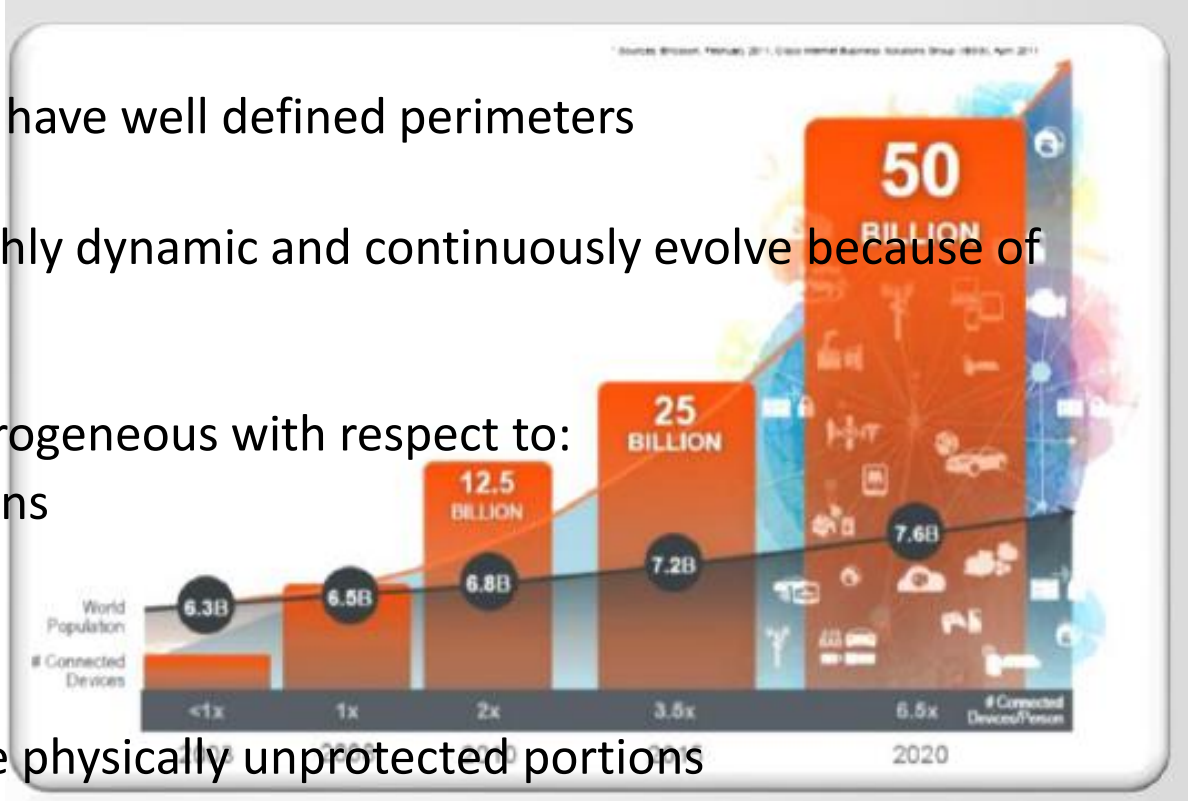
Using a Secure IoT Platform Based on STM32 MCUs

George Kornaros
Univ. of Applied Sciences of Crete, Iraklio, Crete, GR

Lausanne, March 30, 2017

IoT Risks

- IoT systems do not have well defined perimeters
- IoT systems are highly dynamic and continuously evolve because of mobility
- IoT are highly heterogeneous with respect to:
  - Communications
  - Platforms
  - Devices
- IoT systems include physically unprotected portions

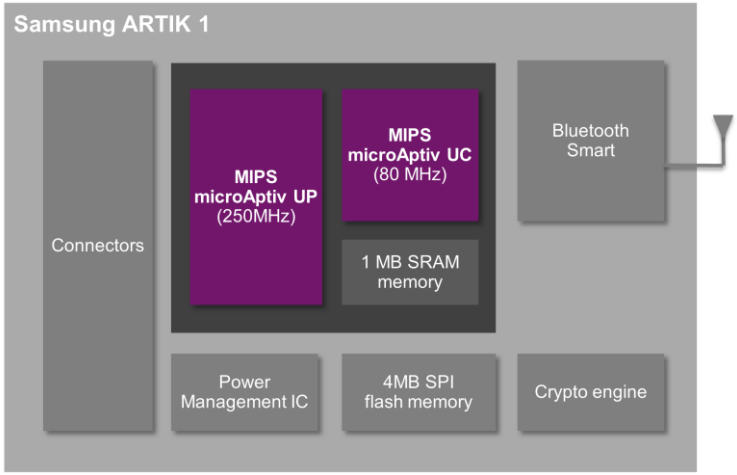


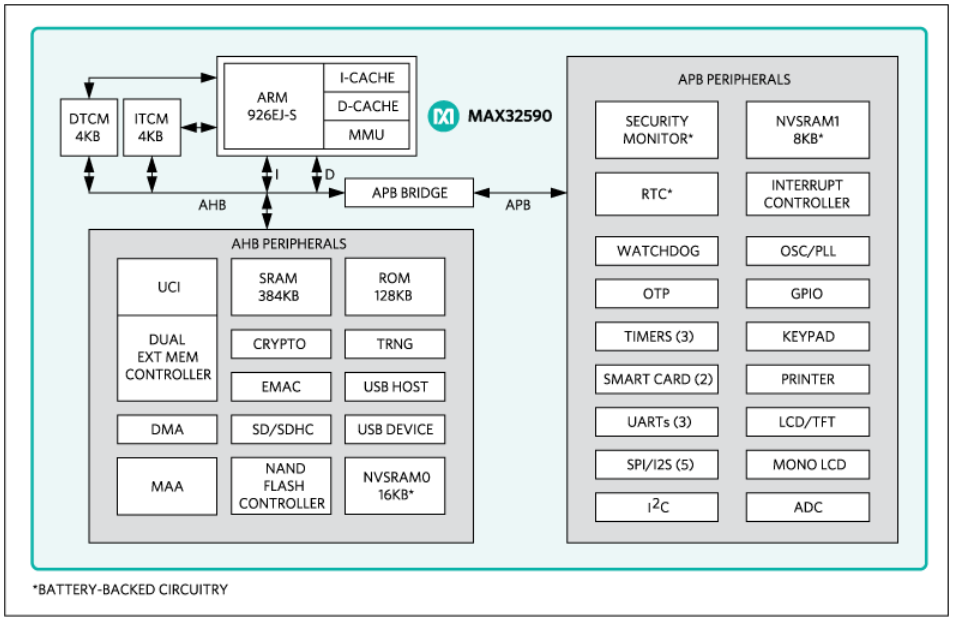
Significantly expanded attack surface

IoT Ecosystem Security

- IoT ecosystem relies on
  - confidential and trusted communications
  - Encryption end to end
  - Sender authentication
- Applications secure execution
  - Root of trust: each ‘stage’ verifies the integrity and/or authenticity of the next stage
  - Process partitioning, memory-space partitioning
- Secure storage, data at rest
  - Encrypt sensitive application data
  - Encrypt sensitive customer personal data

Misc Industrial Solutions





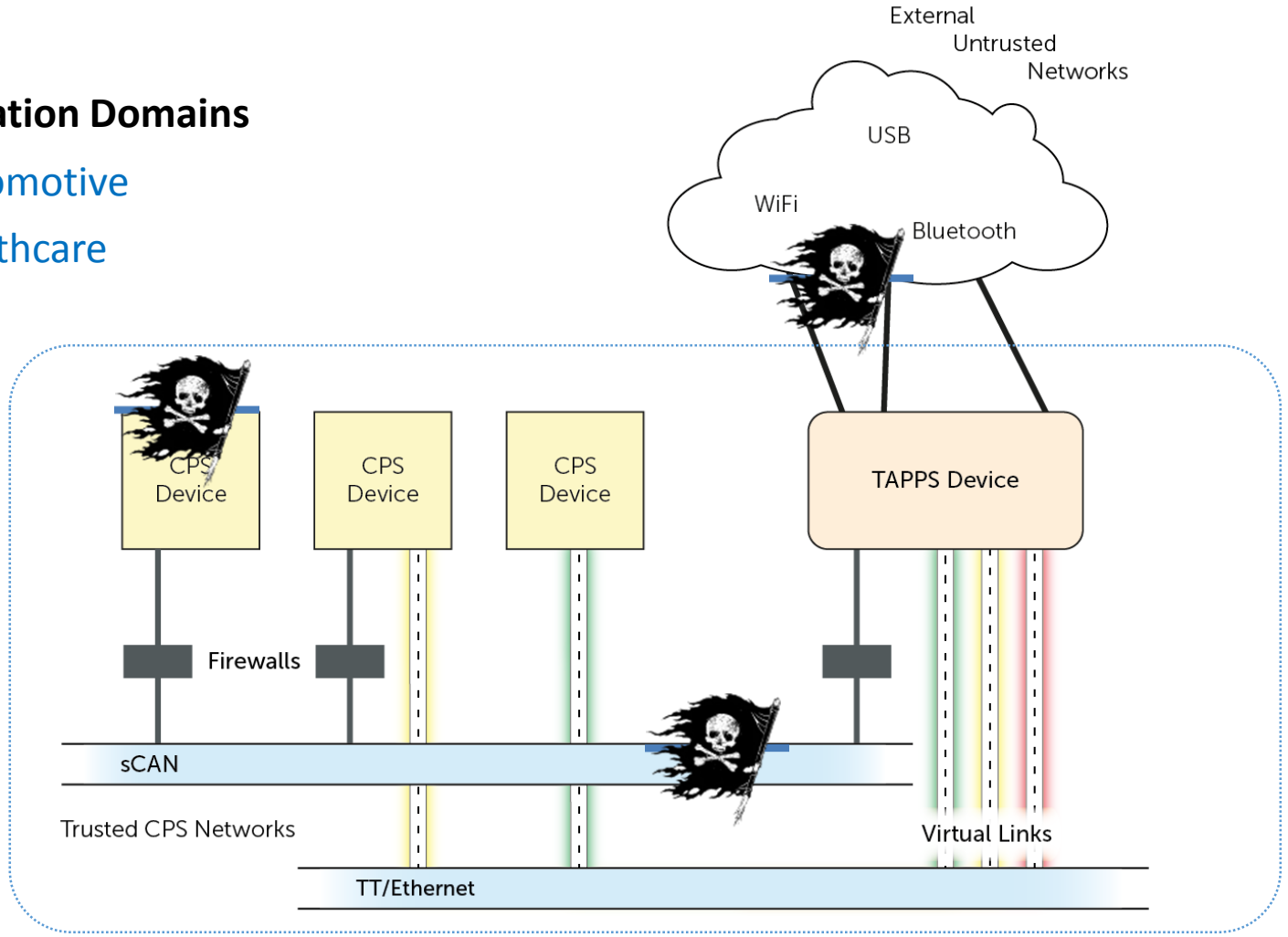
ARTIK 1 features a MIPS32-based, dual-core application processor, flash storage, a crypto engine and Bluetooth Smart radios for communication

DeepCover® embedded security solutions cloak sensitive data under multiple layers of advanced physical security to provide the most secure key storage possible.

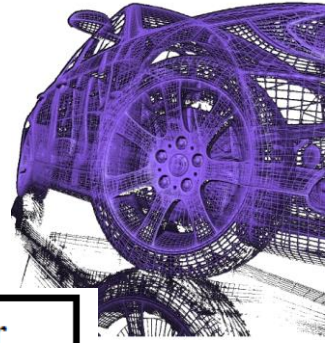
Open IoT Ecosystem

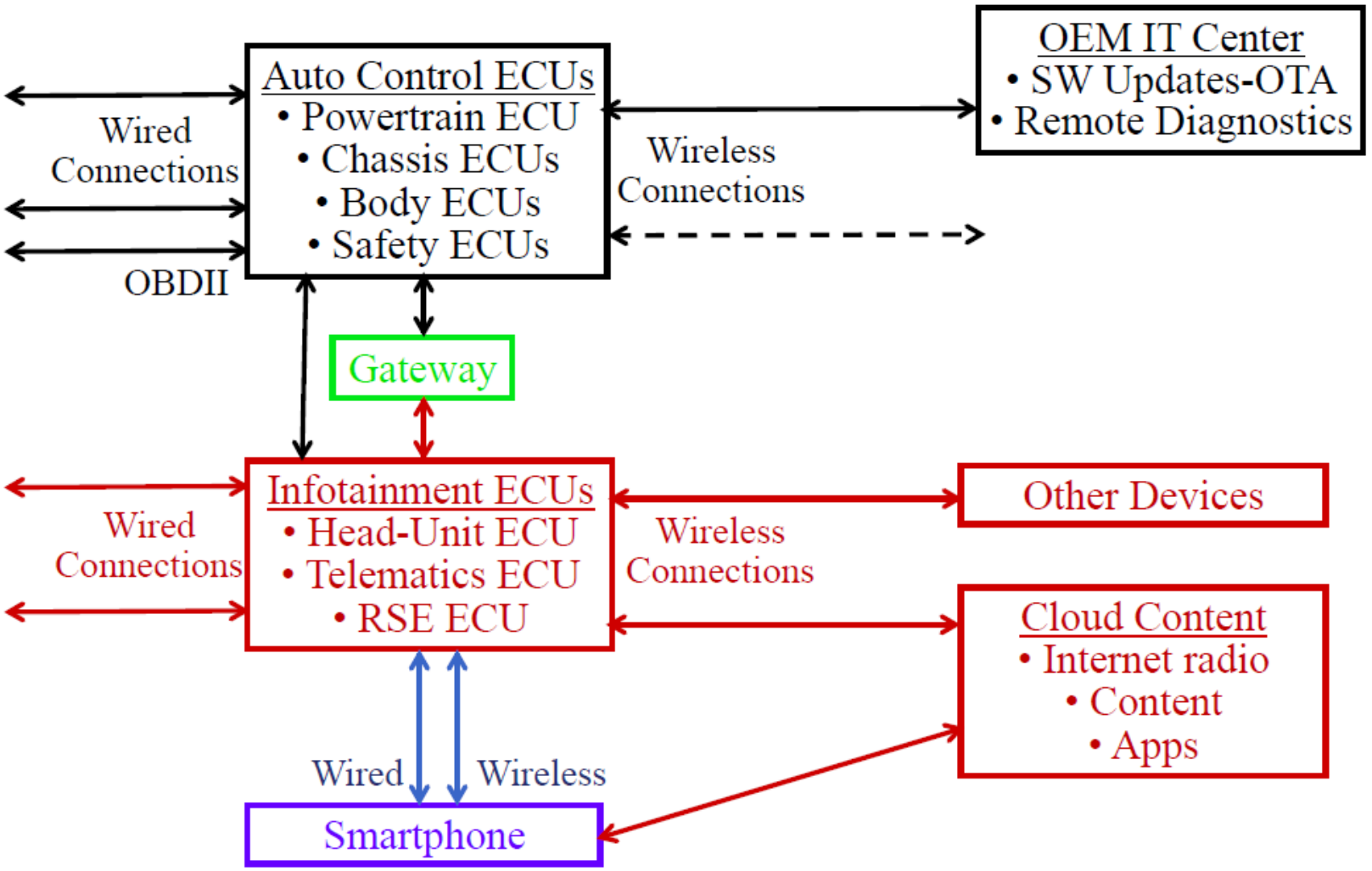
Application Domains

- Automotive
- Healthcare



Research in Connected Vehicle





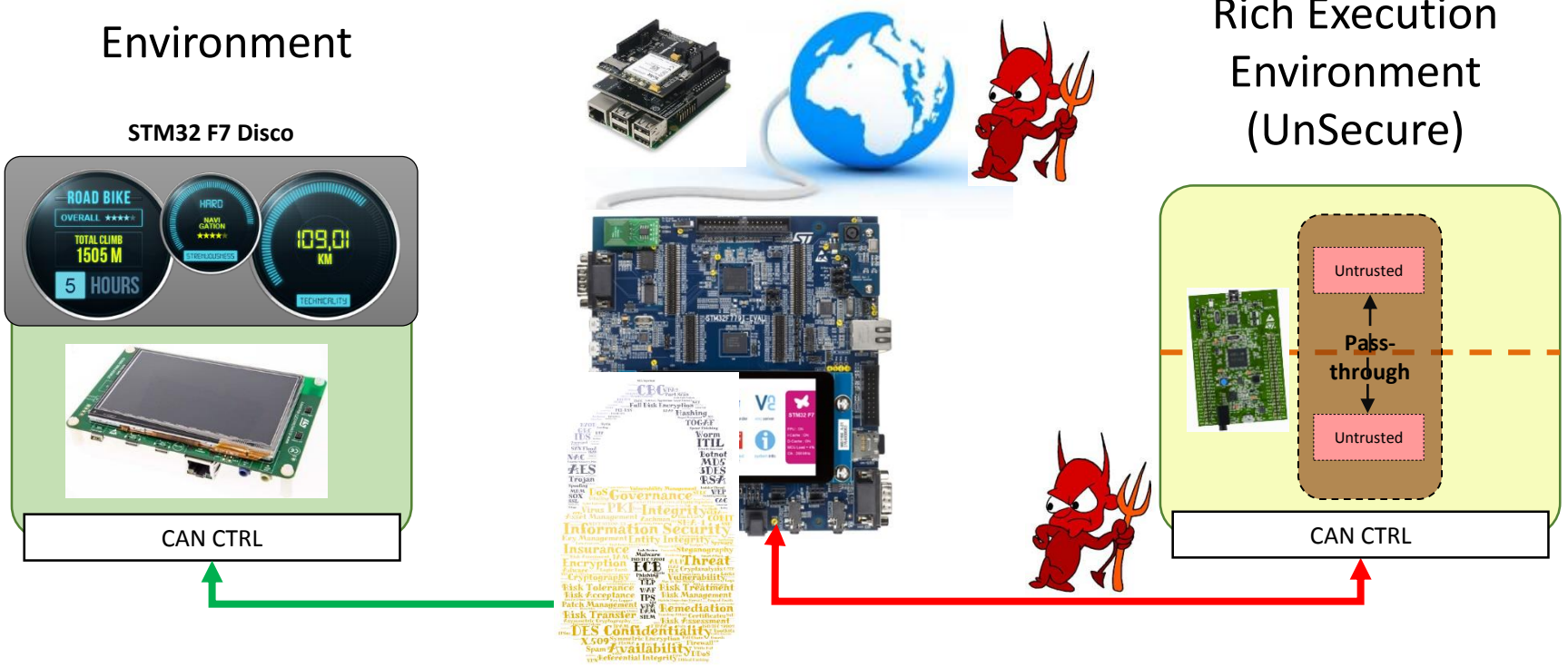
Gateway: STM32F779NI

- STM32F779NI microcontroller
  - with 2-Mbyte Flash memory
  - 512+16+4-Kbyte RAM
  - CAN,I2C,RS232,Eth,USB
  - Cryptographic acceleration

Remote Attack through Network I/Fs

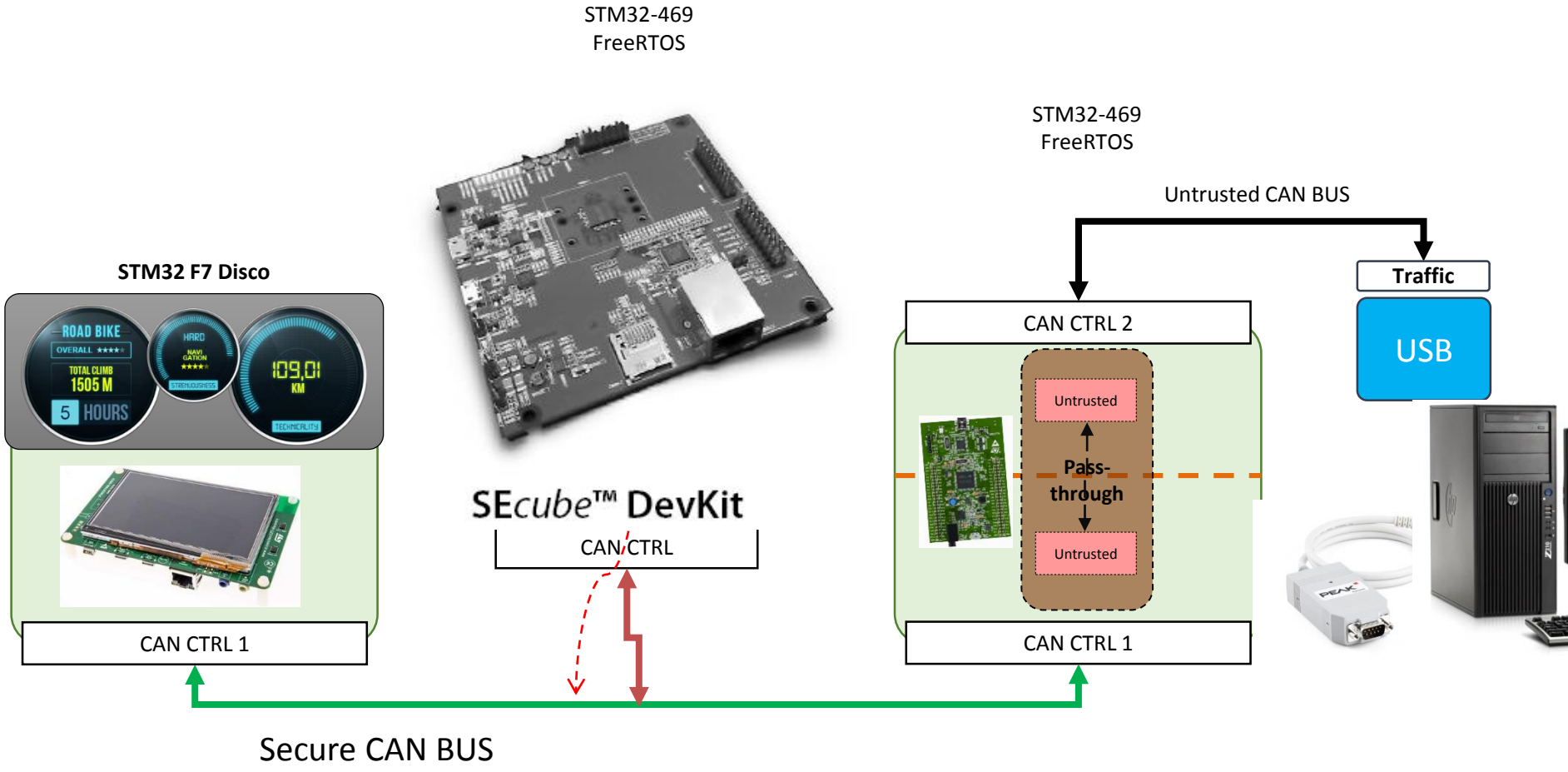
Secure Execution Environment

Rich Execution Environment (UnSecure)

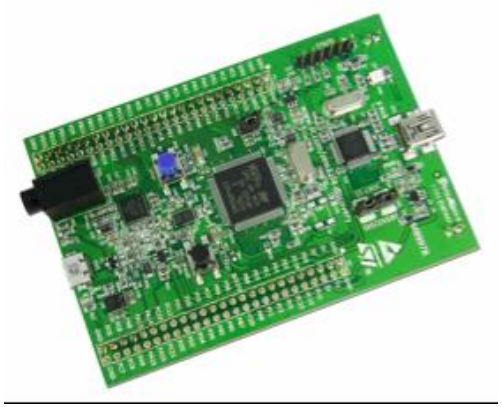


- Remote firmware update, malware attack
- CAN-based attack: compromised CAN messages
- REE tamper ECU functionality

Remote Attack through ODB

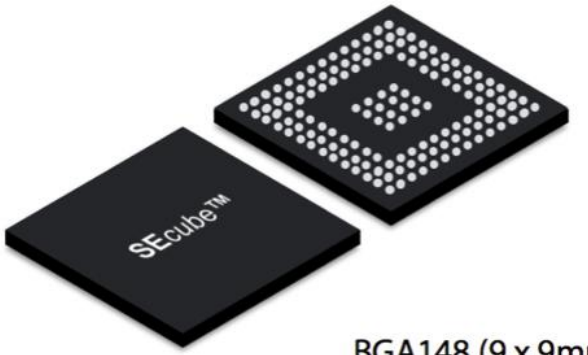


SEcube: Single Chip Security Platform



+

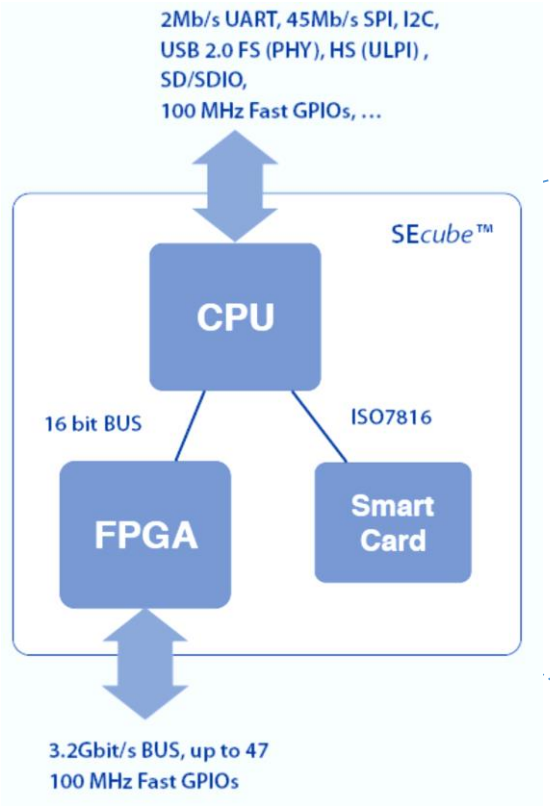
+

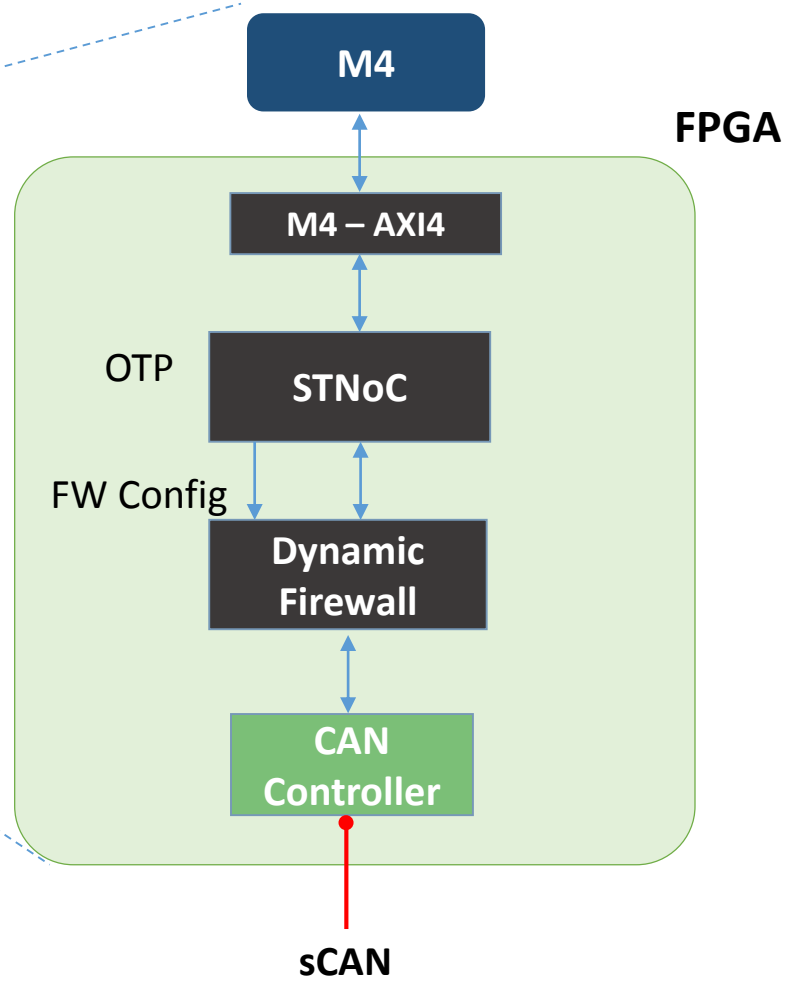


BGA148 (9 x 9mm)

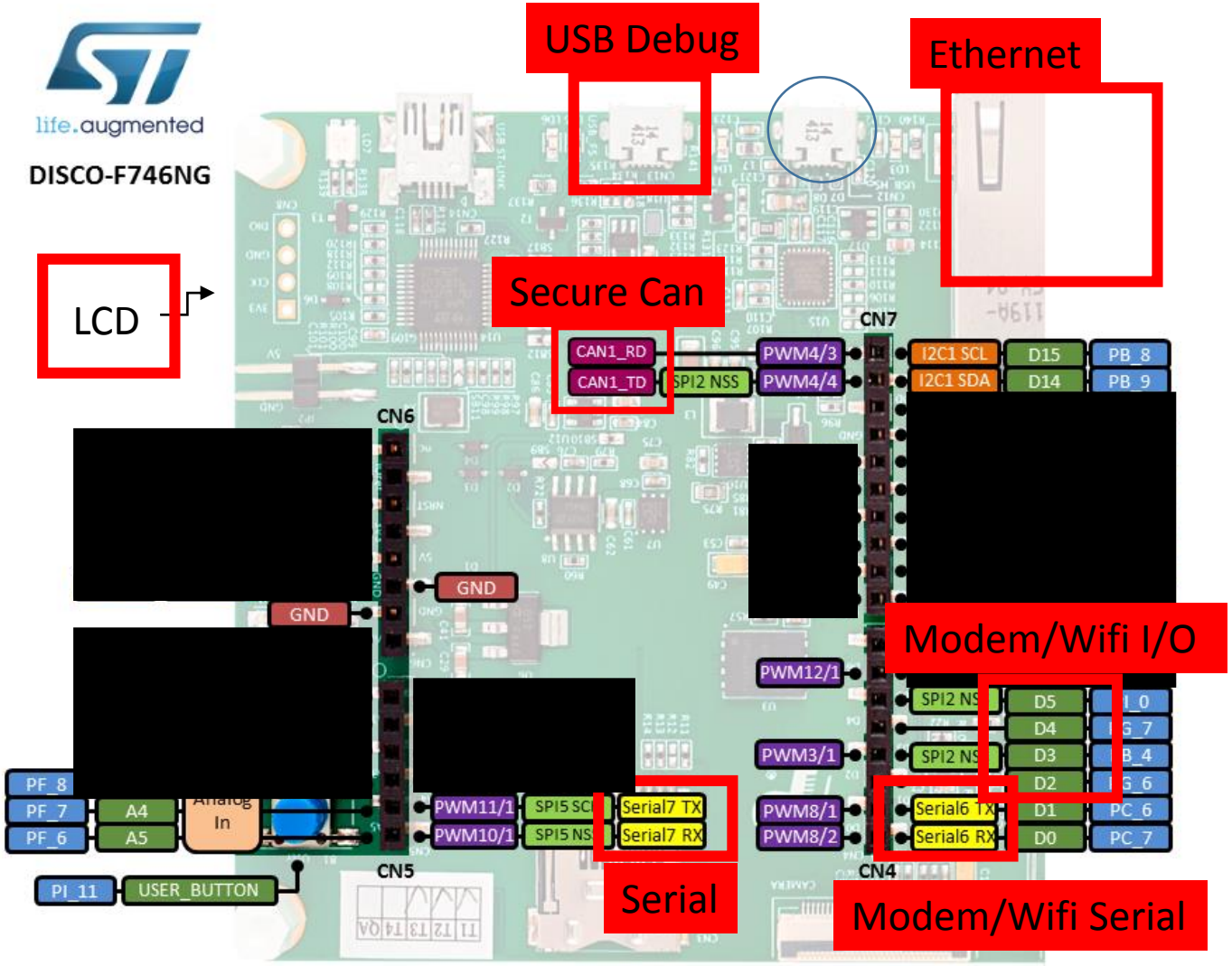
- STM32 M4, Floating Point, Low Power CPU
- FPGA for Hardware Custom Developments
- Security Controller (Smart Card)

SEcube FPGA Firewall

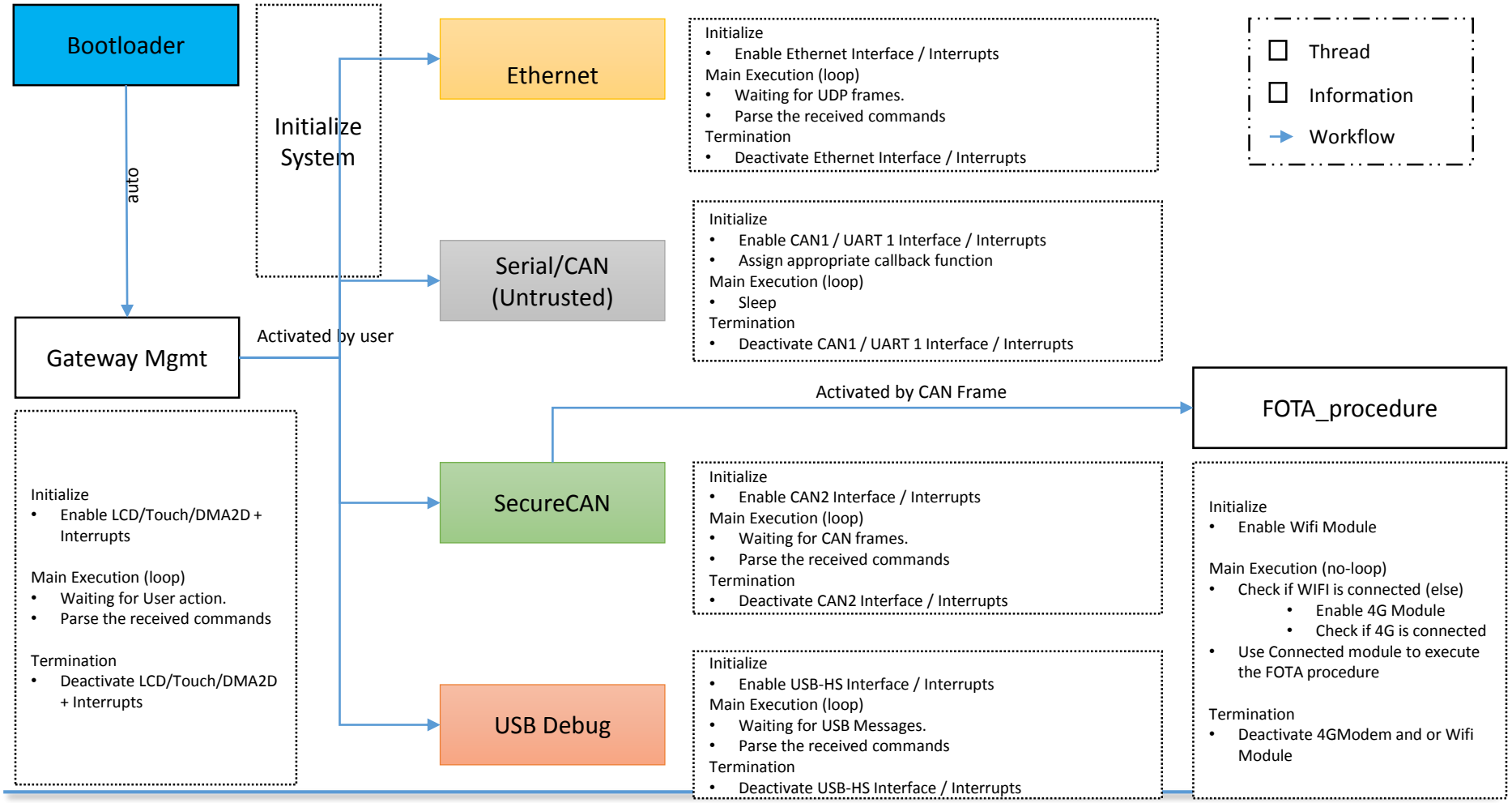




STMF7 Interfacing



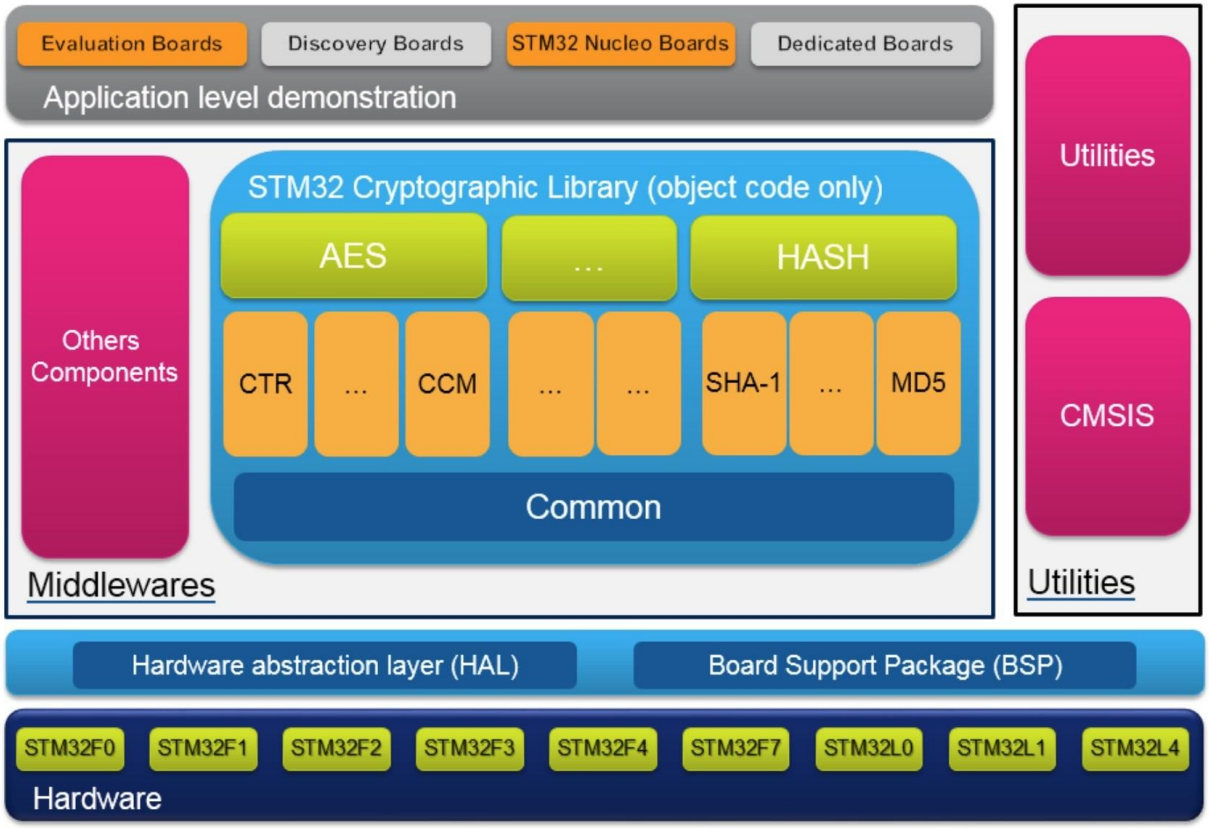
Gateway Architecture



Cryptolib: Cryptographic Modular Middleware

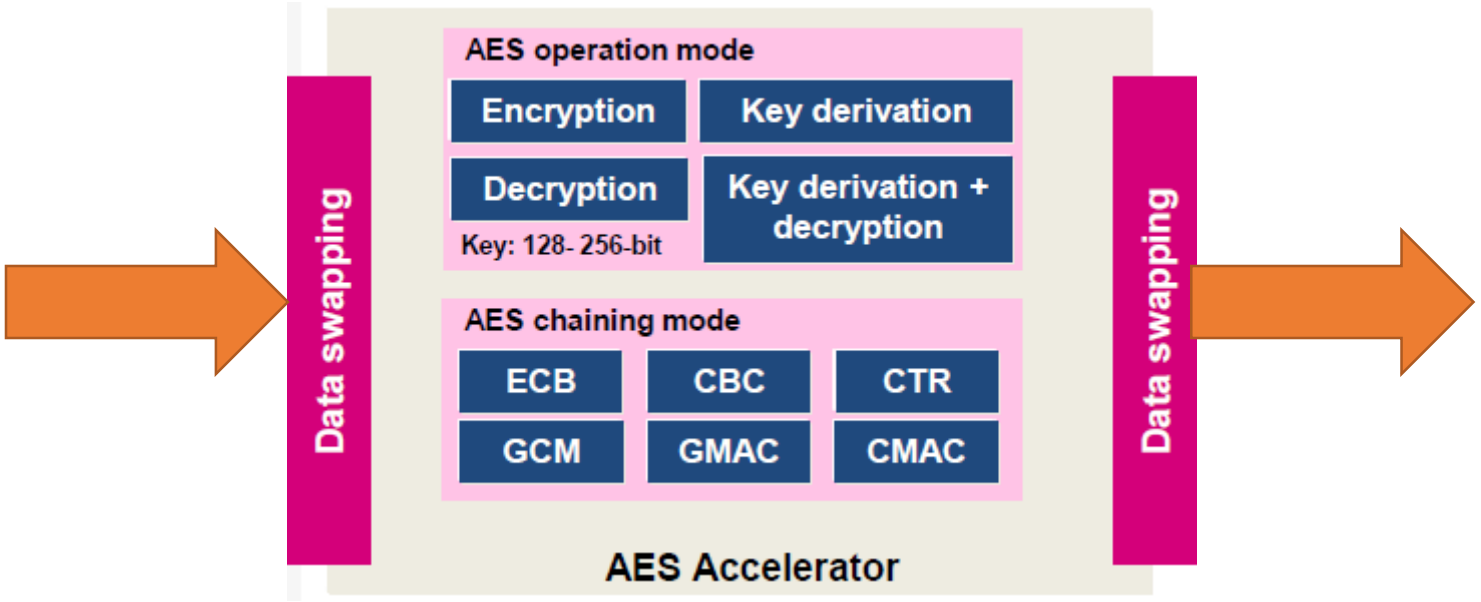
- **AES–256**
- **SHA–512**
- **Elliptic Curve Digital Signature Algorithm (ECDSA)**

- **Certified** by the Federal Information Processing Standard (FIPS), and National Institute of Standards and Technology (NIST).

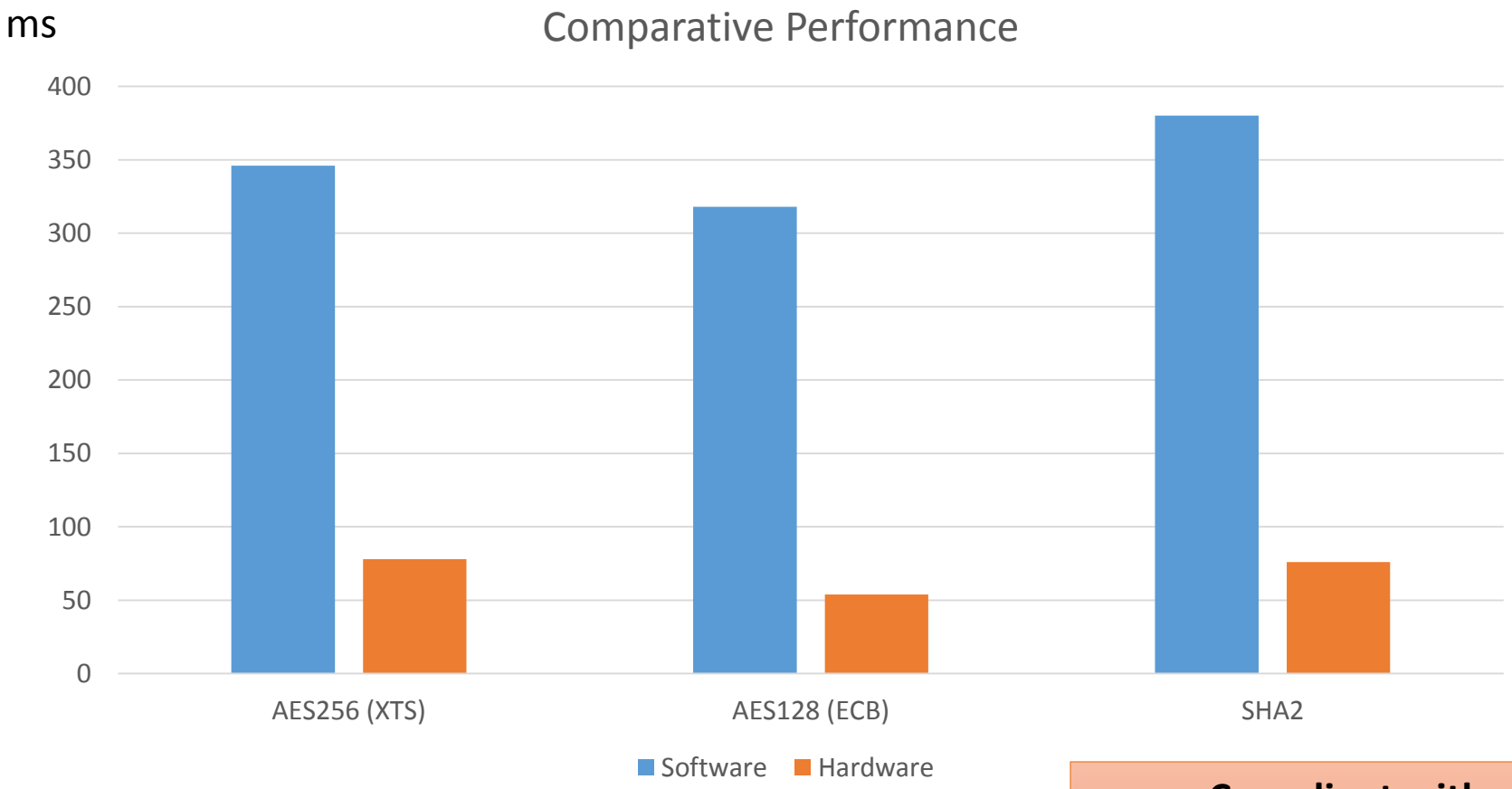


Encryption Accelerators

- **NIST FIPS 197 compliant implementation of AES**



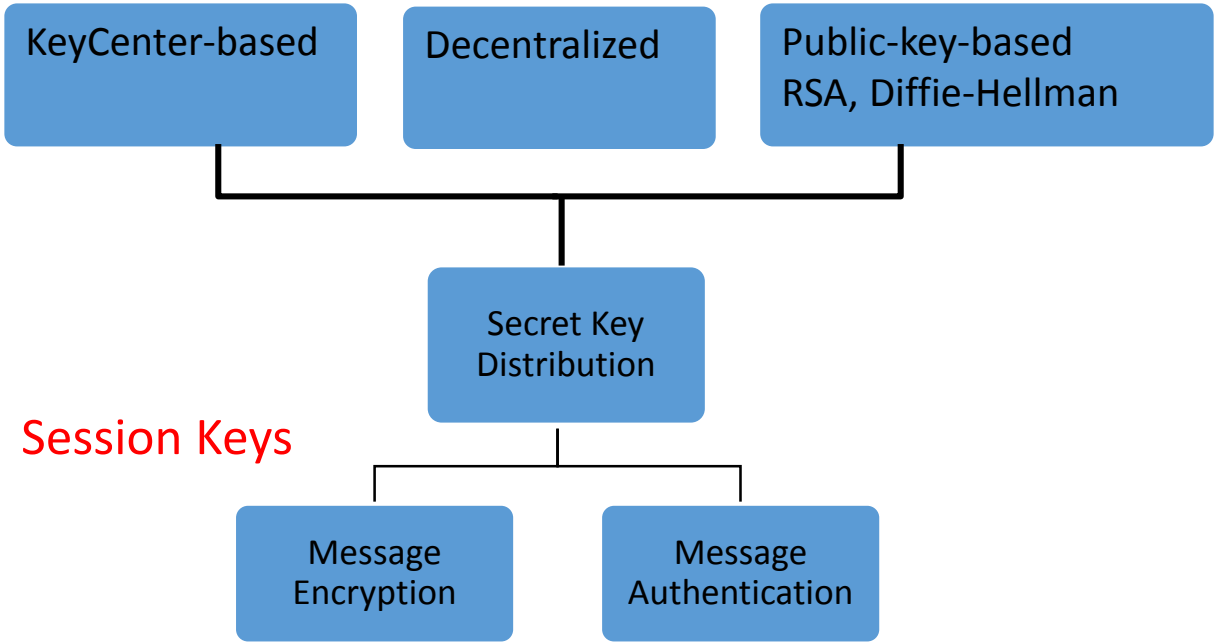
Crypto Acceleration on STM32F779NI



10K Iterations on 16B, CPU Freq: 192 MHz

Compliant with:
FIPS Pub 180-2

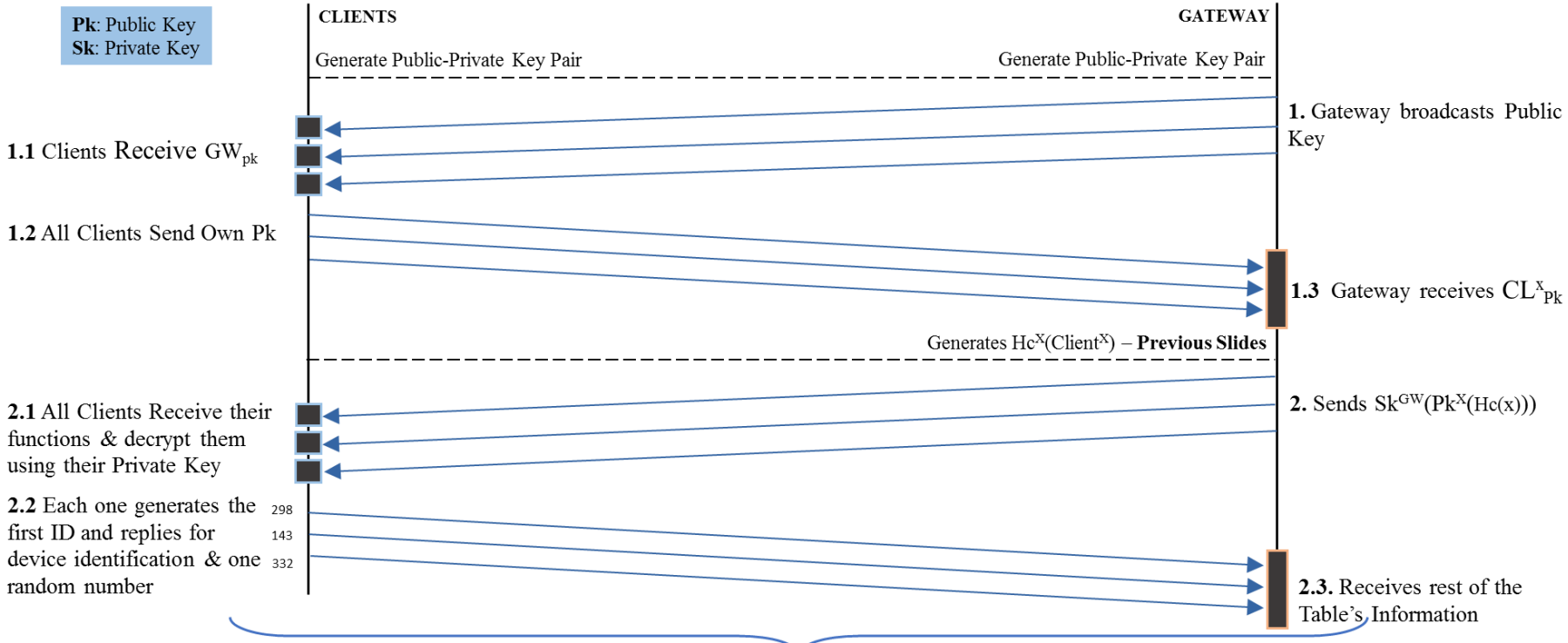
Key Management



- A secret key becomes insecure when used for a long time

RSA-based Key Management

Security on Startup

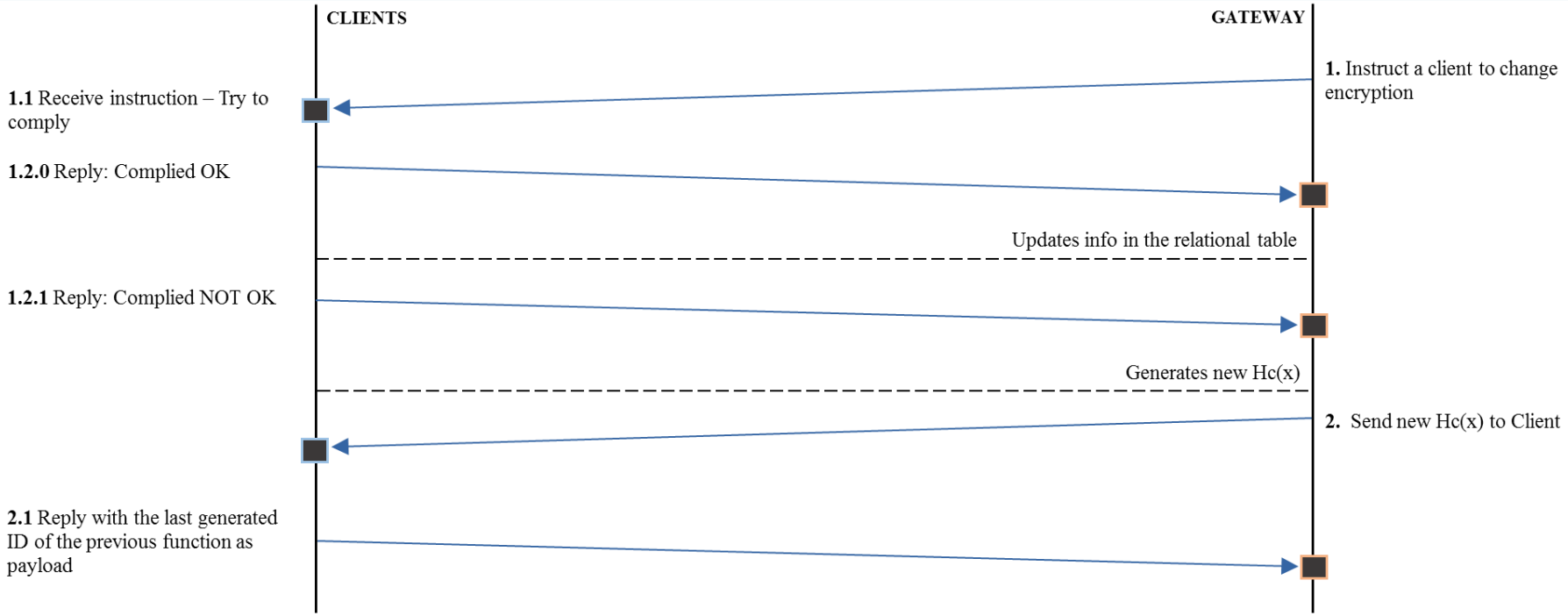


Relational Table Stored In Gateway

ID	H(x)	Encryption Method	Key	Dev.Info	Random #	Last Update
298	X^2/3	IDEA	ffa0b1ca	Rear window	348589	01231100
143	X^4/3	RSA	abc330c	Breaks	234408	01234556
332	X^2	DES	333ccsd	Left Tail Light	348092	01234888

RSA-based Key Management (cont)

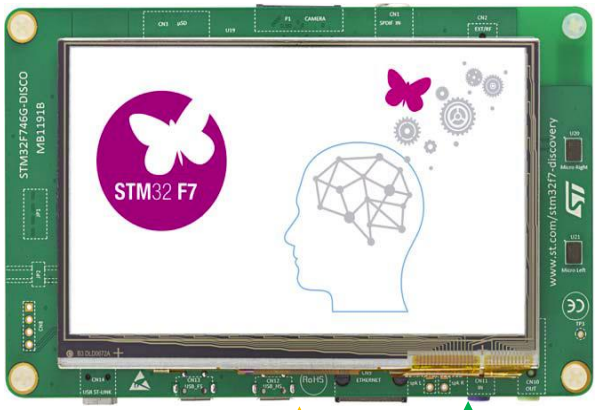
Runtime (per client)



In case of error : Try again or Alert for possible hacking

Mixed-critical Environment using STM32F746

Android/Linux
Apps
Video Streaming
(e.g., GPS
positioning)

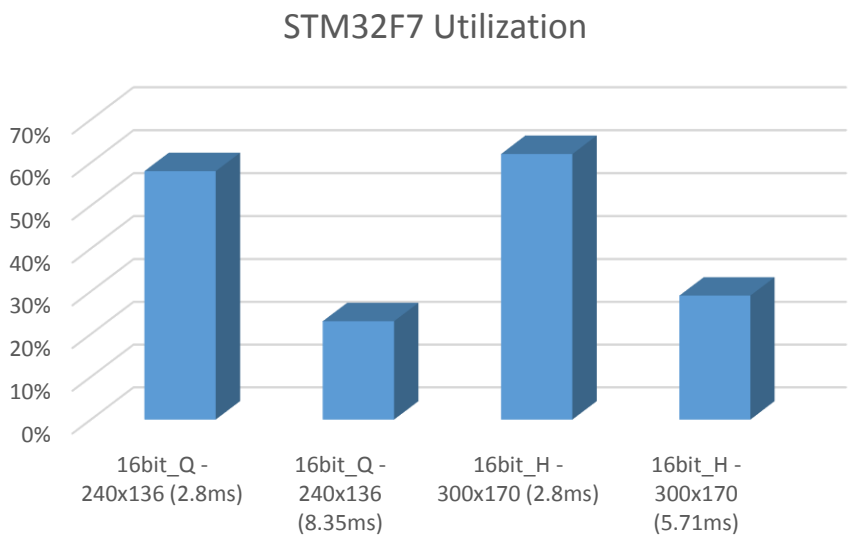


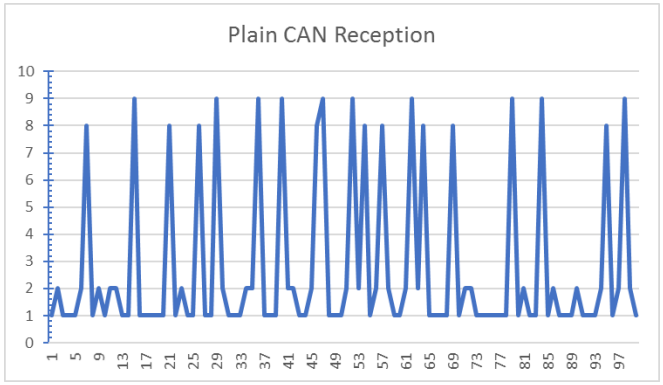
Ethernet

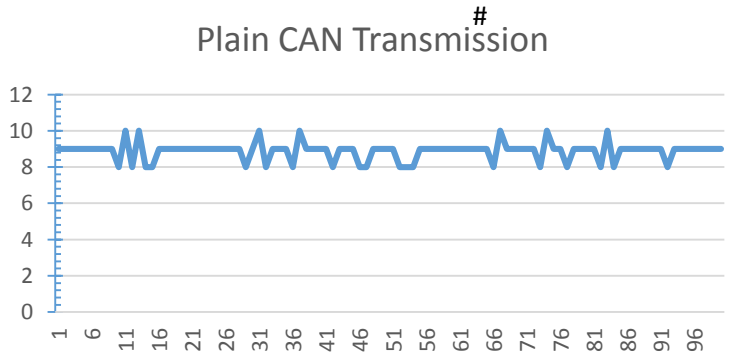
CAN Bus

Headroom with Video Streaming to STM32F7

- Raw (BMP) video streaming over Eth-UDP
- 23.8 fps
  - 16bit_Q - 240x136x2bytes
  - 16bit_H - 300x170x2bytes
- 20-60Mbps Eth BW







Video Streaming on STM32F7

Questions ?

Thank you!

Contact

George Kornaros

Email: kornaros@ie.teicrete.gr

www.tapps-project.eu

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