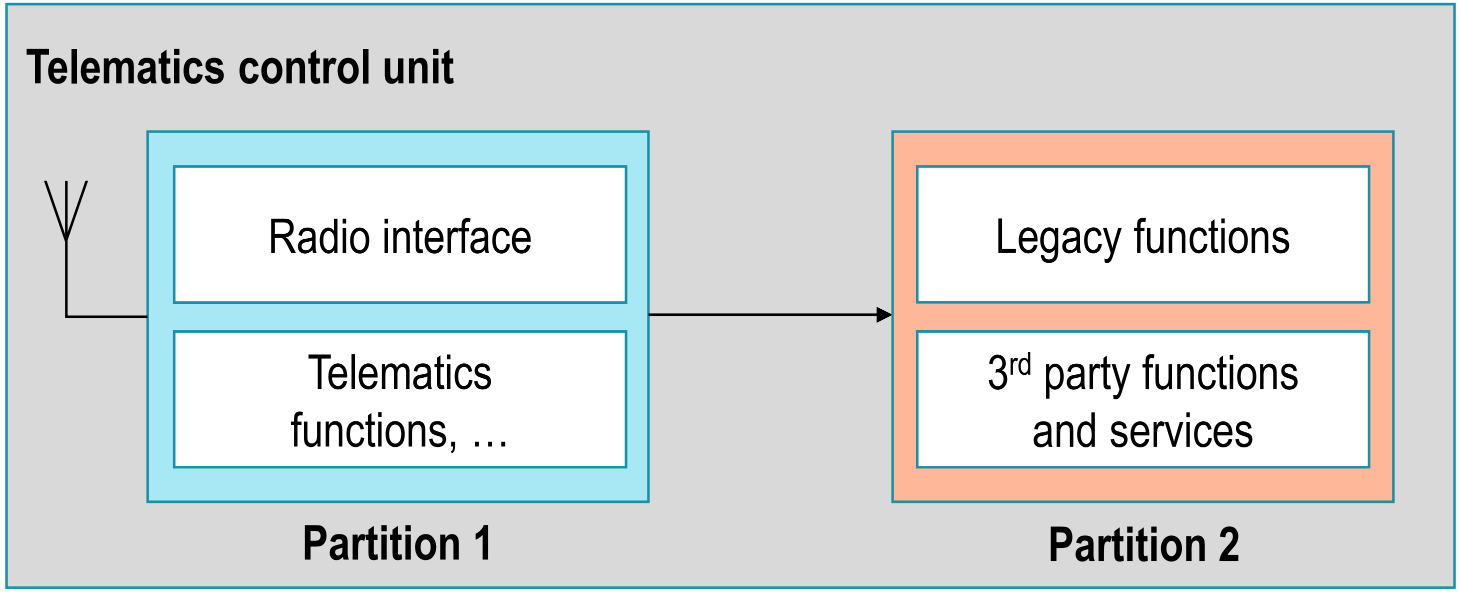


Reuse of legacy functions

- Time to market and tough quality requirements pose an enormous challenge when implementing complex telematics solutions. This task can be simplified by making **reuse of technical solutions** already validated in the field.

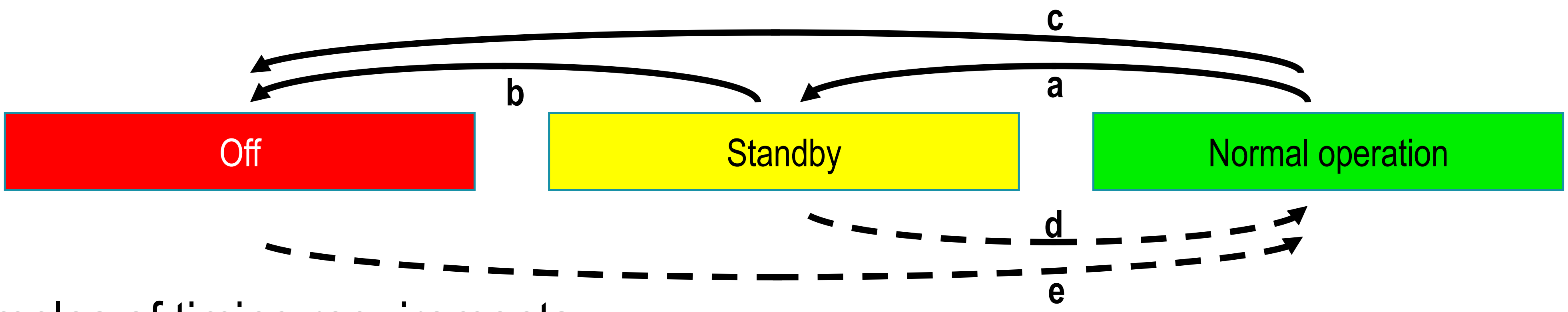
- Similarly, business opportunities can arise through the **integration of 3rd party functions** and services in the telematics control unit.

- A means to deal with the challenges of integrating and validating legacy or 3rd party solutions is to run these in a dedicated system partition.



Startup timing – cold start and warm start

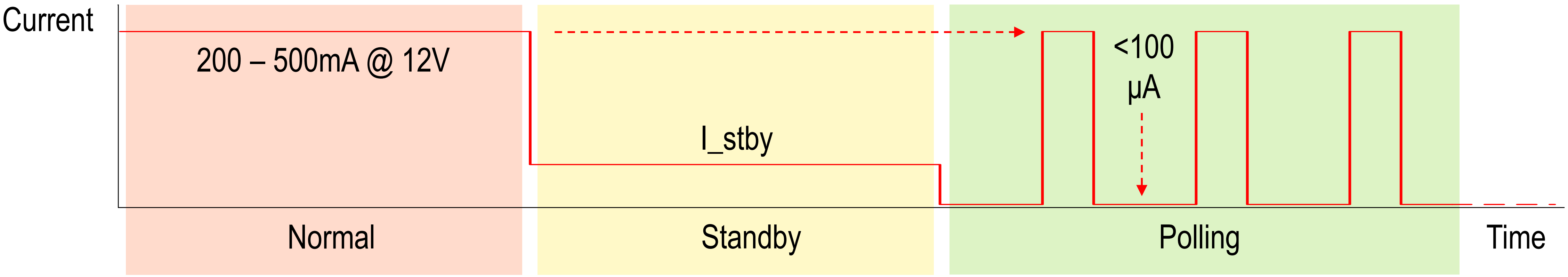
- The three fundamental power modes supported by many telematics systems give rise to two startup procedures: cold start and warm start.



- Examples of timing requirements:
  - Cold start: Diagnostic equipment 1st response CAN 50 – 200ms / Ethernet 1s (3-4s)
  - Cold start: Anti theft systems (imobilisation) validated using a ‘time to first data’ of 200ms
  - Warm start: Remote services (e.g. door unlock) telematics response ≈ 50ms giving an overall end-end response in the range of 200ms

- **Startup time** is a vital aspect when considering system partitioning!
  - Systems using a heavier operating system (e.g. Linux) can allow time critical functions to operate in a dedicated partition using a real time operating system.

System current consumption



- Standby operation offers customer value!
  - Typical energy budget for a light vehicle telematics system would be <1000mAh @ 12V
  - **Standby operation** must be as long as possible – 7 days is considered to be acceptable
  - This translates to an average current consumption (I_stby) of ca. 5mA

→ Modem: ca. 2mA

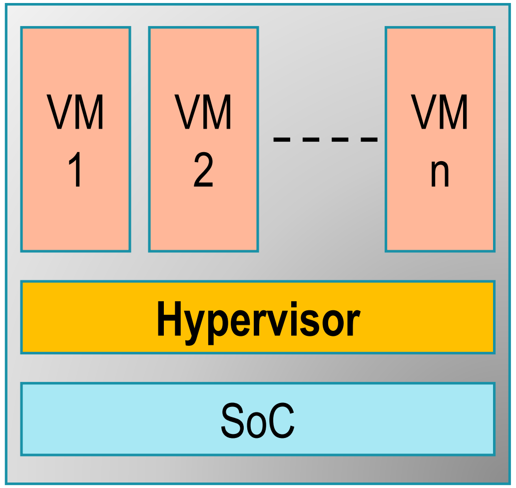
→ Processor: ca. 3mA (i.MX 8X, 1GByte LP-DDR4)

The system solution must allow the necessary configurations and optimisations to allow these figures to be reached!

Hypervisor

- The hypervisor offers a means to achieve rigorous system partitioning. As such, an appropriate hypervisor serves as the basis for cyber security, functional safety and reuse of legacy functions.

- For systems embracing functional safety, the hypervisor must be validated to the relevant **ASIL level**.



- The **hypervisor architecture** is important when dealing with factors such as cyber security.
  - Assignment of resources and further partitions must be kept simple and separate from vulnerable interfaces!

- It is also vital that integration of the selected hypervisor does not compromise key system performance criteria such as **startup timing, jitter** and **power consumption**.

- **Simple VM integration** is an important feature to simplify software maintenance!

Meet the Speakers

Tino Löffler

Cloud Connectivity
Competency Center Director

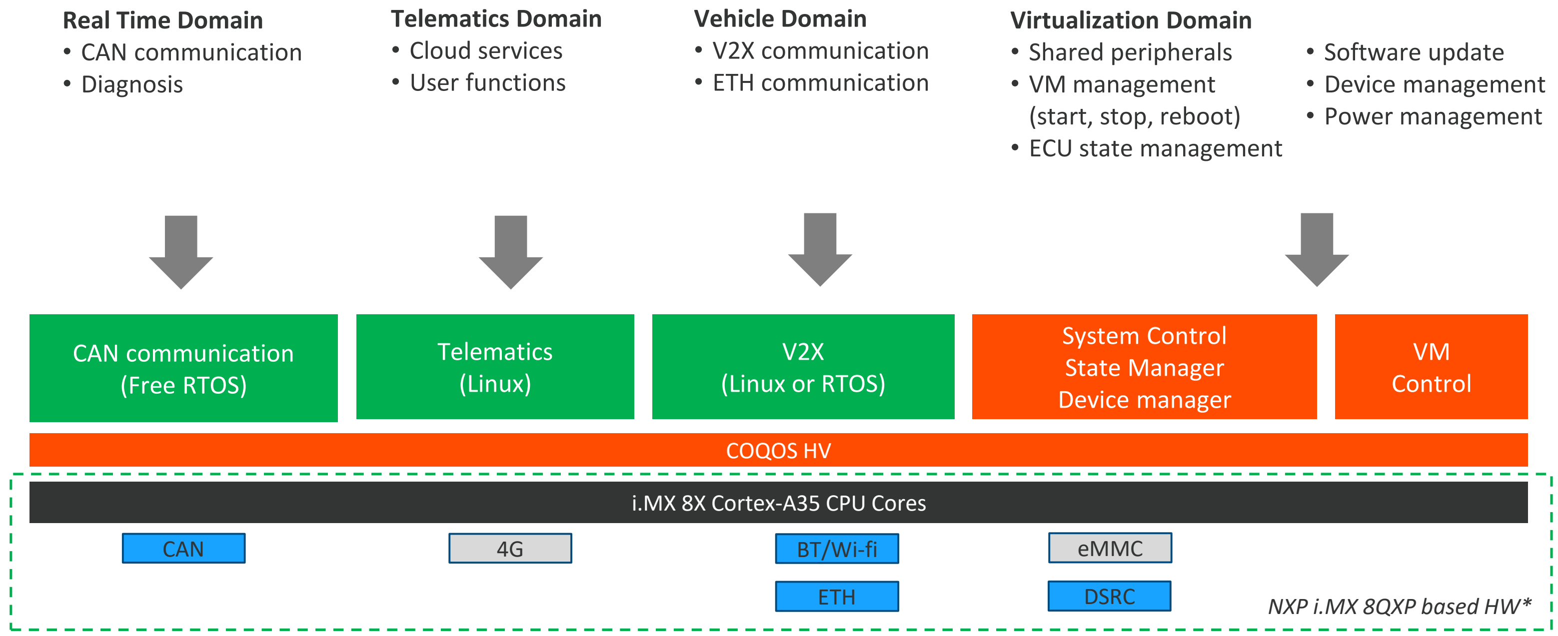
OPENSYNERGY

Part 2: How virtualization addresses these points

Strong separation, while respecting requirements on **boot time**, **current consumption** and **communication characteristics**

Reference architecture for virtual TCU

Goal: To prove that a virtualized TCU fulfills today's telematics requirement



**: can be ported to any variant of i.MX 8X products family.*

Legend: 3rd Party Peripheral (grey) · OpenSynergy (orange) · ACTIA (green) · NXP i.MX 8XS (dark grey) · NXP Peripheral (blue)

- **Performance & stability**
  Overloading one VM does not have a negative effect on jitter and latency of communication
- **Freedom from interference**
  Crashing or overloading one VM do not affect the other VMs
- **Security**
  Achieving strong separation between vehicle and external network
- **Power management**
  Achieving Suspend-to-RAM with low power consumption coordinating every VM
- **Early function availability**
  Providing early availability of critical functions during boot time and being able to quickly resume operation from suspend mode

Reference architecture for virtual TCU

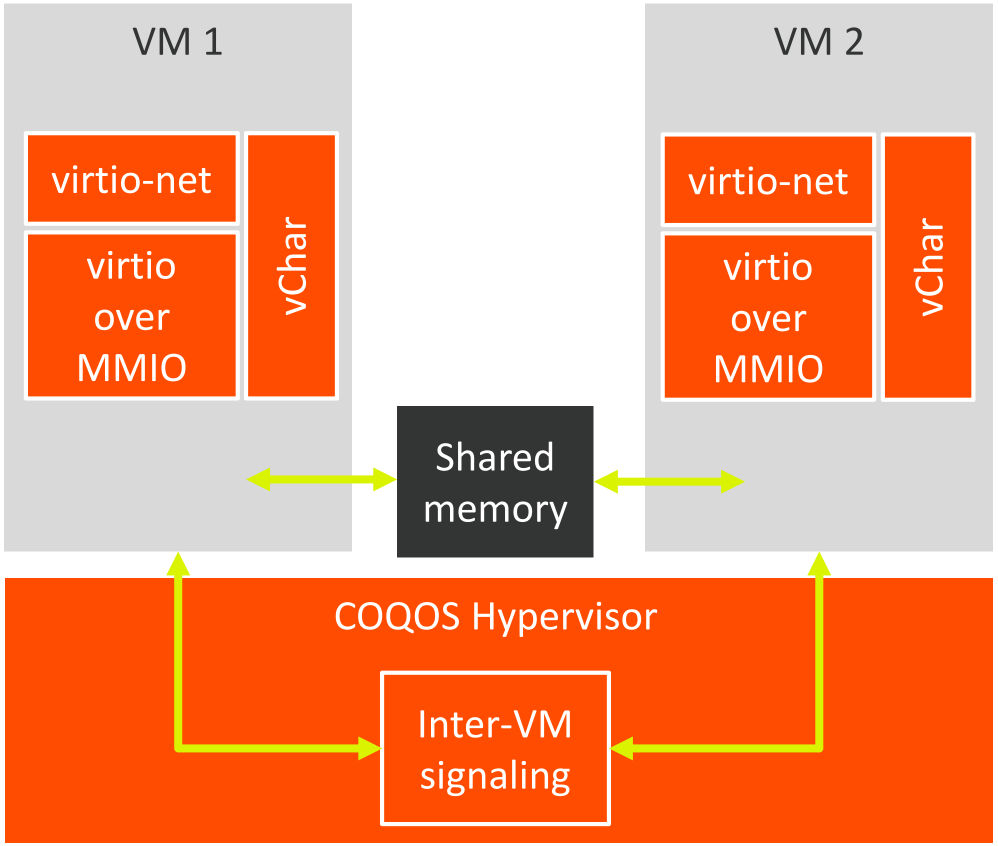
- **Strong Separation**
- **Low Overhead Inter-VM Communication**
- **Efficient Device Sharing**
- **VM State Management**

- **COQOS HV -** Minimalistic, statically configured, type 1 hypervisor
- **COQOS IXCF -** Built on top of efficient HV primitives (Inter-VM signaling via SW interrupts and shared memory)
- **VIRTIO -** “De-Facto Standard For Virtual I/O Devices”
- **COQOS SDK State Manager -** Software toolbox to control global state of guests and the overall ECU

COQOS HV

- Is a **minimalistic Type-1** Hypervisor
- Takes maximal advantage of **hardware virtualization extensions**
- Supports **full virtualization** of the CPU for the guest OS
- Has a **lean and innovative design providing high performance, safety and security without legacy burdens**
- Builds upon **years of experience** in research and automotive mass production
- Has **no open source** components
- **TÜV certified**: First hypervisor complying to the new version of ISO 26262
- Supports **full automotive** use-cases and automotive **multi-core** SoCs

COQOS IXCF



- **Inter-VM signaling is mapped to virtual guest interrupts. Sender is reliably identified by IRQ number.**
- **Shared memory is statically defined, mapping provided to the guests.**
- **Security through configuration**
  - Always point-to-point, can be configured bi-directional or uni-directional
  - Non-bypassability guaranteed for A-B-C configurations (B cannot be by-passed)
- **Higher abstractions are built on top in the VMs**
  - vChar - character device for easy and fast transfer of messages
  - virtio-net - full fledged network device

VIRTIO

- **Essential I/O devices that make up a complete platform suitable for automotive use**
- **Based on VIRTIO to allow multiple interoperable implementations**
- **Backed by major industry players and organizations**
- **Wide operating system support**

Available in COQOS & upstreamed

Available in COQOS & upstream in progress

Android | AGL Linux | Genivi | RTOS

COQOS Virtual Platform

virtio-blk
- Block Device
- Persistence management

virtio-scmi
- Clocks
- Regulators
- Sensors
- Power Management

virtio-net
- Network Device

virtio-console
- Console
- Serial

virtio-gpu
- 3D GPU
- 2D GPU (Display)

virtio-audio
- Audiov

virtio-video
- Camera
- Video Codecs

virtio-entropy
- Random Number Generator

virtio-input
- Human Input Device

virtio-vsock
- Virtual sockets

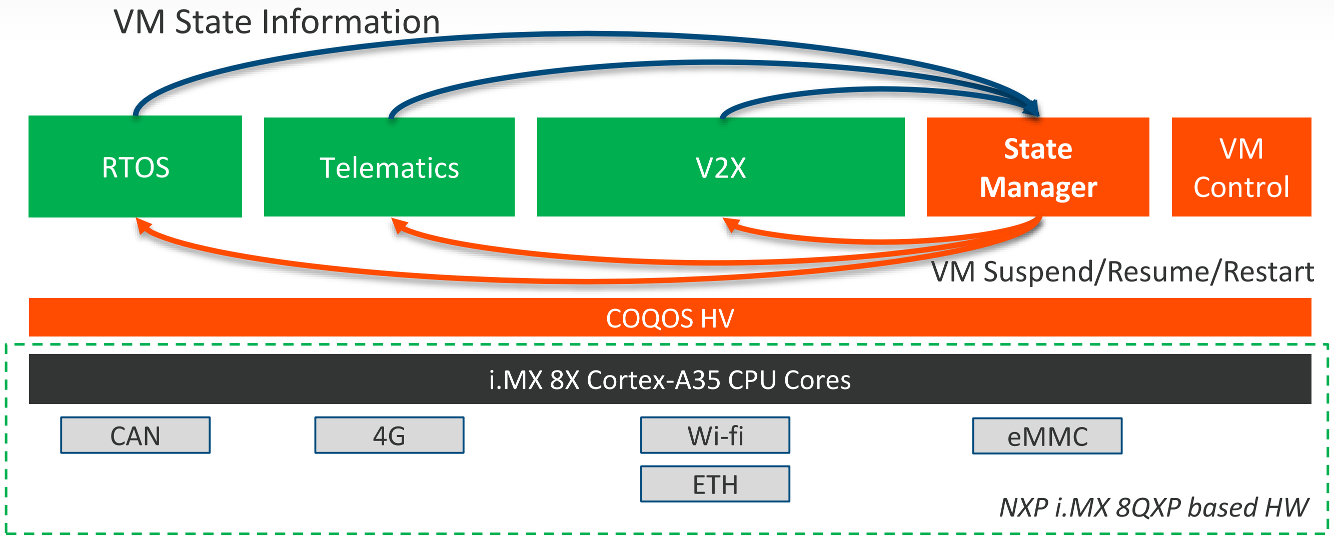
virtio-usb
- USB device
- USB host

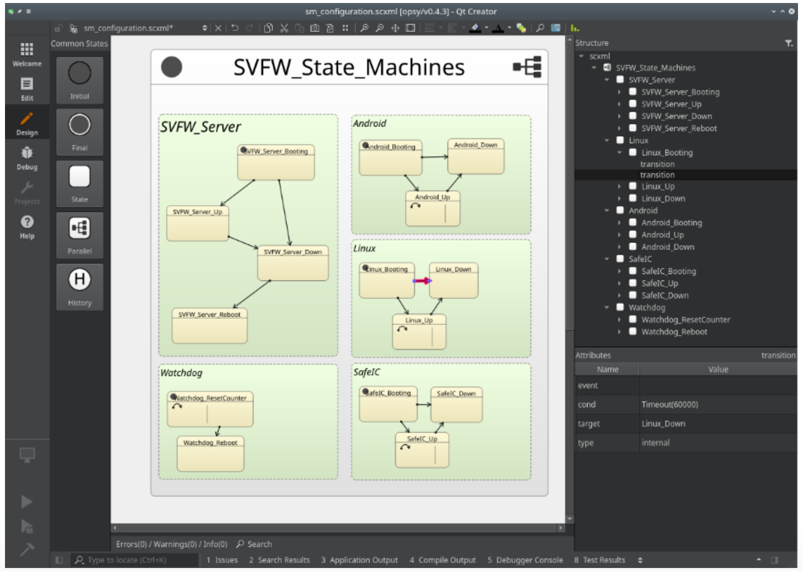
virtio-…

COQOS State Manager

Software toolbox to control global state of guests and the overall ECU

- Behavior can be configured in form of state machines via SCXML standard
- 3rd party configuration tooling for state machines available
- Messages between client and server can be configured via simple XML file





CONTACT

Headquarters

Berlin

OpenSynergy GmbH

Rotherstraße 20
D-10245 Berlin
Germany
Phone +49 30 / 6098 5400

Further Locations

Utah

OpenSynergy, Inc. (USA)

765 East 340 South
Suite 106
American Fork, Utah 84003
USA

California

OpenSynergy, Inc. (USA)

501 W. Broadway, Suite 832
San Diego, California 92101
USA
Phone +1 619 962 1725

Munich

OpenSynergy GmbH

Starnberger Str. 22
D-82131 Gauting / Munich
Germany
Phone: + 49 89 / 2153 9073

E-Mail info@opensynergy.com
Web www.opensynergy.com

Meet the Speakers

Julie Duclercq

Director of i.MX Automotive Business Development

NXP

Part 3: How Automotive i.MX 8X Application Processors address these Telematics System Requirements

Virtualized Telematics Systems Webinar

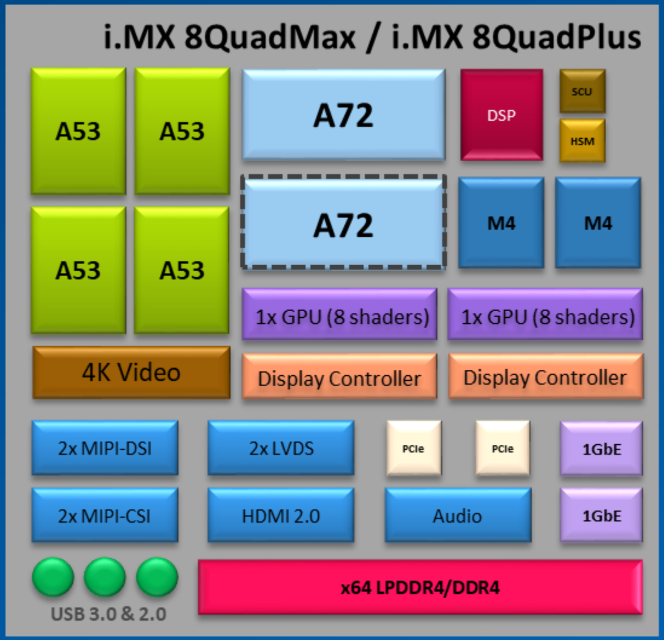
JUNE 30TH, 2020

Julie Duclercq
EMEA AUTOMOTIVE BUSINESS DEVELOPMENT DIRECTOR FOR i.MX PRODUCTS

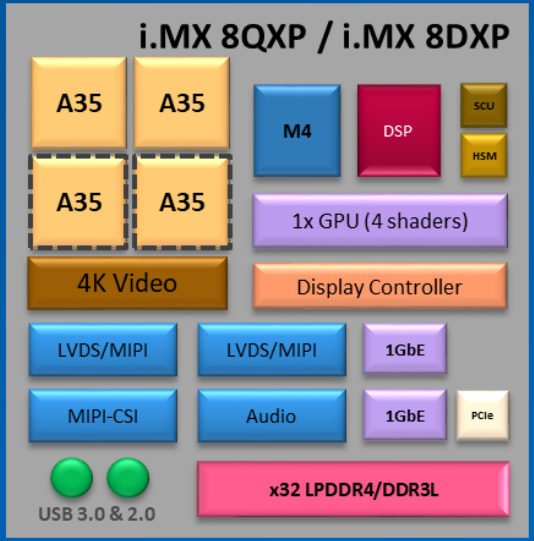
NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

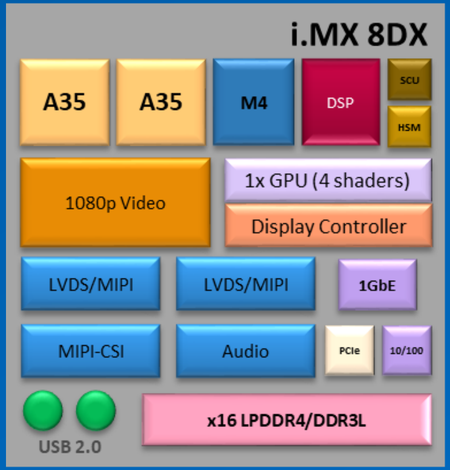
i.MX 8 Series Roadmap Update

Scalability of Embedded Processing for Automotive & Industrial Applications



Devices qualified and shipping mass production and supported on 15 year longevity plan from 2020 general market launches





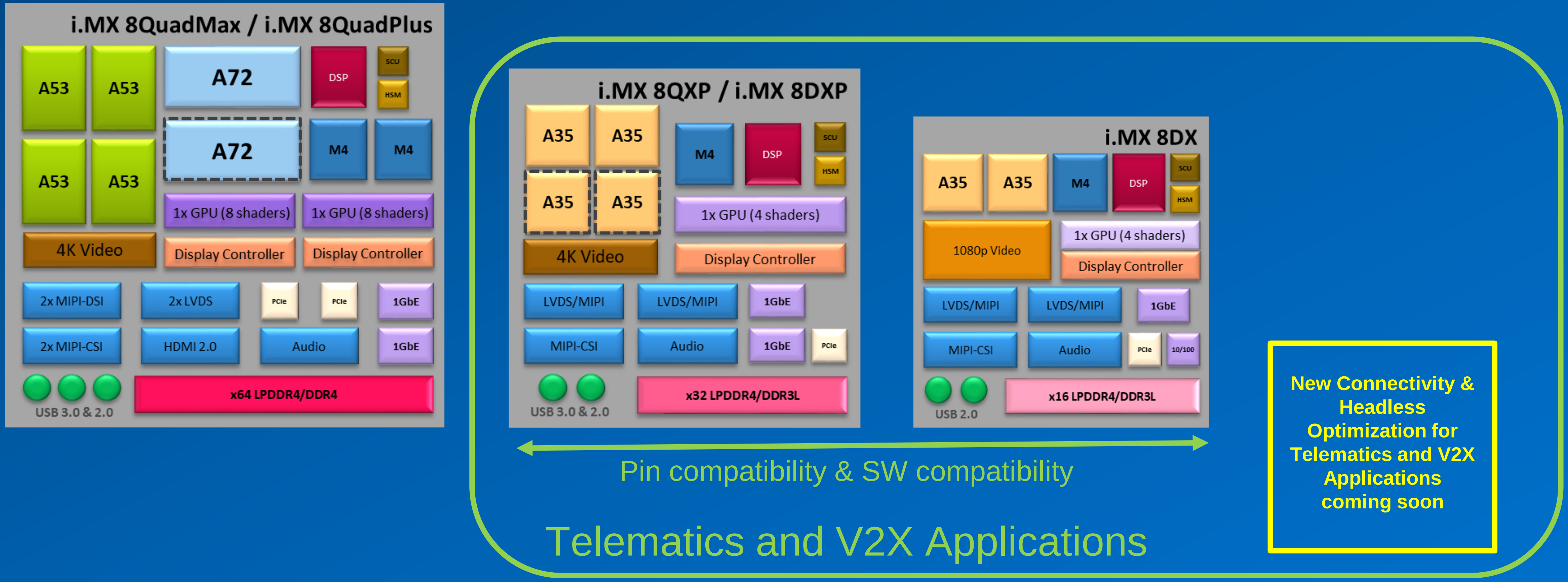
New Connectivity & Headless Optimization for Telematics and V2X Applications coming soon

HMI, Vision, Audio and Voice Enabled with i.MX

Simplified eCockpit, Real Time Domain, Safe Camera/Display/Audio

i.MX 8 Series Roadmap Update

Scalability of Embedded Processing for Automotive & Industrial Applications



i.MX 8X ADVANCED SAFETY AND SECURITY FEATURES

eXtended Resource Domain Control
Isolated DDR Regions of any Bus Master in the System

Cortex M4 CPU with Dedicated Tightly Coupled SRAM with ECC
Offers Isolation of Real Time and Time Critical Functions

Error Correction Code on DDR3L
Eliminates Extra DDR Device from System

Firewalled Security Subsystem
Secure CPUs are Isolated from Main System and Accessed Through Common i.MX 8X APIs

Secure, Encrypted Off-Chip Storage
Secret Keys can be Encrypted and Stored in External NVM with Decryption by IC-level Key

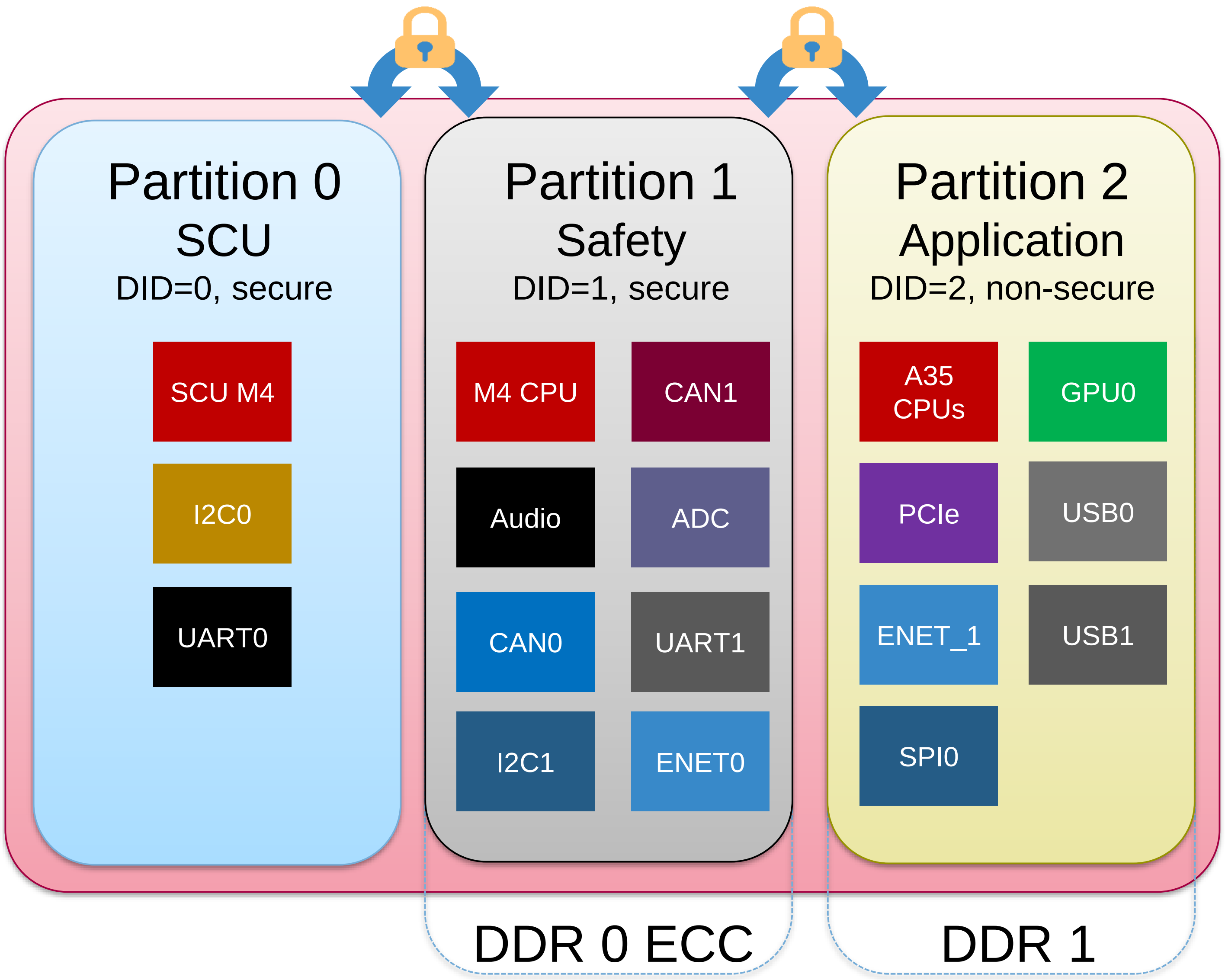
i.MX 8X Resource partitioning

eXtended Resource Domain Control

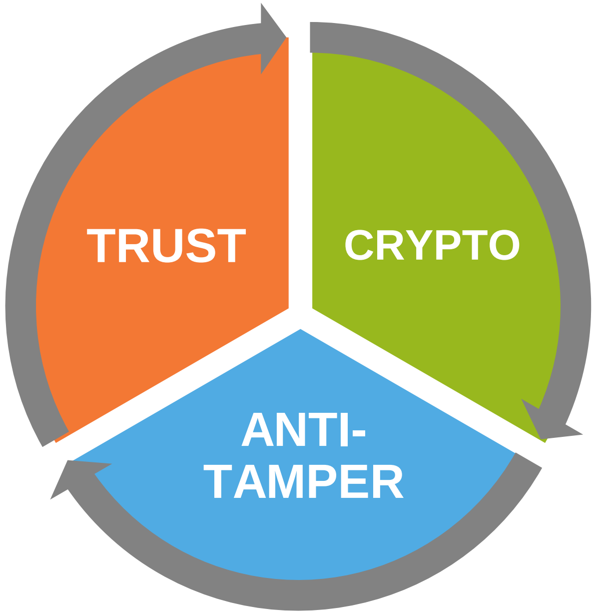
- The system controller (SCU) commits peripherals and memory regions into specific domains as defined by the customer application (up to 16)
- Any communication between domains are forced to use messaging protocols
- If a domain peripheral tries to access other domains illegally, a bus error will occur

Benefits of XRDC

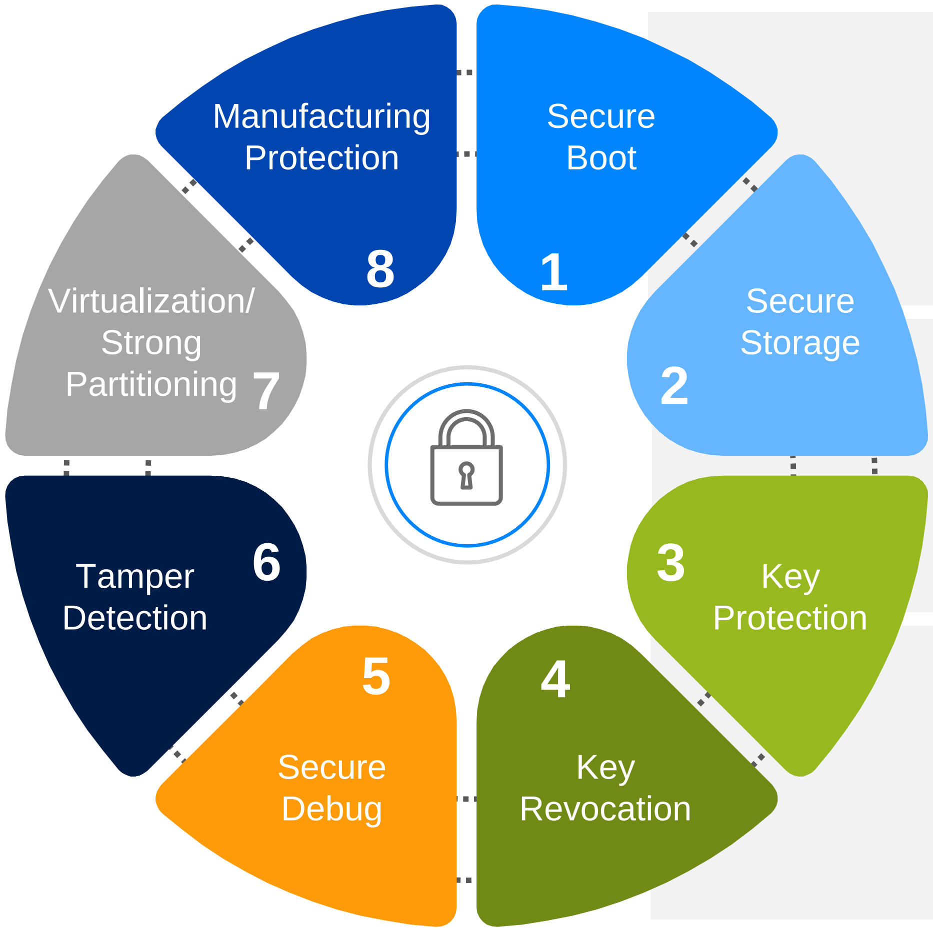
- Offers unique hardware partitioning to enforce isolation. This capability significantly simplifies also the virtualized system development. This advanced hardware virtualization enables rapid deployment of multiple operating systems on top of an hypervisor, such as OpenSynergy COQOS
- Secure memory regions may run with or without ECC based on domain requirements
- Peripherals can migrate between domains depending on early access requirements (Ethernet, CAN)
- Reporting of immediate illegal accesses helps track down hard to find race conditions before they go to production. (AKA Sandbox Methods)



AUTOMOTIVE PRODUCT LONGEVITY



I.MX 8X - SECURITY



BASELINE SECURITY
Secure Boot
Secure Debug
Secure Storage

TAMPER DETECTION
Detect Tamper Events
Tamper Response

ADVANCED SECURITY
Key Protection
Key Revocation
Strong Partitioning

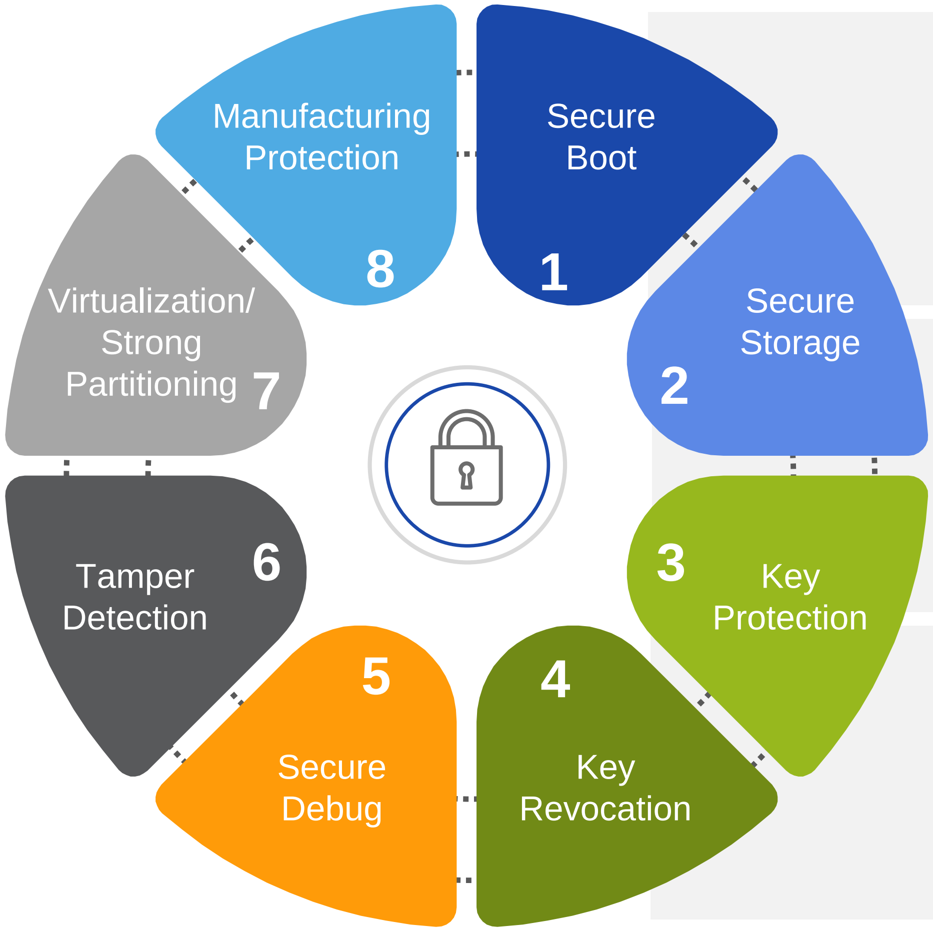
Mobile and stationary machines want full access to cloud-based knowledge

This requires **faster, more reliable** and secure connectivity

NXP is focused on **secure communications** and tamper resistance

Leadership experience in security markets: over 10 billion smart cards sold

I.MX 8X - SECURITY



BASELINE SECURITY
Secure Boot
Secure Debug
Secure Storage

TAMPER DETECTION
Detect Tamper Events
Tamper Response

ADVANCED SECURITY
Key Protection
Key Revocation
Strong Partitioning

SECURE CONNECTIONS
FOR A SMARTER WORLD

Meet the Speakers

Krzysztof Walczak

Customer Delivery Manager

TCU Reference Platform

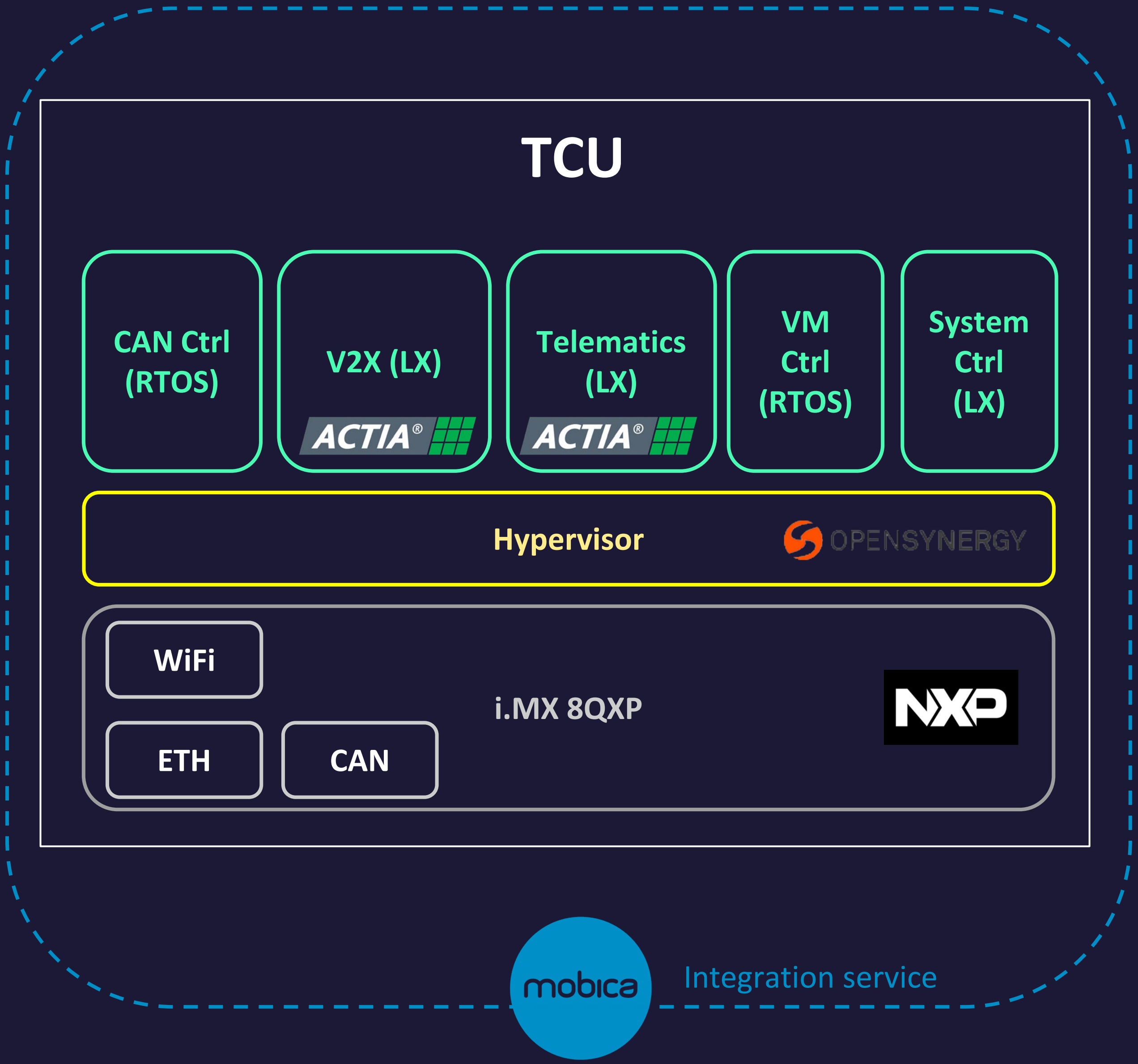
Joint Reference Platform

Core development

OpenSynergy, NXP, ACTIA and Mobica have realized a joint reference platform demonstrating the key characteristics of a hypervisor-based Telematic Control Unit (TCU).

Core development components

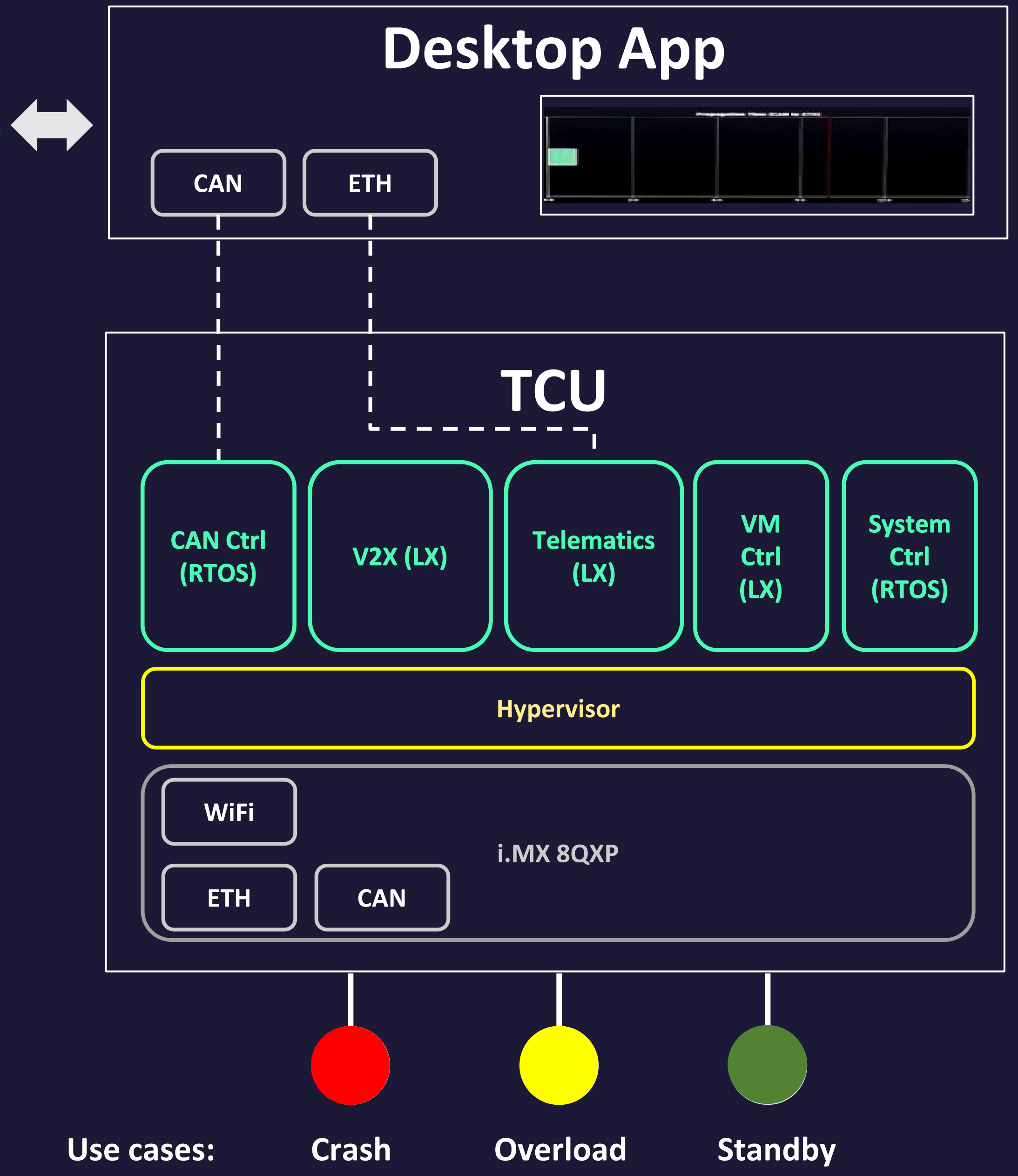
- OpenSynergy provided virtualization platform COQOS Hypervisor SDK.
- NXP provided Automotive i.MX 8QXP/i.MX 8DXP/i.MX 8DX Application Processors for Telematics
- Actia provided ACU6 based TCU on which telematics VM has been integrated to connect the car with a fleet management office.
- Mobica provided customized software integration service to put all system components together.



Development Assumptions

Value proposition:

- **Freedom from interference** - crashing or overloading one VM do not affect other VMs with different ASIL levels (e.g. eCall).
- **Security by separation** - strong separation between vehicle and external network.
- **Early function availability** - critical functions (e.g. CAN) are available early during the boot time.
- **Power management** - enabling suspend to RAM to achieve long standby times with low power consumption.
- **Easy TCU deployment**- enabling customer to focus on development and integration of actual services.
- **Scalability and integration** - customization of telematics solution carried out by experienced service partner so that customer can save more time and energy for concentrating on its core business.



TCU Reference Platform

Demo setup:

- Desktop Application
- TCU Hardware (ACU6)

Key performance indicators:

- Network throughput
- Jitter performance

Use cases:

- Crash
- Overload
- Standby

KPIs measurement

Crash

Overload

Standby

VMs visualization

- Visualization of various VMs running on Hypervisor as well as changes of the system state

Throughput measurement

- Throughput of the message coming from the vehicle to another interface

Jitter performance measurement

- Jitter performance of CAN and Ethernet messages

Fleet management system

- Collecting data from the Telematics Control Unit

Demo Live

Thank you

Krzysztof Walczak krzysztof.walczak@mobica.com

To find out more

- Watch our video presentation
- Schedule a live demo with one of the team
- Get in touch with our speakers

Thank you