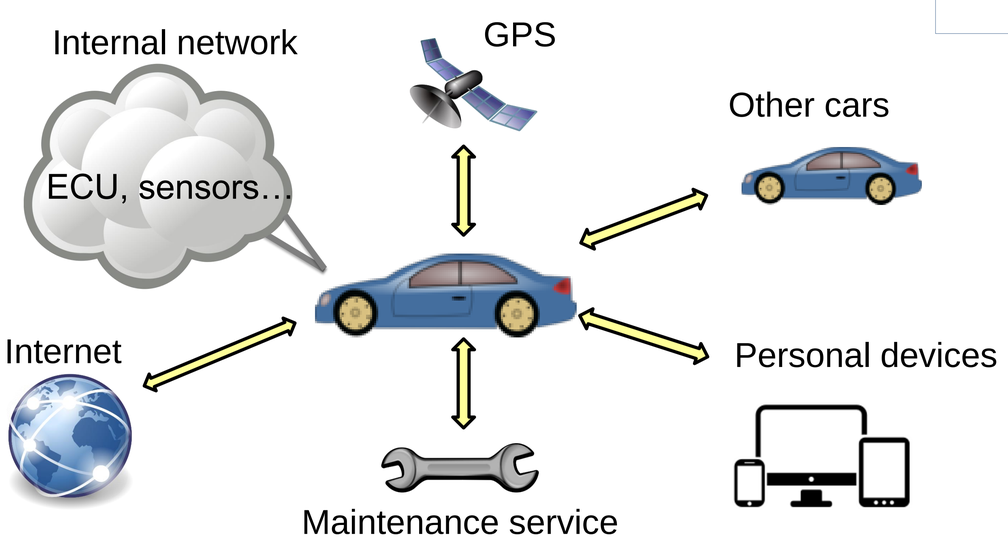
TETRACOM: Technology Transfer in Computing Systems

FP7 Coordination and Support Action to fund 50 technology transfer projects (TTP) in computing systems.
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 609491.

Analysis of security risks & threats and the design of a hardware secure module to perform cipher algorithms for automotive applications

Luca Fanucci, Francesco Falaschi, Berardino Carnevale, Luca Crocetti, Università di Pisa, Italy
Harman Hunjan, Sandro Rosi, Maria Carmela Simone and Samson Bisase, Renesas Electronics Europe Ltd, Bourne End, UK

TTP Problem

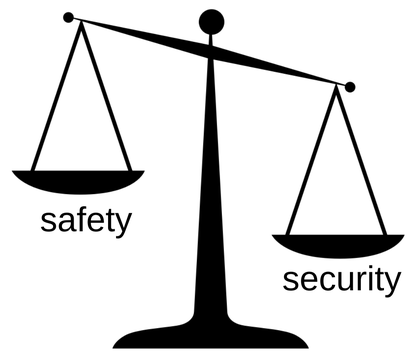


Problem and context

- Increased car connectivity with external entities and other cars
- Security issues that can involve safety related ECUs over the car internal network

Pure software solution drawbacks

- Slowness in safety timing constrained environments
- Resource inefficiency
- Weak SW level security countermeasures



TTP Solution

Secure HW (SEC-HW) for each ECU microcontroller that guarantees:

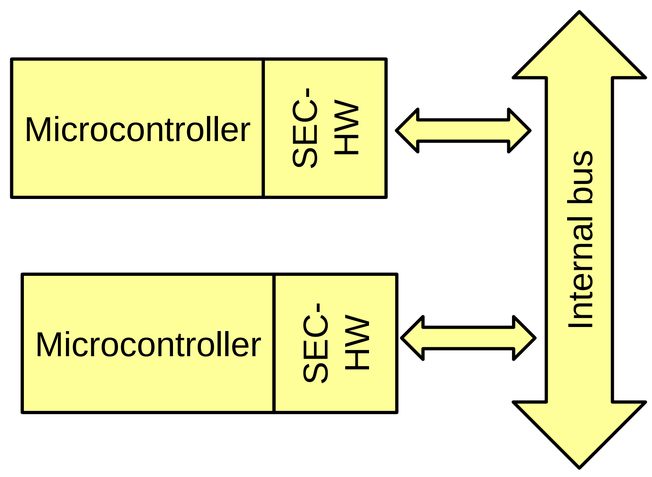
- Memory/data encryption (using cryptographic algorithms)
- Random number generators
- Bus data encryption
- Tamper resistance

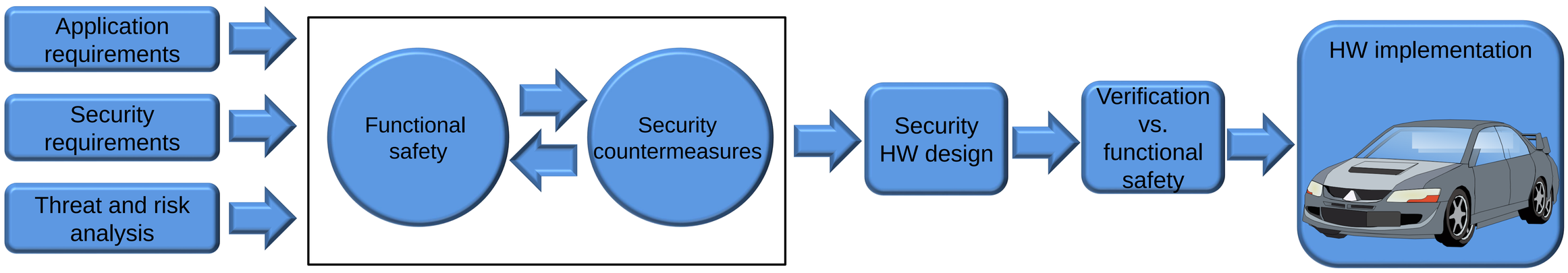
The Safety-Security trade-off is carefully evaluated to do not decrease the performances in terms of :

- Latency/throughput
- Area
- Power consumption

Architectural choices:

- Strong flexibility that allows a SEC-HW for each application-security requirement (e.g. strong security -> AES-256, low security AES-128)
- AES cryptographic algorithms fully compliant with the MACsec IEEE 802.1AE standard
- Key exchange of the cryptographic algorithm fully compliant with the MACSec Key Agreement (MKA) IEEE 802.1X-2010 standard





TTP Impact

Increased security of the automotive environment

- Protection of the data flowing over the internal buses
- Reduction of risk for the user, in particular when safety critical tasks are required
- Strong flexibility in order to cover additional threats, technologies and requirements
- Reduction of costs on high volumes using optimized special circuitry instead of general purpose hardware

Additional security features

- Identification of malicious software, using the hardware as trusted security anchor
- Acceleration of the security hardware using specialized security hardware

Future work

- Security countermeasures to protect the user in case of communication with other car or the infrastructures
- Privacy and authenticity protection when communicating with external entities

TTP Facts

Contact: Luca Fanucci
E-mail: luca.fanucci@unipi.it
TETRACOM contribution: 50,000 EUR
Duration: 01/05/2014-01/05/2015

UNIVERSITÀ DI PISA

RENESAS