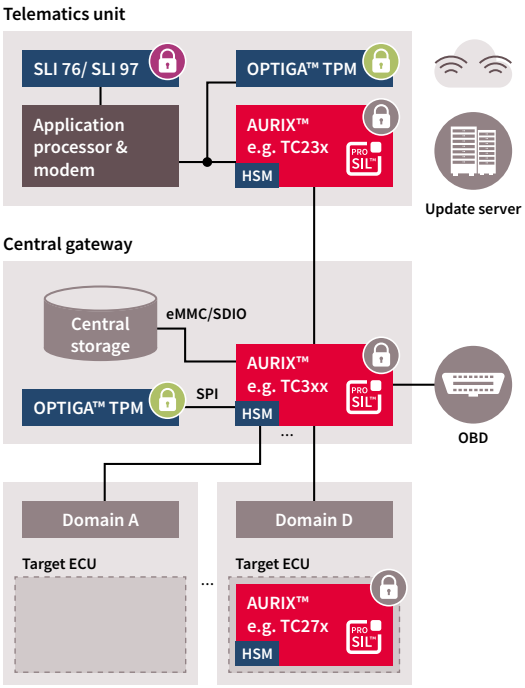
Car security for trusted driving

Software update Over The Air (SOTA) secured by Infineon's security controllers

High expenses at vehicle manufacturers for fixing software issues by costly recalls are driving their desire to use mobile communication channels in order to remotely execute software updates over the air (SOTA). The benefits of this remote update are really compelling, but the security aspect and with it the potential consequences on the car's safety need to be considered.

An insufficiently secured external connection, which is used to run software updates, could open up the door for potential hackers to the complete board net architecture of the car und thus its safety systems. So in the end a driver's life could be dependent on the security protection mechanism of the vehicle.

Infineon's security controllers are offering security protection for different use cases in a SOTA system. The graphic below shows a simplified proposal of a SOTA system architecture, where dedicated security controllers are taking over specific security functions.

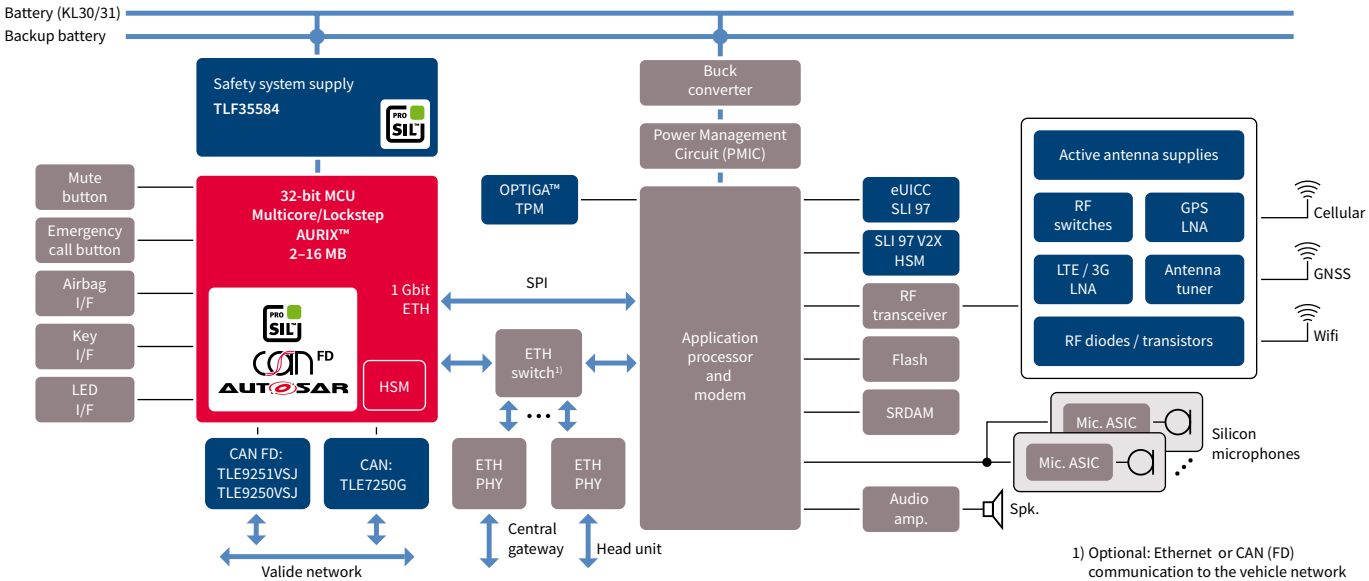


Service authentication
- Mutual authentication between car and OEM update server
- Encrypted transport channel
- Cellular network access

Verification and central storage
- Service pack reception
- 1st verification (OEM signature)
- Storage in car central memory

Update of target ECU
- Service pack reception
- 2nd decryption & verification (Tier signature & key)
- Flashing of code memory

Telematics Control Unit (TCU) – protecting the connected car



The TCU connects the car to the outside world and thereby enables numerous new applications:
- In the event of a serious accident, eCall automatically dials the regional emergency number
- Software in different ECUs can be updated remotely, to either add new features or remove software bugs
- Remote diagnostics and concierge services

Proposed security functions:
- The TC2xx and TC3xx AURIX™ microcontrollers to protect the car network
- The SLI 76 and SLI 97 security controllers for cellular network access. They are tailored to in-vehicle-usage by offering an extended temperature range (-40°C to 105°C) AEC-Q100 qualification and support PPAP
- The SLI 97 V2V for vehicle-to-vehicle and vehicle-to infrastructure communication
- The OPTIGA™ TPM (Trusted Platform Module) as standardized turn-key solution to protect the integrity and authenticity of application processors

www.infineon.com/sota