Connected Cars
What does it mean for the vehicle Electrics/Electronics-Architecture and for the semiconductor suppliers?

Marc Osajda
Marketing Manager, Freescale Semiconductor

ISO IEC ITU International Telecommunication Union

Abstract

Without any doubt “connected vehicle” is the next big step in mobility. We are living in a fully connected world; however our vehicles are still relatively closed system, providing very little embedded connectivity and communication with the external world while moving. This will evolve driven by new societal needs, but also to enable electro mobility, reduce road fatalities and provide better services.

However the electrical/electronic (E/E) architecture of future connected vehicles will have to evolve in order to take into account new challenges: Significantly more data exchanged, security of exchanged data, functional safety requirements.

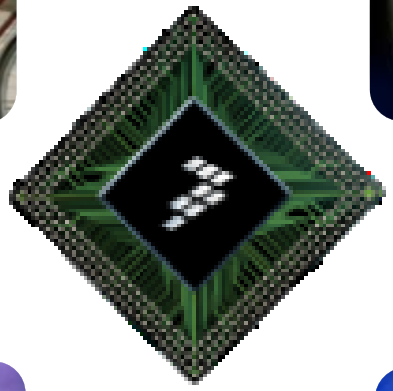
These new vehicle E/E architectures have also significant implications for the semiconductor industry. Computing power requirements is exploding, memory size is growing exponentially with more and more complex software, power consumption reduction is a must, ISO26262 compliant solutions is becoming standard, and security/anti tampering features are being requested at the silicon level.

This presentation will describe how the semiconductor industry is addressing theses challenges.

Automotive World Mega Trends

Mobility for **Everyone**

Safety for **Everyone**



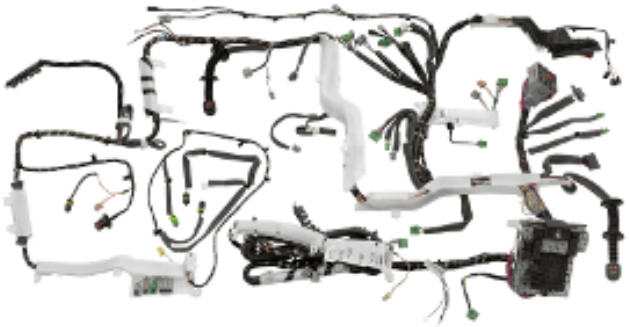
Cleaner world for **Everyone**

Everyone **Connected**

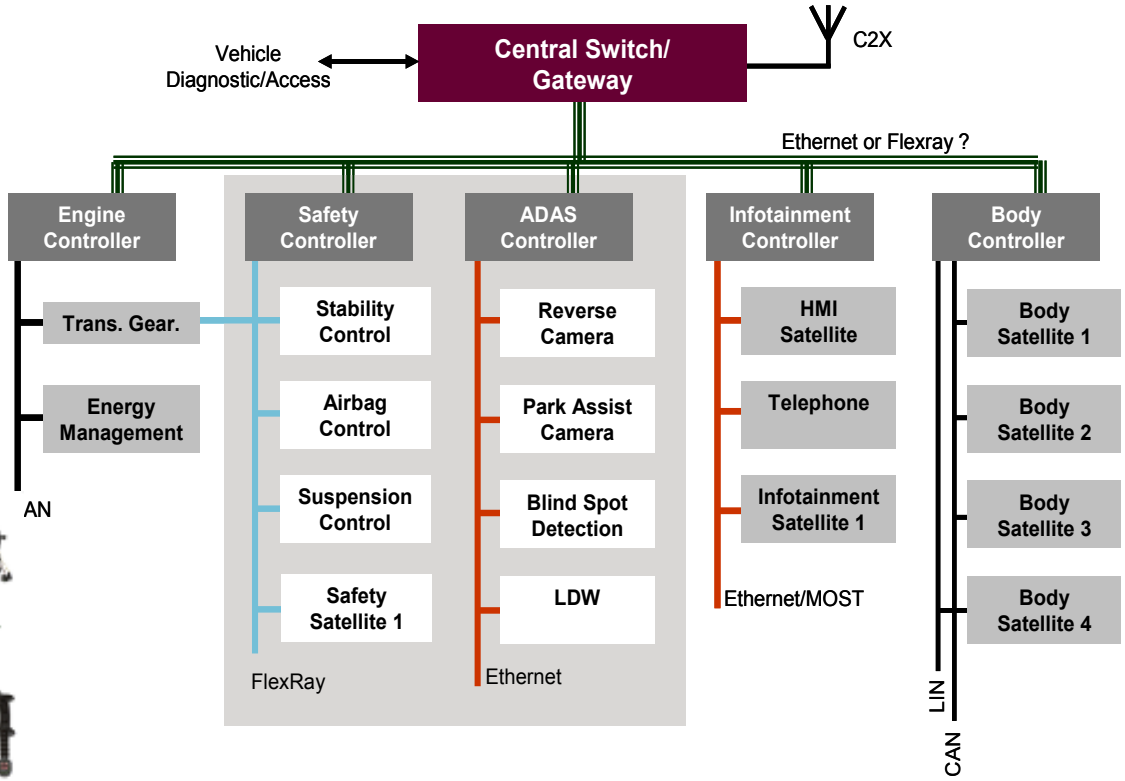
ISO IEC ITU International Telecommunication Union

New Trends in Vehicle Architecture

- Vehicle E/E architecture is
  - Too **complex**
  - Too much **power**
  - Too many **ECUs**
  - Too many **cables**
  - Too many **connectors**
  - Too much **weight**
  - Too many, too many…



Future Evolution
Domain Based Network



ISO IEC ITU International Telecommunication Union

New Architectures driving new requirements

Requirements	Semiconductor solutions
High Computing Power	Multi-Core SoC's, Embedded NVM, 55nm Technology.
Complex Software	Autosar MCAL & OS, Middleware/ Libraries provided by Semiconductor suppliers and Eco-System Partners
High Bandwidth Network	FlexRay & Ethernet to be embedded on all Future Domain Controller MCUs.
Low Power	Multicore, MCU+Power Managemenent IC (SBC) bundle, Partial networking.
Safe	ISO26262 Functional Safety compliant silicon solutions Multi core lockstep architecture
Secure	**Embedded Cryptographic features**

Automotive Security –Attacks & Motivations

- **Potential Attackers**
  - Car owner
  - Car driver
  - Tuner
  - Garage employee
  - Organized crime
  - Hackers

- **Potential Motivations**
  - Professional financial gain
  - Comfort gain
  - Enhanced driving fun
  - Circumventing regulatory requirements
  - Just-for-fun and reputation

Security in Automotive ECUs : Market Events

Event	Demonstration
August 2007 Keeloq broken	Crypto 2007 conference paper ***How To Steal Cars - A Practical Attack on KeeLoq*** By intercepting several transmissions from the electronic key and analyzing them, a master key is worked out in about one day. It can unlock all cars using that master key within a few minutes.
May 2010 OBD-II Interface hacked	2010 IEEE Symposium on Security and Privacy paper ***Experimental Security Analysis of a Modern Automobile*** Malicious code in vehicle gateway enables control of high-speed CAN (brakes) via the slow-speed CAN (OBD)
August 2010 TPMS vulnerabilities exposed	2010 USENIX Security Symposium ***Security and Privacy Vulnerabilities of In-CarWireless Networks: A Tire Pressure Monitoring System Case Study*** Risks: Inter-Vehicle Spoofing, Tracking profiles

Automotive Security
What is it all about?

Security risk	Example / Field of application
Immobilizer	Traditional security application (RKE), Engine Management, Gearbox, Steering
Data Set Protection	Car data „theft“, mileage manipulation, ECU behaviour manipulation, etc
Component protection entity authentication	Prevent re-use of ECUs from stolen or wracked cars
Software Integrity data-origin authentication	(Un)authorized chip-tuning, feature enablement, navigation data, etc
Confidentiality and Privacy	Off-board navigation, toll collect system, location-based services, etc
Rights Management & Copy Protection	Navigation map data, music, video, etc
Denial of Sevice (DoS) &Malware	Car2x communication

Industry Example: SHE - Secure Hardware Extension

- BMW, Audi and escrypt developed the **SHE** specification

- Security module with a specific set of **cryptographic** functions
- Includes protection for cryptographic keys
  - No CPU or debugger access to keys
  - Secure key distribution protocol
- Developed as a **free and open standard**

Implementation on Silicon

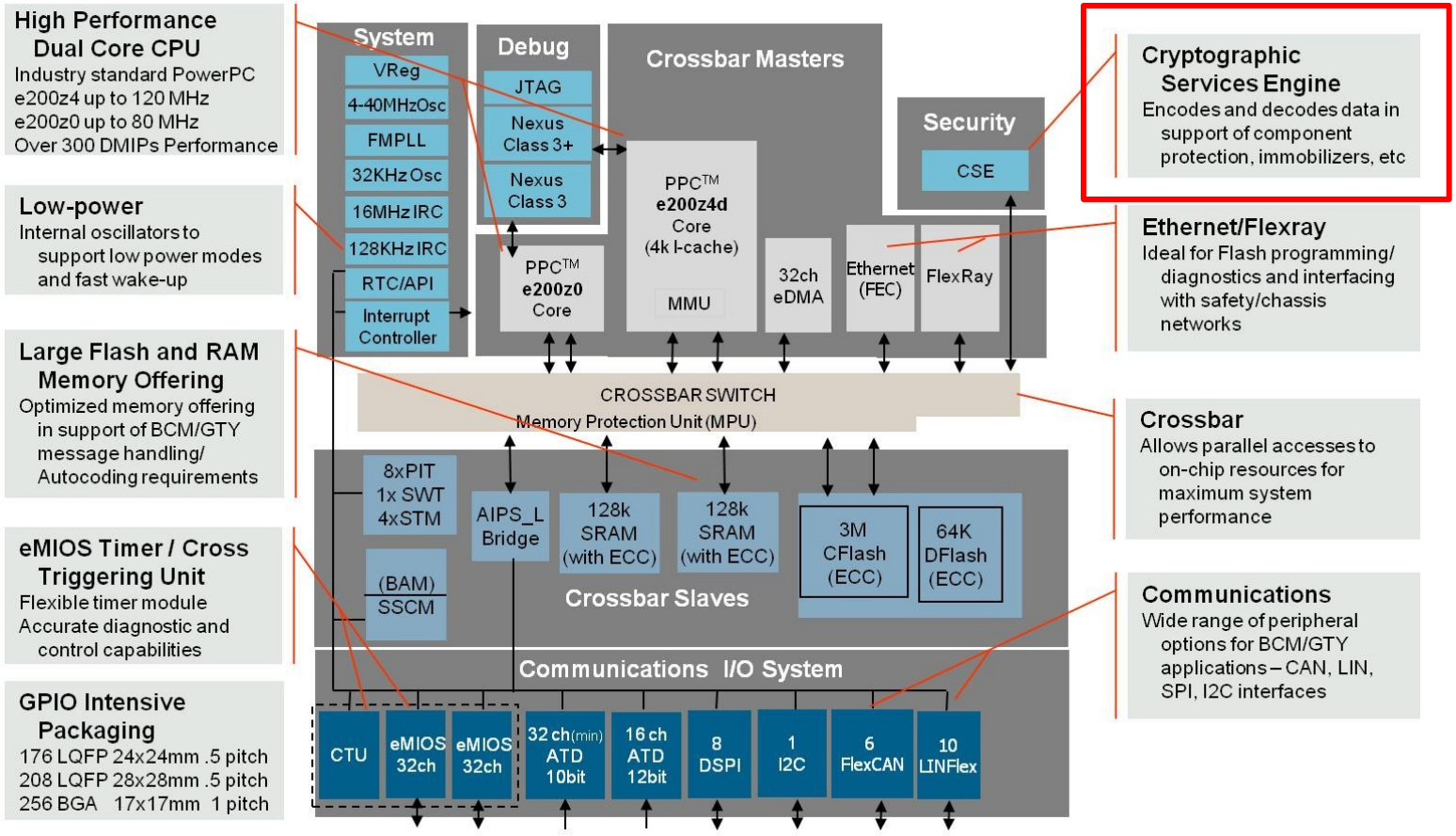
- The **Freescale MPC561xB/C** devices are the first microcontrollers for automotive that incorporates a **Cryptographic Service Engine** (CSE) to address the **SHE** requirements

  - Enables Secure Transmission of information between electronic control units (ECUs)
  - Data are encoded and decoded for various functions
    - Blocking illegale manipulation of vehicle's mileage
    - Activating Immobilizer to prevent vehicle theft
    - Preventing individual ECUs from being dismantled and reused in other vehicles
  - **Product Launch: March 1st, 2011 @ Embedded World, Germany**

ISO IEC ITU International Telecommunication Union

Freescale MPC56xx – The next generation of MCUs

The device is intended to be used in high end body controller and central gateway applications



Deployment of Security in Automotive Systems

- **Today**
  - Mainly Car Access systems
- **Starting soon**
  - Device Protection
  - Enabling of functions)
  - NFC for car access
- **Mid to long term-Term**
  - Connected Vehicle, C2x
  - Application Stores / Cloud computing
  - Protection of IP-based car networks

ISO IEC ITU International Telecommunication Union

Summary

Summary

- Increasing electronic complexity
- All ECUs to be interconnected through central gateway
- Security weakness demonstrated
- Car to be connected to the external world
- Semiconductor devices to be protected at the silicon level
- Expect cryptographic engine requirement to be standard for all new MCUs
- Best defense: Make attack unprofitable

Thank you for your attention

The Official Automotive
Semiconductor of

ISO IEC ITU International Telecommunication Union