# ELECTRONICS AT THE CORE OF THE AUTONOMOUS, CONNECTED AND ELECTRIFIED VEHICLES REVOLUTION

https://www.youtube.com/watch?v=Bg8zw1SWiJA&feature=youtu.be

https://www.youtube.com/watch?v=2Y7uLbpehcQ&list=PL13CyHsHfOt1GC19RsPv-FvITnbbnd2e0&index=7


Prof. Ing. Sergio Saponara

**+39 3468790937**

**sergio.saponara@unipi.it**

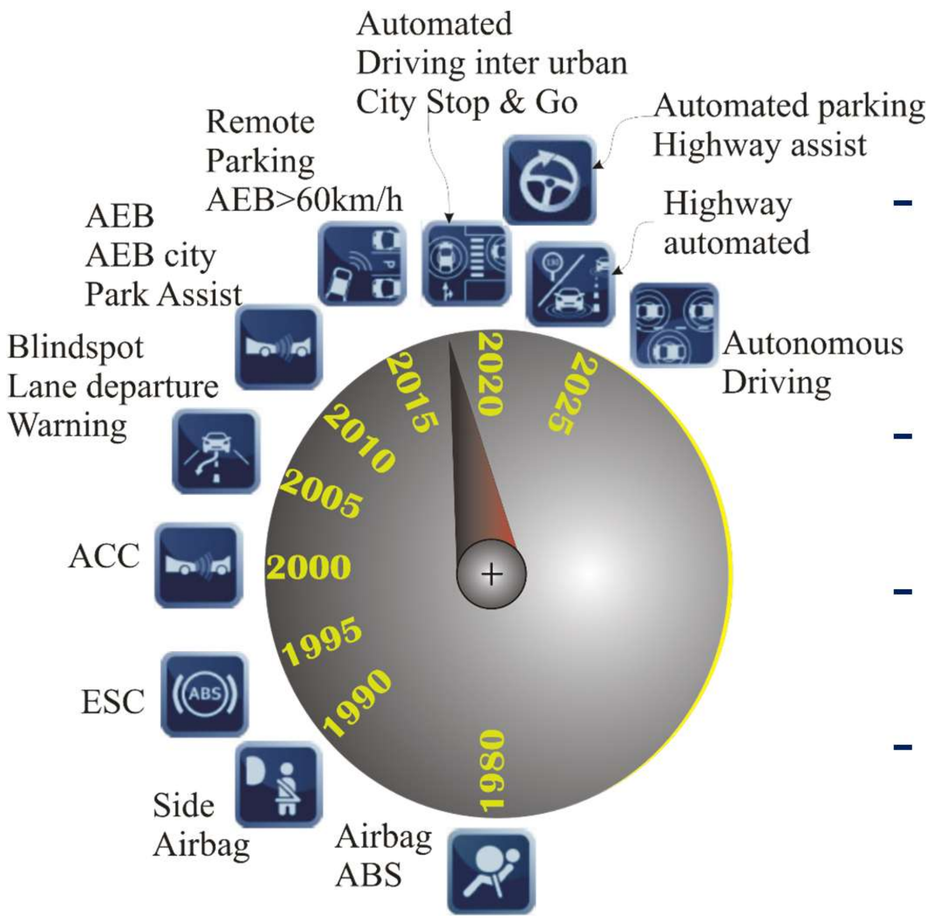
**https://www.linkedin.com/in/sergio-saponara-3031431/**


SIE 2021, Trieste, 8 July 2021

# Outline

- Trends in smart vehicles & intelligent transport systems (ITS) and impact for society/economy
- University pillars: opportunities for continuous education, R&D, and technology transfer in Electronics
- Example R&D case studies:
  - Integrated Power Converters for 48 V micro/mild-hybrid vehicles
  - ITS surveillance X-band Radar
  - Cybersecurity acceleration

# Trends in smart vehicles and ITS




## A research theme of high economical and social impacts

- **Improving safety** (1.3M killed people/year worldwide**, 3.2k/year killed & 242k/year injuried in Italy***)
- **Reducing CO2** (diesel-gate cost 31.3 Billions for carmakers*)
- **Improving life conditions with less pollution/traffic-jam**
- **Improving user experience** (comfort, digital lifestyle, status symbol, inclusive mobility for all, HMI, infotainment)
- **High economic value** (70M of new vehicles/year#, 40M of e-bikes/year sold worldwide##)

***https://www.istat.it/it/files//2020/07/Road-accidents_2019_EN.pdf

**https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

*https://www.reuters.com/article/us-volkswagen-results-diesel-idUSKBN2141JB

#https://www.statista.com/statistics/200002/international-car-sales-since-1990/

##https://www.bike-eu.com/market/nieuws/2020/01/deloitte-study-e-bike-sales-in-2023-at-40-million-units-generating-19-billion-euro-10137172

# Trends in smart vehicles and ITS

**ACE: vehicles are becoming Autonomous, Connected, Electrified**

**Spin-off of the research results towards Robotics, Industry4.0, Logistics, Avionics, Energy Management…**

**Huge investments from Semiconductor and ICT companies and joint alliances with Tier-1&OEM car companies *(e.g. INTEL-BMW, FCA-Google, NVIDIA-Bosch-VW-Continental)***

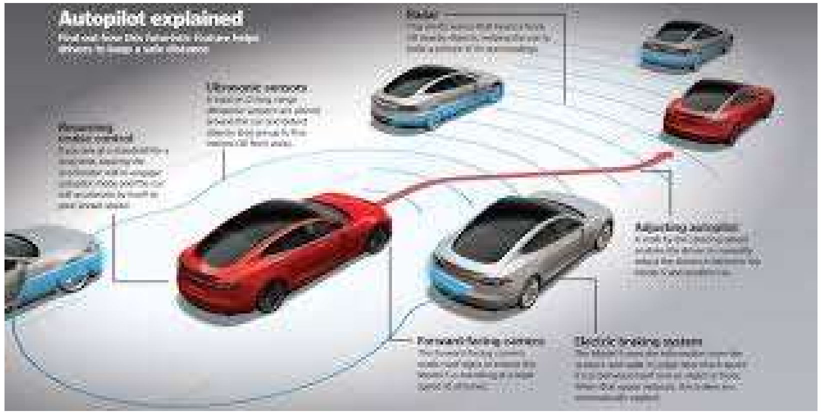
**INTEL ($15.3 billion Mobileye acquisition) estimates the vehicle systems, data and services market per year to be up to $70 billion by 2030***

**VW group committed to $86** billion investments in 5 years in electrified and digital vehicles**

**https://www.reuters.com/article/volkswagen-strategy-idUSKBN27T24O

*https://newsroom.intel.com/news-releases/intel-mobileye-acquisition/#gs.56yyye

# ICT-Automotive industry alliances




**New CE0 of Ferrari (iconic car brand) from an Electronics company (B. Vigna from STMicroelectronics)**

https://www.ferrari.com/en-EN/articles/ferrari-appoints-benedetto-vigna-as-chief-executive-officer

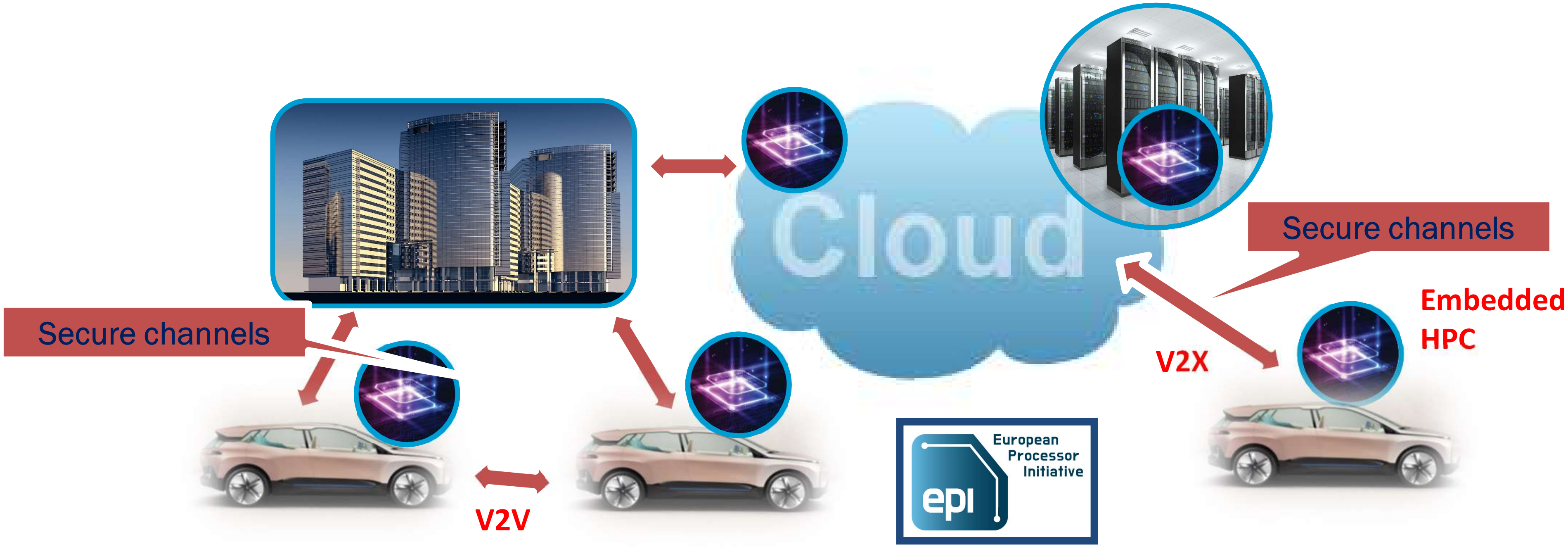
# ICT-Automotive industry alliances

5GAA Association

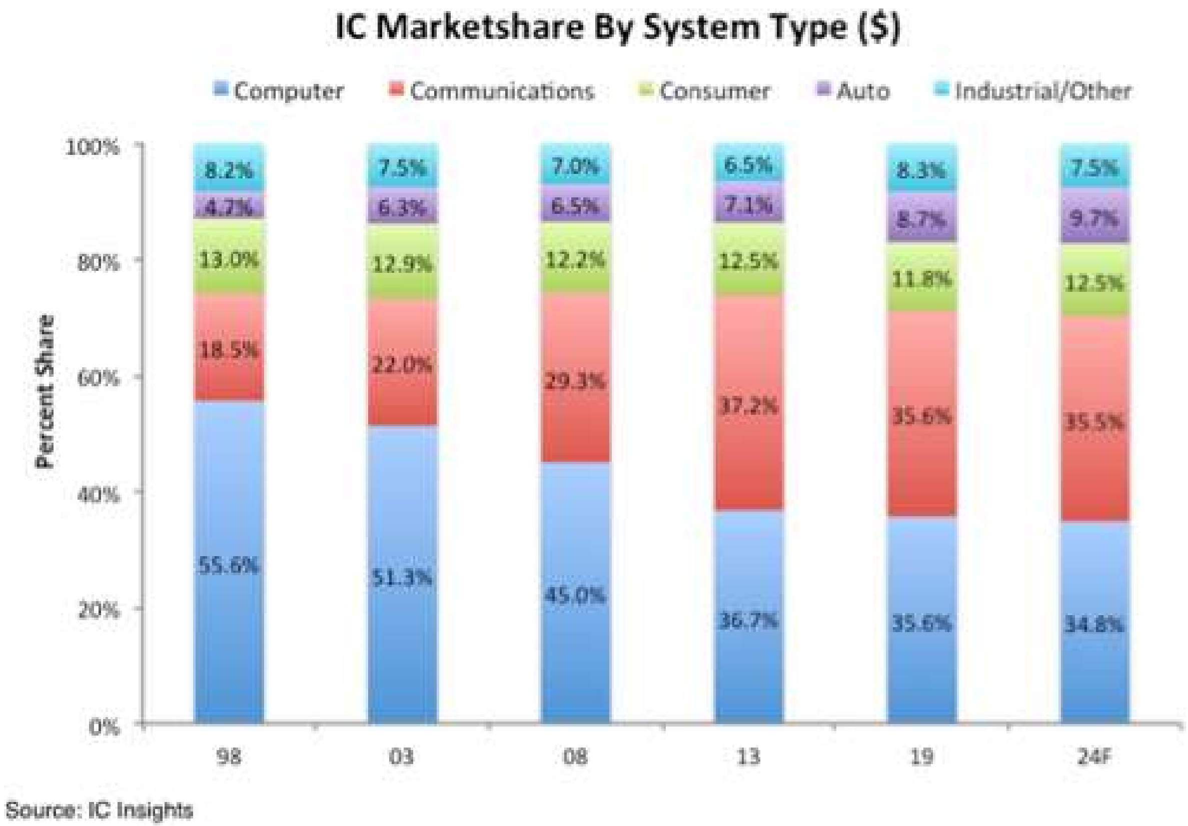
Audi BMW GROUP 中国移动 China Mobile Continental The Future in Motion DAIMLER DENSO ERICSSON FEV

FICOSA Ford gemalto security to be free HUAWEI intel KEYSIGHT TECHNOLOGIES LG NTT docomo

QUALCOMM ROHDE&SCHWARZ SAMSUNG SK telecom T · · Valeo vodafone



# Automotive ICs market trends




## The big dilemma:
## Assisted driving or fully autonomous driving?

## 100% safety not possible

**What is possible? a statistics of incidents, injured/died people in favour of ADAS**

**Beware of legal issue!!!!!**        **Beware of psychological issues!!!!!**

# Outline

- Trends in smart vehicles & intelligent transport systems (ITS) and impact for society/economy
- University pillars: opportunities for continuous education, R&D, and technology transfer in Electronics
- Example R&D case studies:
  - Integrated Power Converters for 48 V micro/mild-hybrid vehicles
  - ITS surveillance X-band Radar
  - Cybersecurity acceleration

# Vehicle as a platform for pervasive R&D in Electronics

**RF & mmWaves**
(mmW Radar, 802.11p/bd V2X, 5G C-V2X, GNSS)

**Sensors AFE & signal processing**
(Image, Radar, Lidar, Ultrasonics, IMU,..& fusion in real-time)

**Power Electronics**
(SiC&GaN devices, DC/DC converters, inverters, on-board chargers, 12V→48V→ 400V→800V, energy storage&BMS)

**digital twin, RT robust & embedded control**

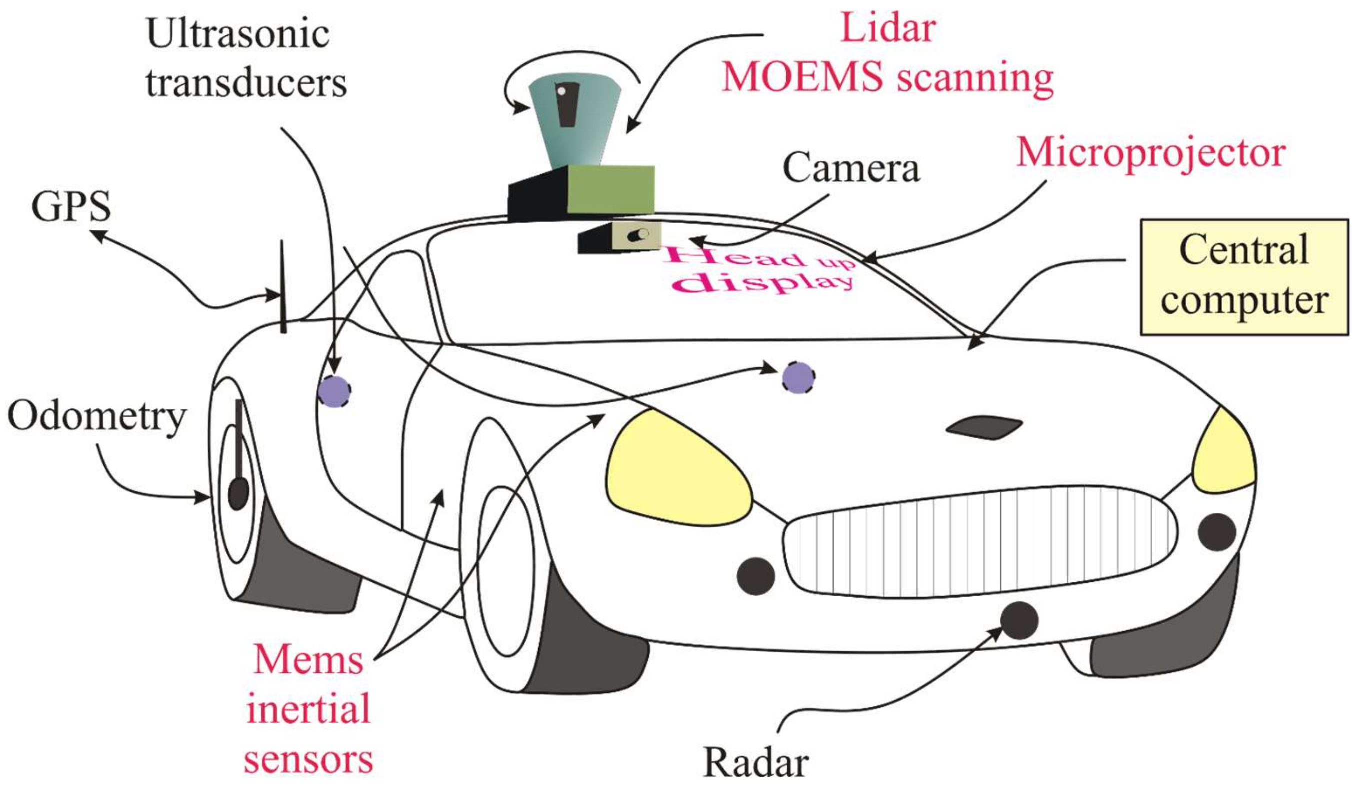
**Opto-electronics**
(Low-cost Lidar, high-speed networking, FBG sensors, lights/display, SiPh)

**Predictive-diagnostic**
(thermal, EMI/EMC, electrical, ageing, vibrations,..) for functional safety

**Sensors device & technologies** (MEMS/MOEMS)

**eHPC & memories** (multi-core, AI & security accelerators, high SIL in harsh environments)

# Example: Sensing & Measurement Perspective




## What?

obstacle detection

## Where?

position and direction of cars and obstacles

## When?

car to obstacle relative speed

## Measurement Performance

**range**, **resolution** and **accuracy** of distance, angles & speed?

reliable (**uncertainty, repeatability**) measures in harsh environment ?

secure (**trusted, identified, private**) measures?

sustainable (low-power, low-cost, life-cycle)

# Scientific R&D funding

**FP7 ATHENIS-3D (2013-2017)** *Automotive tested high-voltage and embedded non-volatile integrated SoC platform with 3D technology*, EU project funds 6 M€, UNIPI funds 0.3 M€, UNIPI leadership **WP5 Test chip development**

**H2020 Hiefficient (2021-2024)** *Highly EFFICIENT and reliable electric drivetrains based on modular, intelligent and highly integrated WBG power electronics modules, project budget 42 M€, UNIPI budget 0.45 M€, UNIPI leadership* ***T3.3 Digital twin WBG-based power converters***

**H2020 EPI (2018-2021)** *European Processor Initiative, EU project funds 80 M€, UNIPI funds 1.55 M€, UNIPI leadership* ***WP9 Cybersecurity***

**H2020 TEXTAR0SSA (Apr 2021-2024):** *Towards EXtreme scale Technologies and Accelerators for euROhpc hw/Sw Supercomputing Applications for exascale, lead of CINI (budget 1.2* M€, UNIPI linked part), *project budget 6M€, UNIPI leadership* ***WP2 IP accelerators*** *(AI, mixed-precision&posits, cybersecurity)*

**H2020 The European Pilot (1 0ct 2021-2024):** *Pilot using Independent Local & Open Technologies, lead of CINI (budget 1* M€, UNIPI linked part), *project budget 30M €*

# Continuous Education

Electrification and digitization of vehicles and ITS → needs of

New (young, 25-30 yrs) engineers expert in vehicular electronics
(device, circuit, system levels; analog, digital; ele & opto) not only in semi conductor industry but mainly in mechanic/mechatronic companies

→ new L8/LM29 (or simply, new curricula in current Electronics Eng.), degrees (e.g. Embedded Mechatronics)

→ more electronics courses in industrial engineering degrees (HW & embedded security LM Cybersecurity, Vehicular Electronics in LM Vehicle Eng., Electronic System for Robotics in LM Robotics and Control Engineering)

Re(Up)skilling of employees (35-55 yrs) with industrial eng. background
Specific short courses (50-100 h/class)
(co-funds available from EU & local institutions; consolidating job positions)

New opportunities available from the PNRR
*(Missione 3: infrastrutture per mobilità sostenibile; Missione 2: rivoluzione verde e transizione ecologica)*

# Continuous Education

https://www.continental.com/en/press/press-releases/2021-01-22-qualification-campaign-246248

**Automotive Electronics & Powertrain Electrification**
12 CFU Corso Perfezionamento, S. Saponara director, re-skill course for 100 Engineers of Vitesco (Continental), 4 classes, 645 h/14 teachers, 200k€ funding, Confindustria/Reg. Toscana support

**2 international summer schools** about 5G (1 edition) and IoT (7 editions, 2 times co-funded by IEEE CAS seasonal school scheme) including circuits&systems vehicular connectivity lectures


New proposal "e-Mobility: Digital & Electrified Products & Systems", 150k€, Pierburg, Magna, Azimuth Benetti, Wass (Leonardo), CNA/Comune Livorno/Regione Toscana support

# Initiatives for students on vehicles at UNIPISA

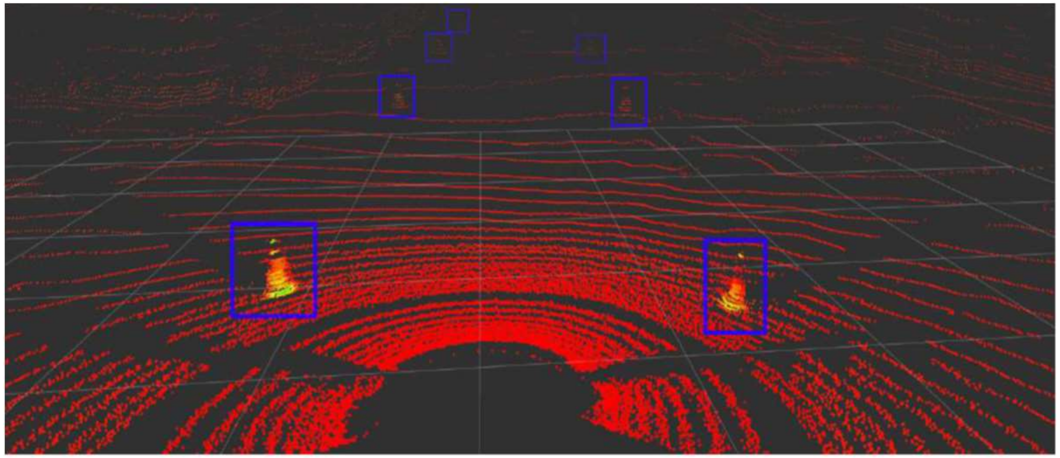
MOVET

Association of Universities + Institutions + 15 Industries operating in Tuscany


E-Team

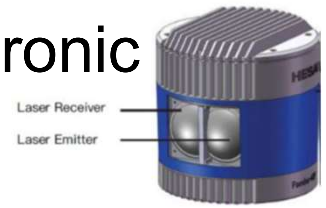
Formula SAE

(Kerub car)



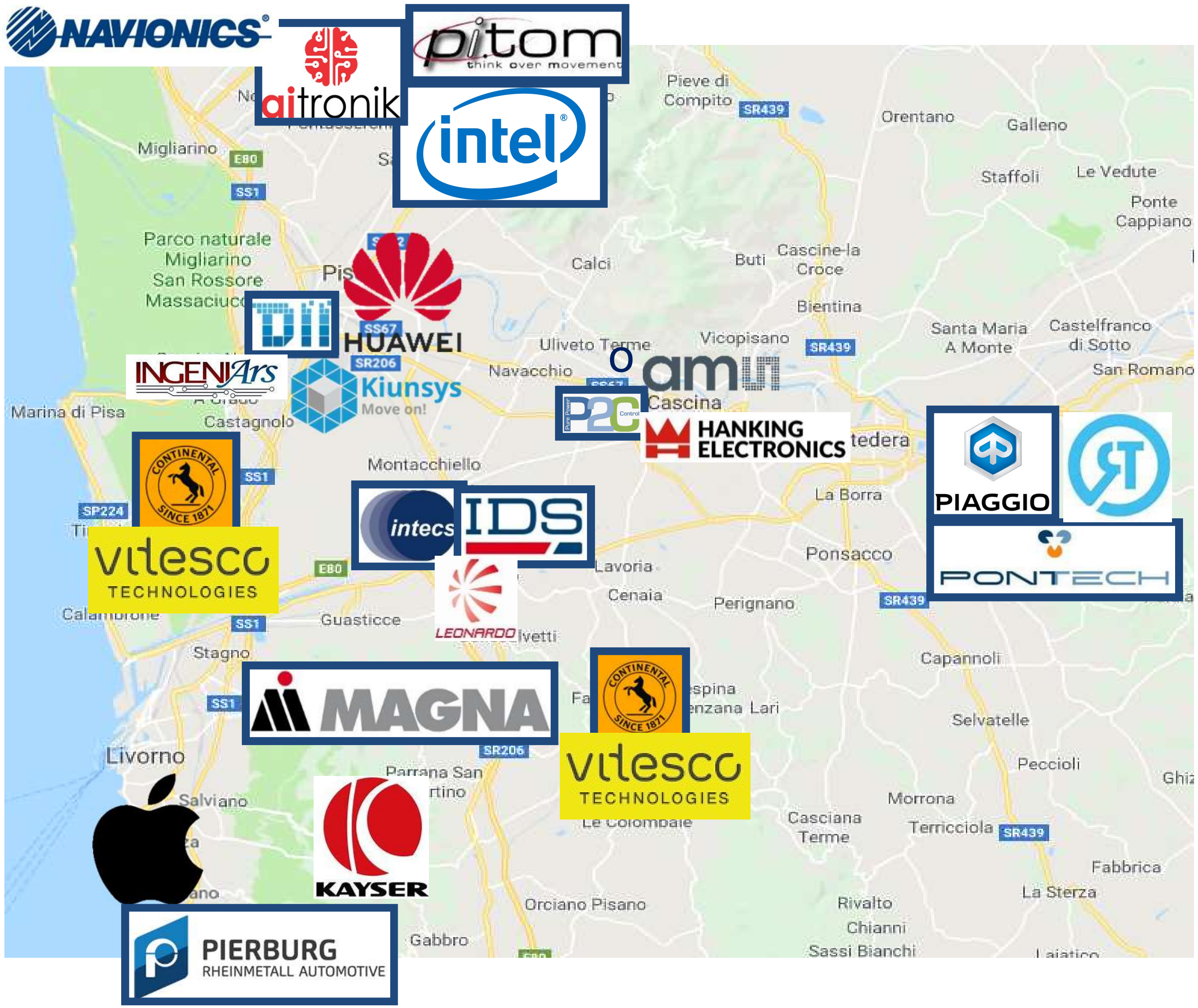
Since 2021 Formula SAE driverless (e.g. cone-recognition with Pandar 40 lidar)

6 Students from Electronic Engineering



# Attract new investments in Italy
# (the Pisa-Livorno Area case study)

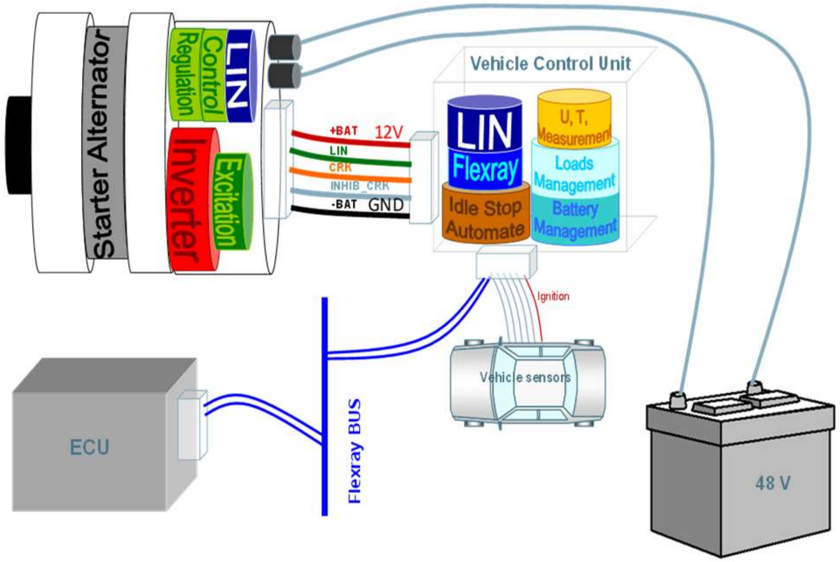
http://www.movet.org/toscana-valley-anche-le-major-hi-tech-lapprezzano/

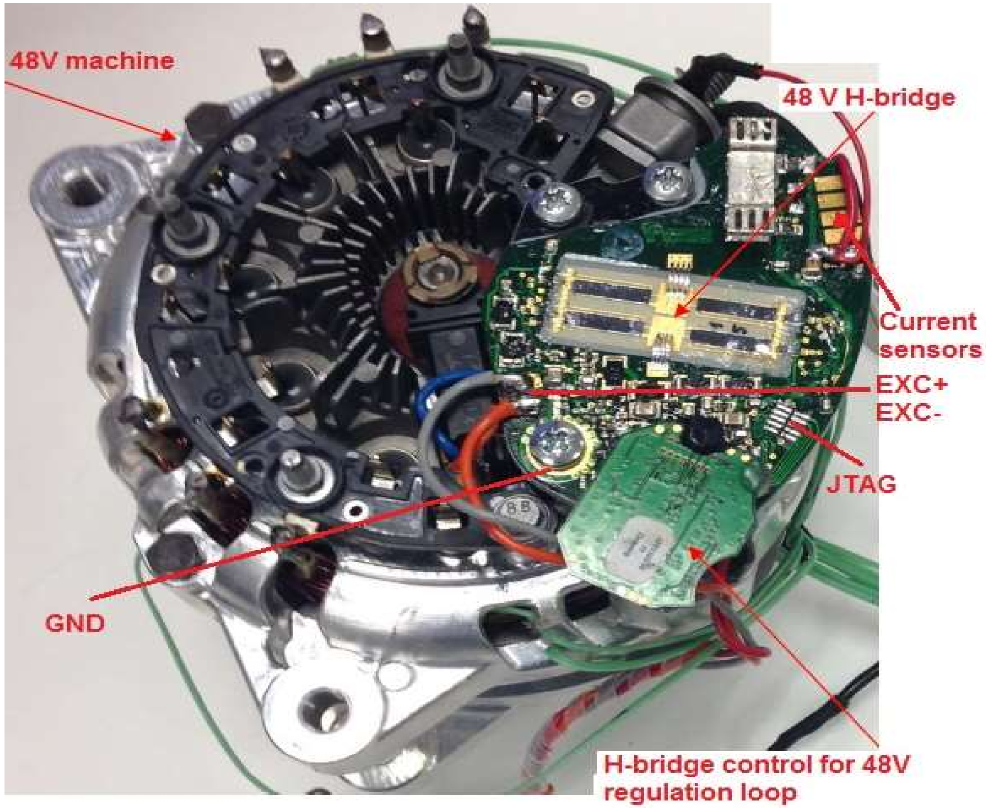


# Outline

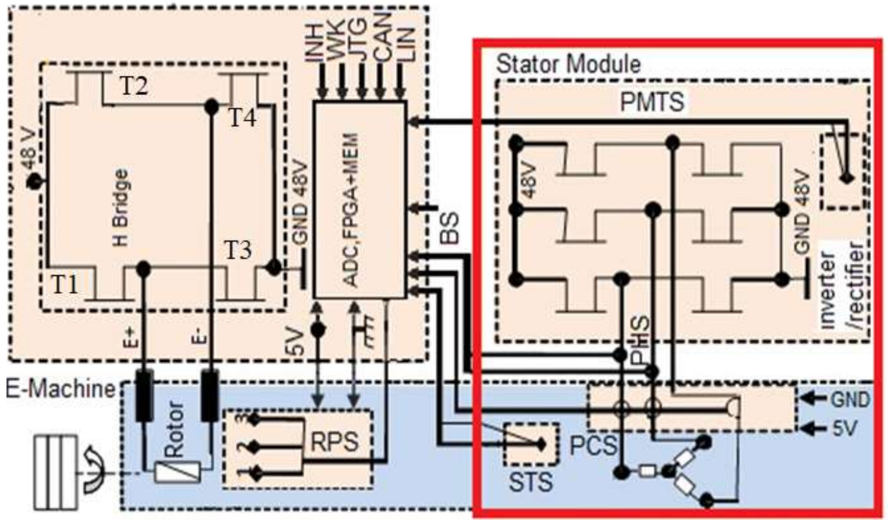
- Trends in smart vehicles & intelligent transport systems (ITS) and impact for society/economy
- University pillars: opportunities for continuous education, R&D, and technology transfer in Electronics
- Example R&D case studies:
  - Integrated Power Converters for 48 V micro/mild-hybrid vehicles
  - ITS surveillance X-band Radar
  - Cybersecurity acceleration

# Integrated Power Converters for 48 V micro/mild-hybrid vehicles



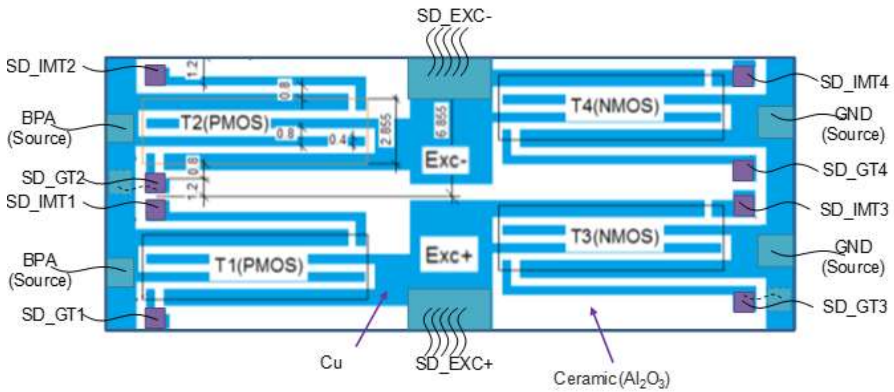



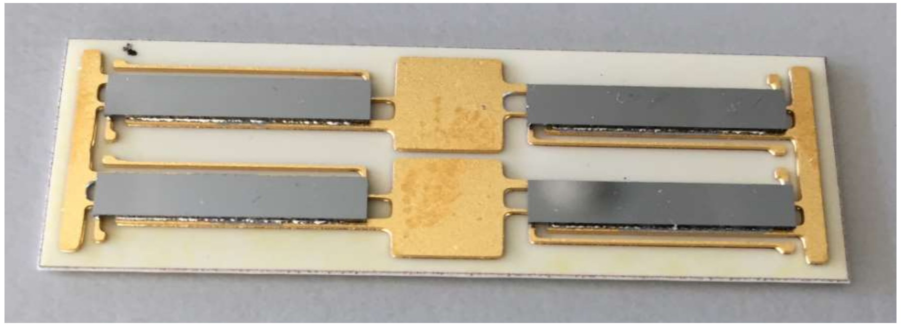

Electric Drives and Power Chargers: Recent Solutions to Improve Performance and Energy Efficiency for Hybrid and Fully Electric Vehicle, IEEE Vehicle Tech. Mag. 2020

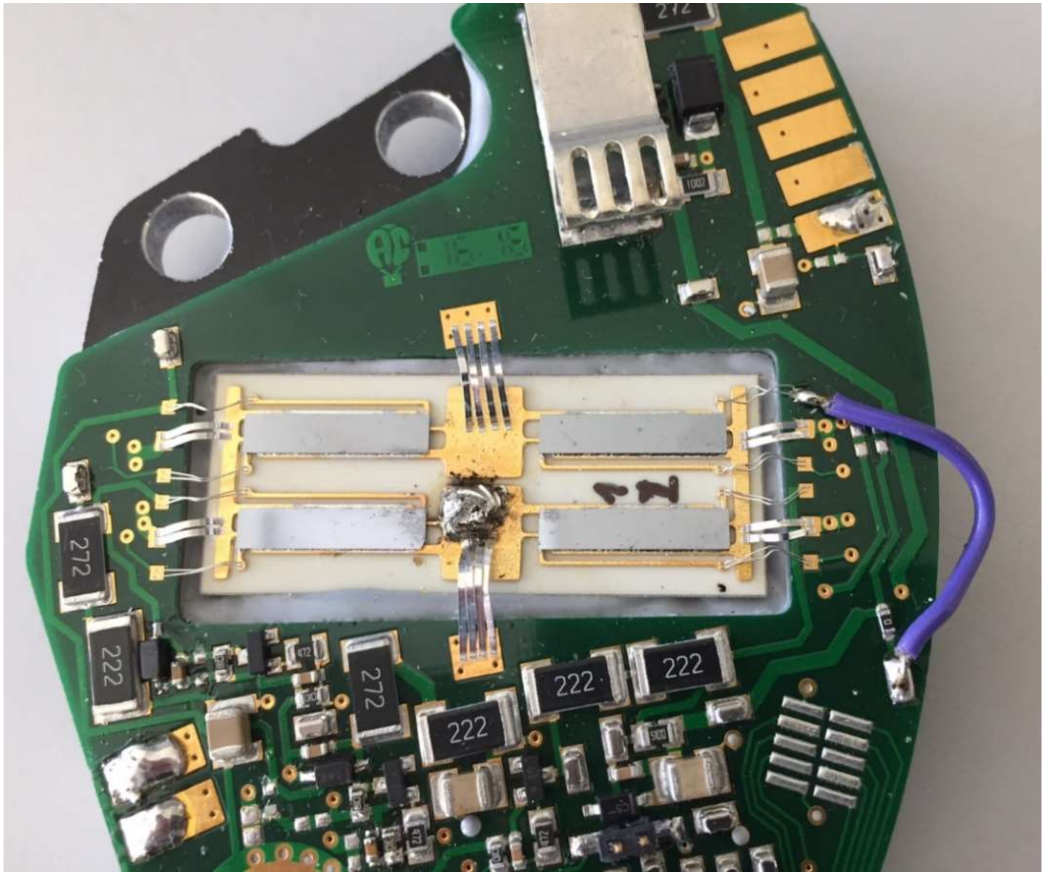


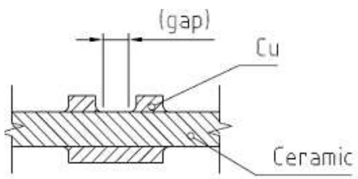

***Collaboration with***
***Valeo & AMS in FP7 Athenis3D***
***MIT in MISTI seed fund scheme***

# 48 V power bridge in 180 nm HVMOS





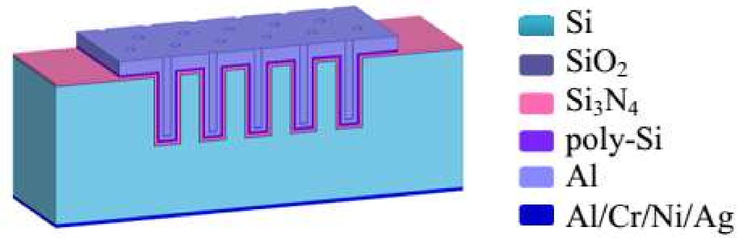


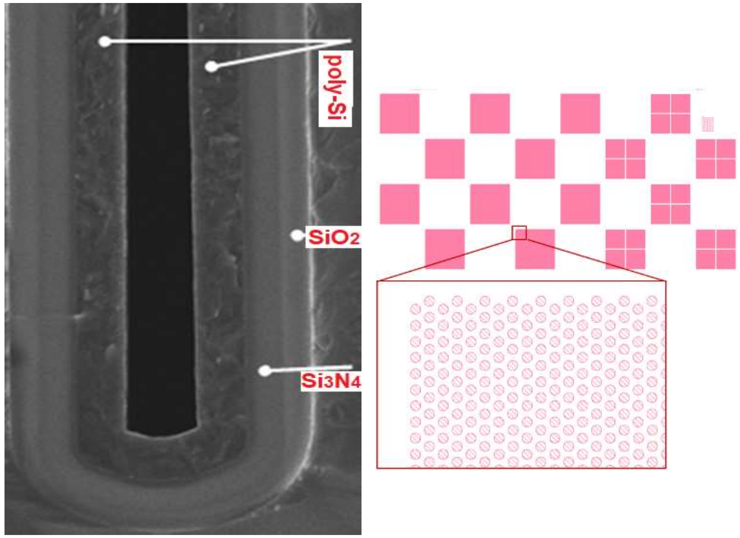
Direct bonded copper to reduce on-resistance

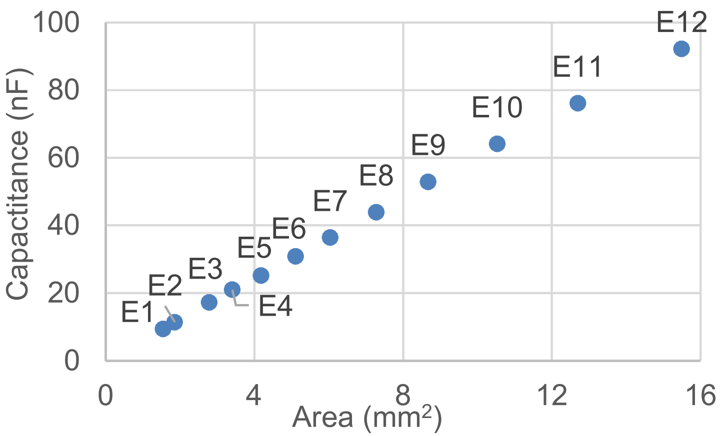
Design and Measurement of Integrated Converters for Belt-driven Starter-generator in 48 V Micro/mild Hybrid Vehicles, IEEE Trans. Ind. App. 2017

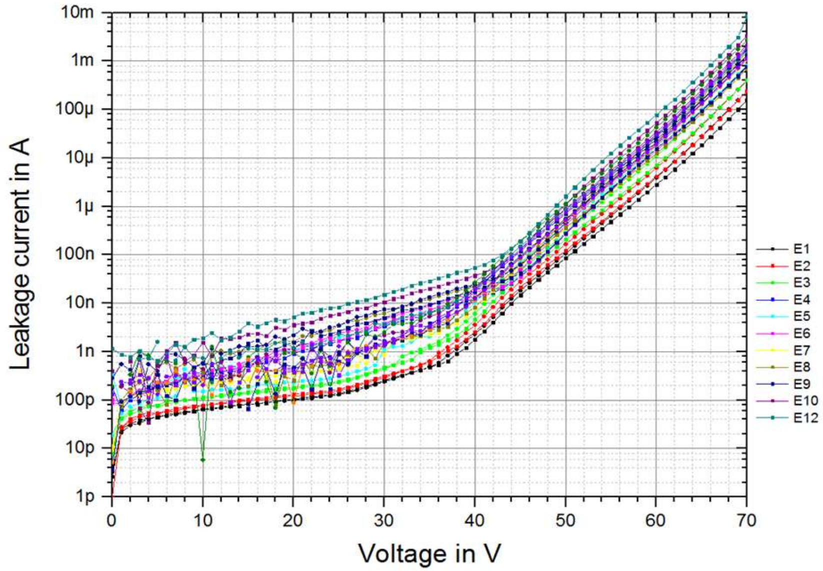
# Integrated silicon-TSV HV capacitors

Fraunhofer IISB



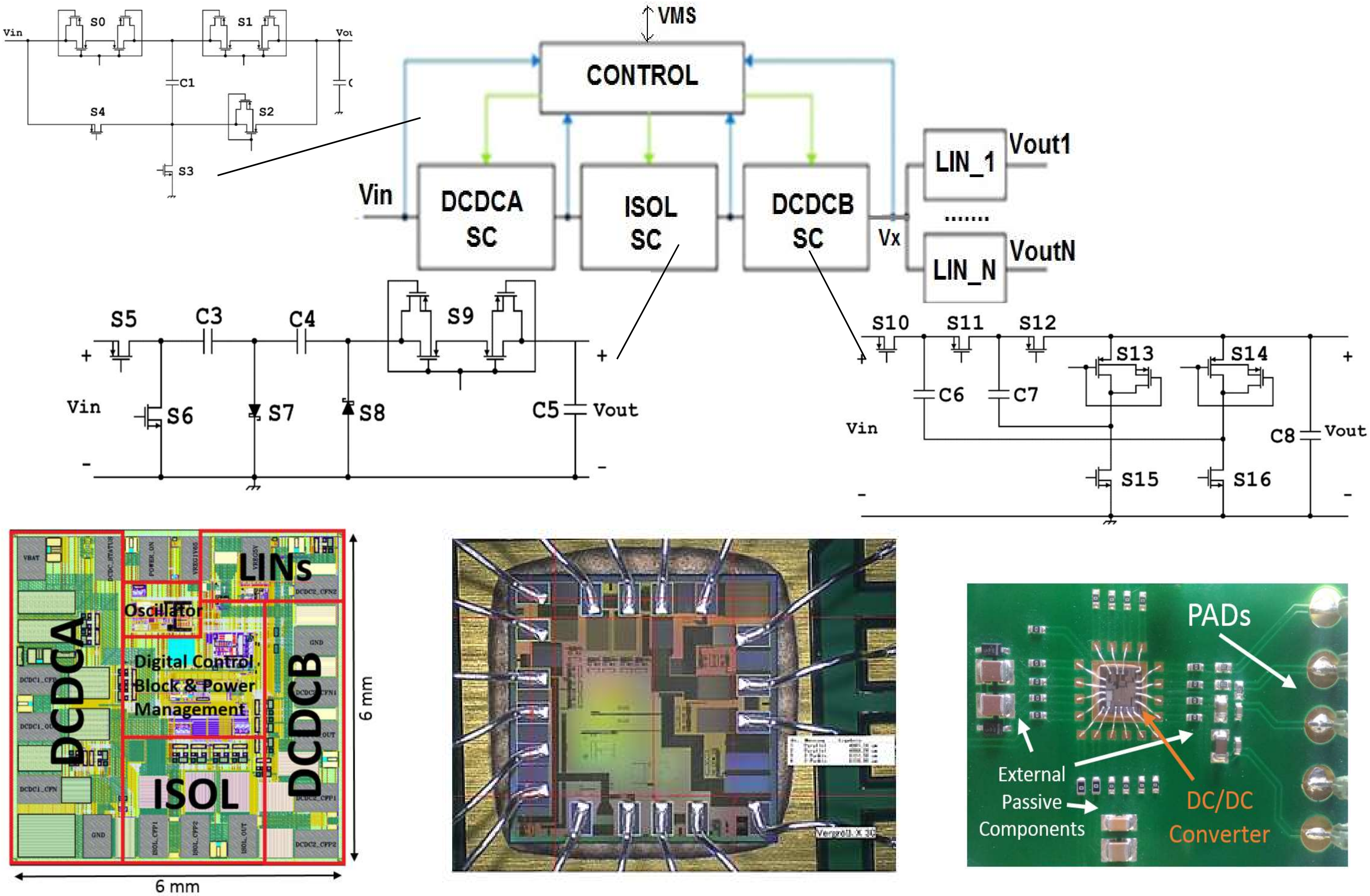




## Integrated MOS-compliant power capacitors up to 70 V

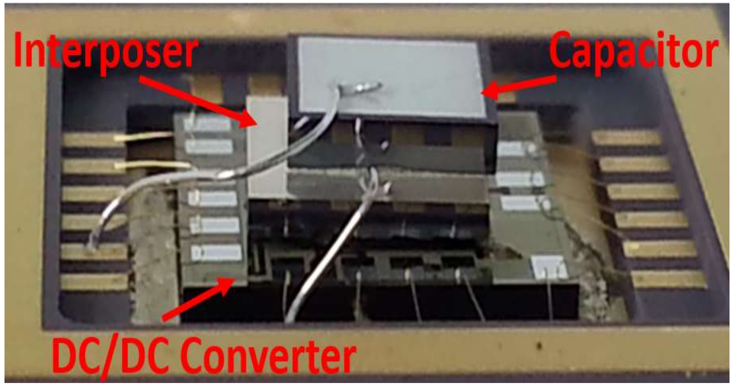
Integrated passive devices and switching circuit design for a 3D DC/Dc converter up to 60 V, Journal of Circuits, Systems and Computers, 2020

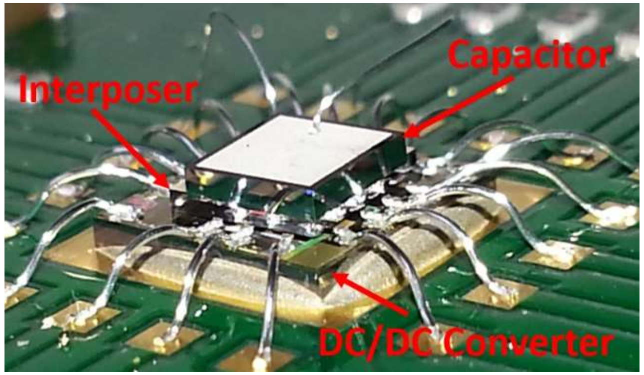
# 48 V Switched-Cap (SC) architecture




IC Design and Measurement of an Inductorless 48 V DC/DC Converter in Low-Cost CMOS Technology Facing Harsh Environments, IEEE TCAS1, 2018

# with capacitors stacked on top

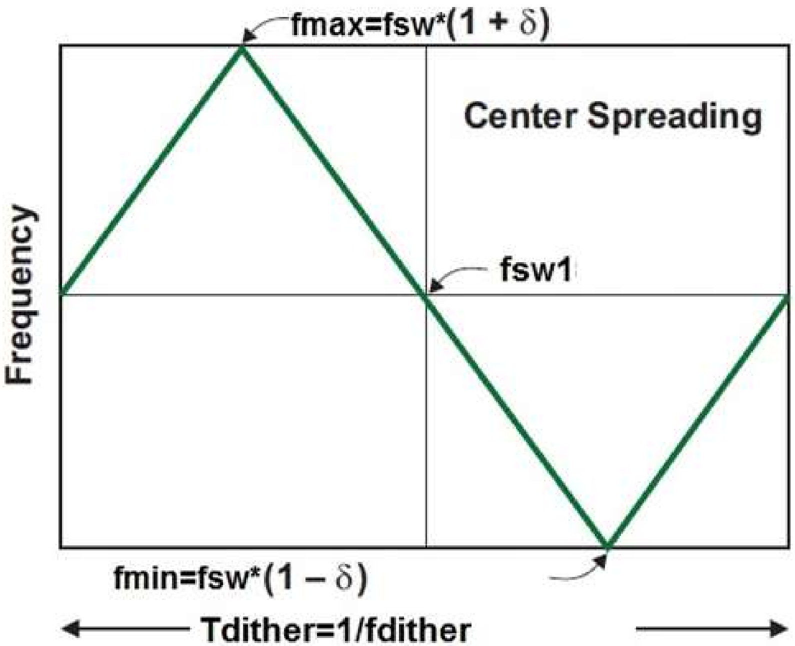


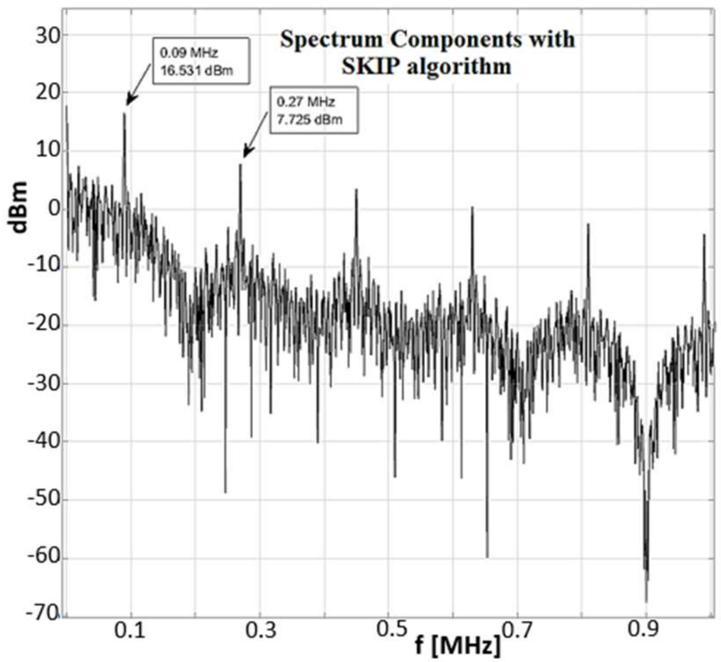




**Similar performance of 3D vs. 2D but much lower area**

6 dB reduction of the EM Interference power emission thanks to SKIP-mode

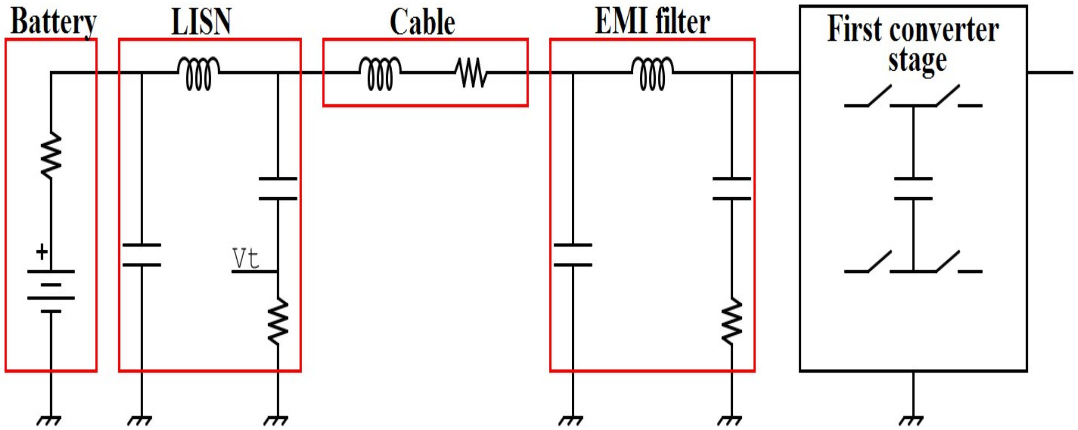
*Extra spectral attenuation with fsw spreading (dB)=10*log[($f_{SW}$*δ)/($f_{DITHER}$/n)]*

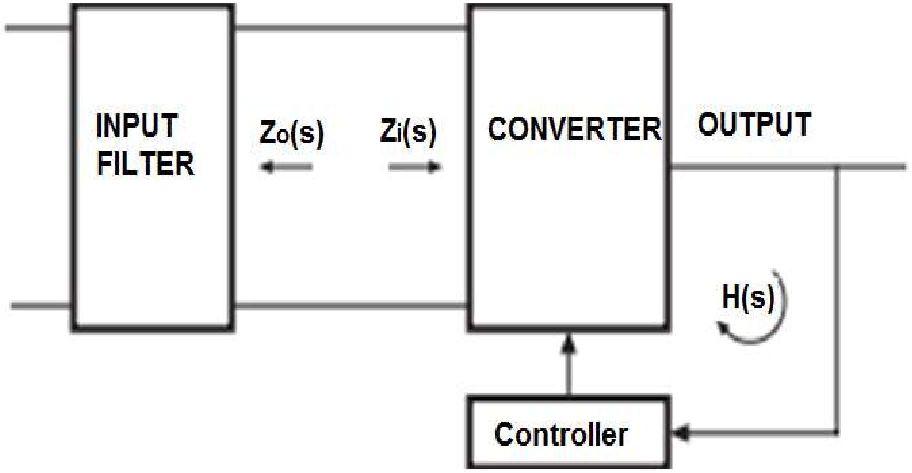


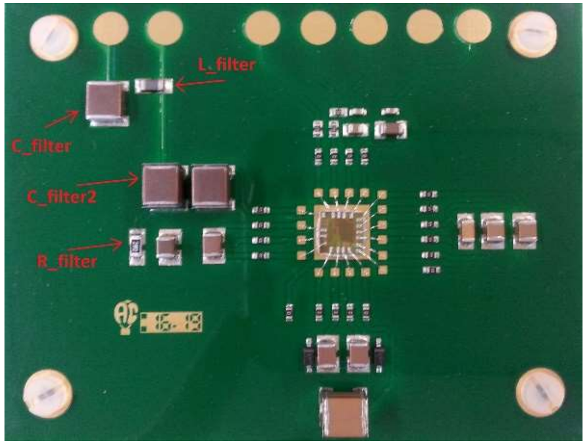

Design and Experimental Measurement of EMI Reduction Techniques for Integrated Switching DC/DC Converters, IEEE Can. Journal of Elec. and Com. Eng 2017

# Anti-EMI filter




The design of anti-EMI filter aware of input converter impedance reduces x 3 the size of the filter components and avoids instability

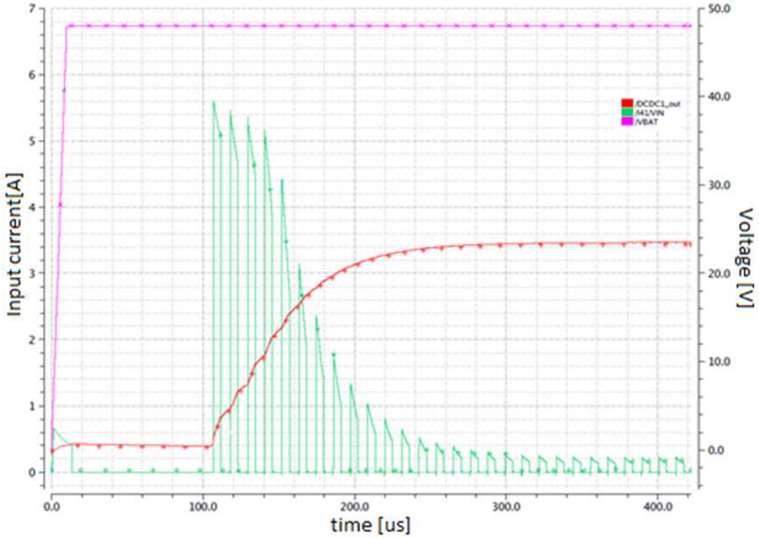


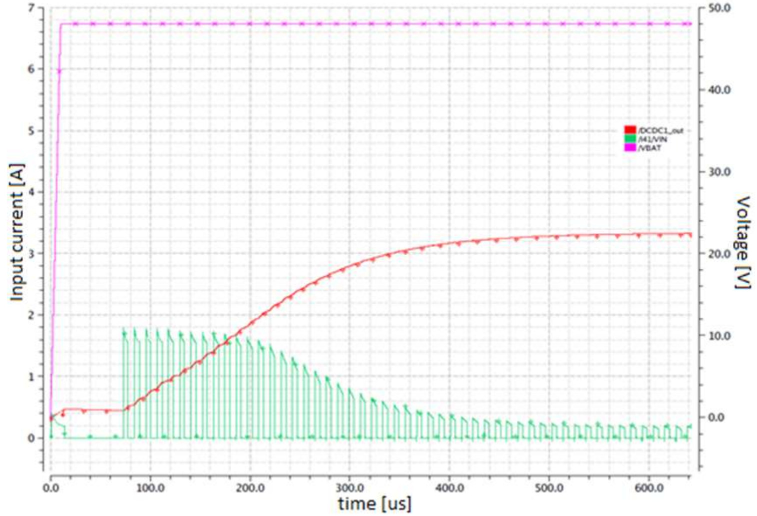

| | Set-up | | EMI measurement results | |
|---|---|---|---|---|
| | $V_{battery,}$[V] | $I_{load}$, [mA] | Freq.peak., [kHz] | Amplitude, [dBV] |
| This work | 8 | 0-300 | 180 | -84, -74.8, -65.4 |
| | 12 | 0-300 | 180 | -87.2, -77.4, -69.8 |
| | 24 | 0-300 | 180 | -77.8, -77.2, -75.4 |
| | 48 | 0-300 | 160 | -74.4, -76.4, -71.4 |
| | 60 | 0-300 | 100 | -71.4, -63, -57.8 |
| [TI] | 30 | 1600 | 10 | -47.5 |

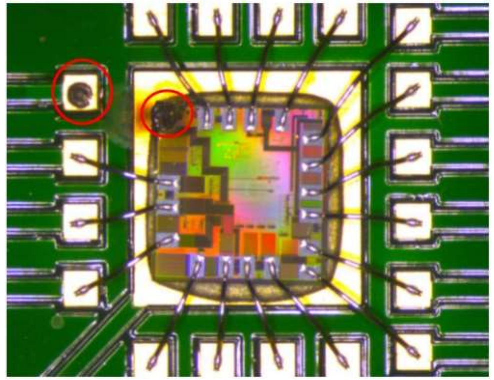
# Soft-start

Input current without/with soft-start modality (current peaks reduced by 3 times).

HV-MOS multiple parallel devices, activated according to a proper sequence



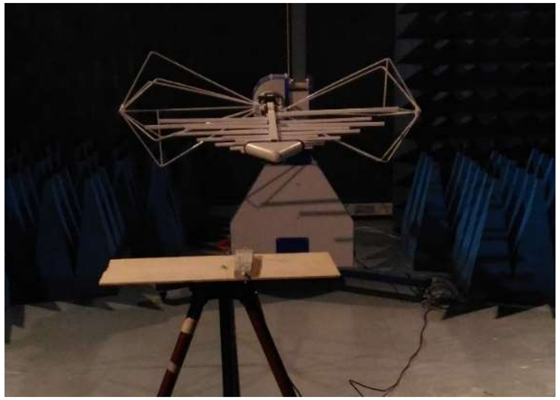



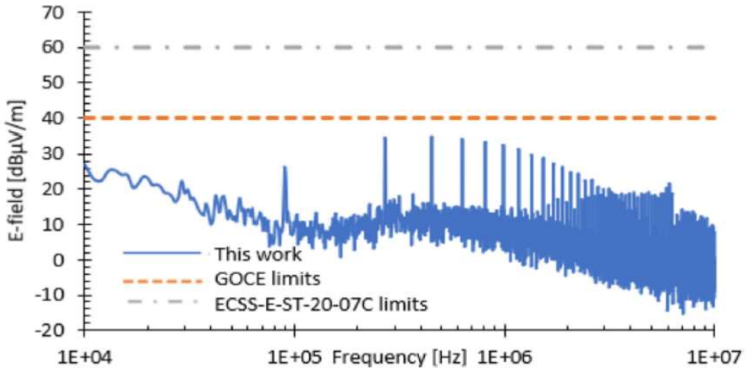



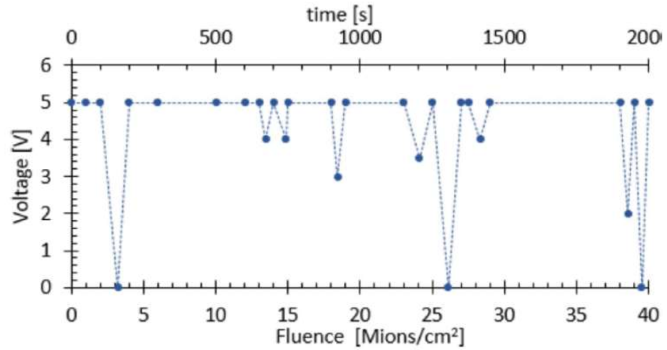
Without soft-start chip damaged by high current peaks at device start

| | Conducted EMI reduction | Radiated EMI reduction | Could be integrated | Low design effort | Low cost |
|---|---|---|---|---|---|
| EMI filter | + + + | - | - - | - - | - - |
| SKIP control | + + | + + | + + + | + | + + |
| Soft-Start technique | + | + | + + + | - | + |

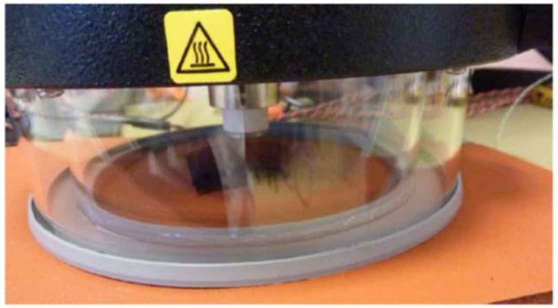
# EMI, temperature and rad tests

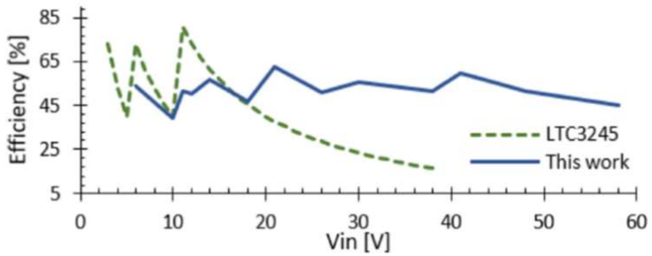


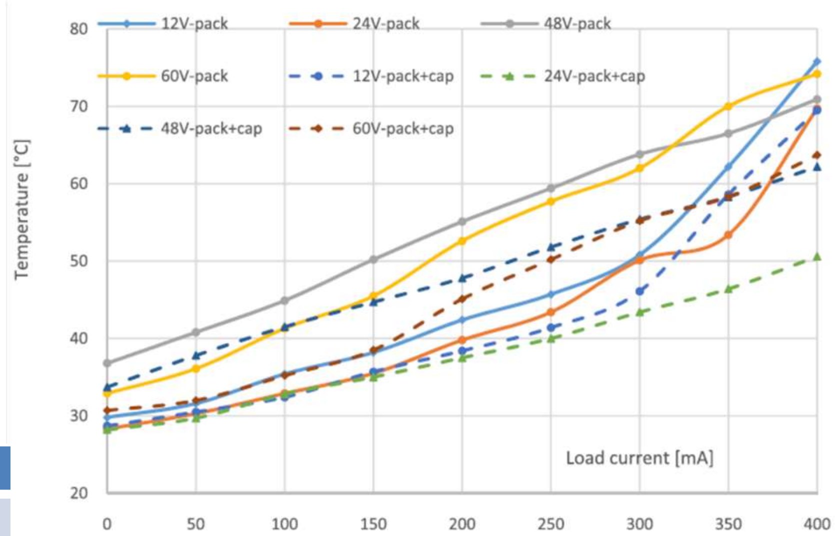



Failure test of the INSUL stage using Si28 with LET = 8.8 Mev·cm$^2$/mg and flux = 20 kions/s.






| | This Work | PT4660 | LT3245 | LM5170 |
|---|---|---|---|---|
| Type | SC+linear | Inductive | SC | Inductive |
| In-Out insulation | Yes | Yes | No | No |
| Input range [V] | 57* | 39 | 35 | 79 |
| PSRR [dB] | -60 | Off-chip LDO needed | | |
| Output voltage [V] | 1.65 / 5 | 3.3 / 5 | 5 | 12 / 48 |
| Max load current [A] | 0.4 | 30 | 0.25 | 5 |
| Rad-hard TID | 43 krad | N/A | N/A | N/A |
| Stand-by current [µA] | 5 | 5000 | 4 | 10 |

Inductorless DC/DC Converter for Aerospace Applications With Insulation Features, IEEE TCAS2, 2020

Electrical, Electromagnetic, and Thermal Measurements of 2-D and 3-D Integrated DC/DC Converters", IEEE Tra. IM 2018

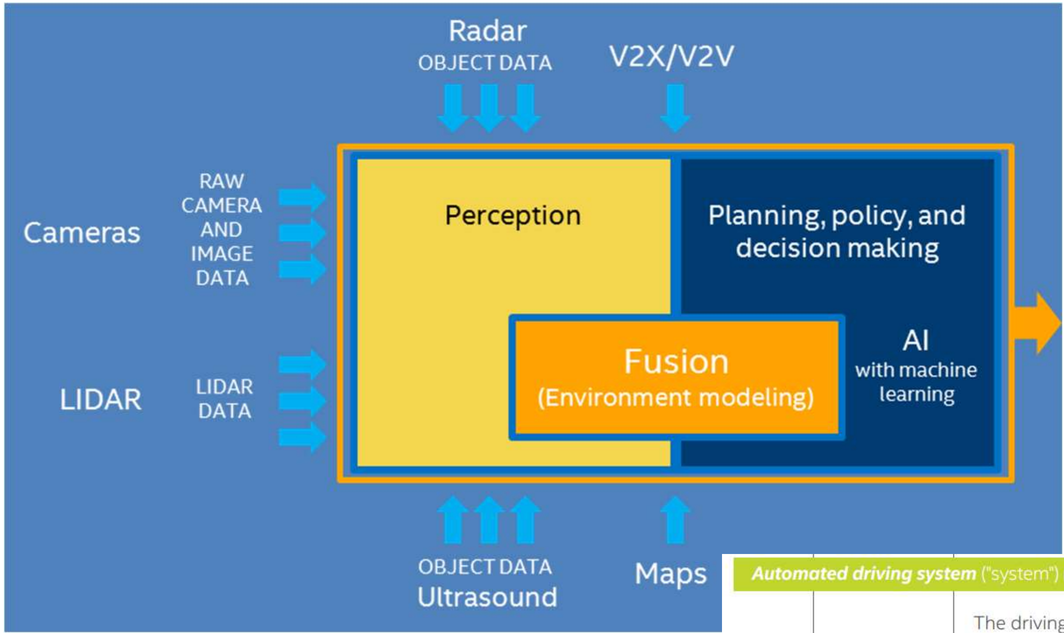
# Outline

- Trends in smart vehicles & intelligent transport systems (ITS) and impact for society/economy
- University pillars: opportunities for continuous education, R&D, and technology transfer in Electronics
- Example R&D case studies:
  - Integrated Power Converters for 48 V micro/mild-hybrid vehicles
  - ITS surveillance X-band Radar
  - Cybersecurity acceleration

# Context-awareness vehicle perception

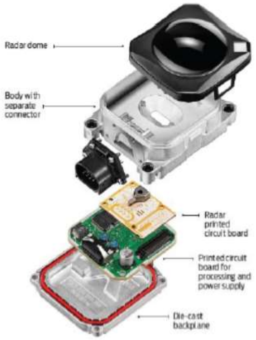
**Autonomous vehicle perception based on multi-sensor fusion**

(VideoCameras, Lidar, Radar, Ultrasounds) + **fusion with V2X data**




| ***Automated driving system*** ("system") monitors the driving environment | | | | | | |
|---|---|---|---|---|---|---|
| 3 | **Conditional Automation** | The driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene | System | **System** | Human Driver | Some Driving Modes |
| 4 | **High Automation** | The driving mode-specific performance by an automated driving system of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene | System | System | **System** | Some Driving Modes |
| 5 | **Full Automation** | The full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver | System | System | System | **All Driving Modes** |

# Context-awareness vehicle perception



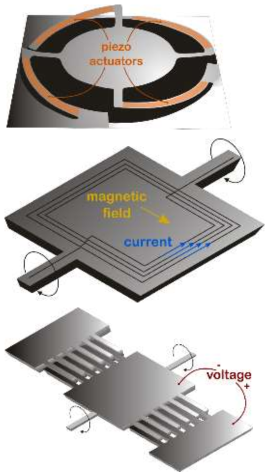
## Radar (Master of Motion Measures)

Active EM sensor (e.g. 24&77 GHz, 10 dBm). Robust in harsh conditions.

250 m range, 0.1m limited accuracy. *Real-time DSP on FPGA for Radar imaging*

*Highly Integrated Low-Power Radars, Artech Book, 2014*

*Radar-on-Chip/in-Package in Autonomous Driving Vehicles and Intelligent Transport Systems: Opportunities and Challenges. IEEE Sign Pr. Mag 2019*




## Lidar (Master of 3D mapping), use still limited by cost

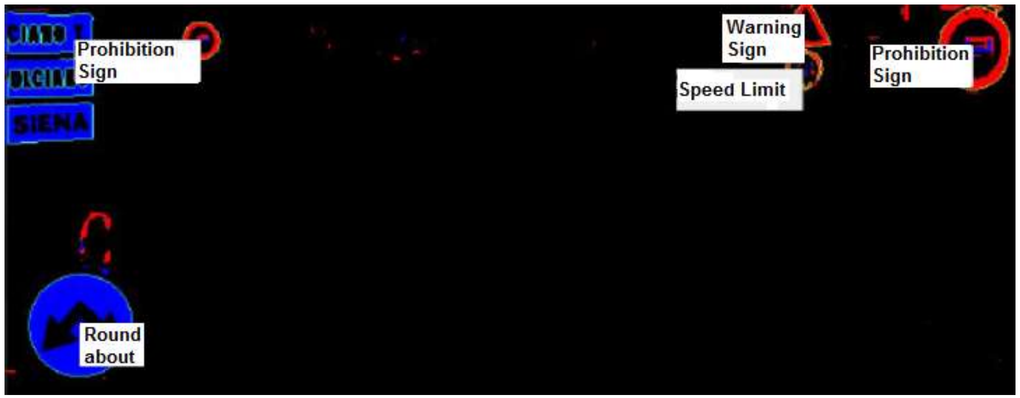
Active Light sensor. Mid Range up to 100 m, good accuracy (0.02 m and $0.1^0$ accuracy). *Micromirror scanning proposal for low-cost & wide FOV*

*Is Consumer Electronics Redesigning Our Cars?: Challenges of Integrated Technologies for Sensing, Computing, and Storage, IEEE Cons. Eletcr. Mag 2018*

## Camera (Master of Classification)

Passive. See colors & textures. Cheap. IR sensors needed for night vision

JRTIP2016 640x480 automotive camera & FPGA, recognition at 15 m, <100 ms

# Real-time transport-surveillance Radar

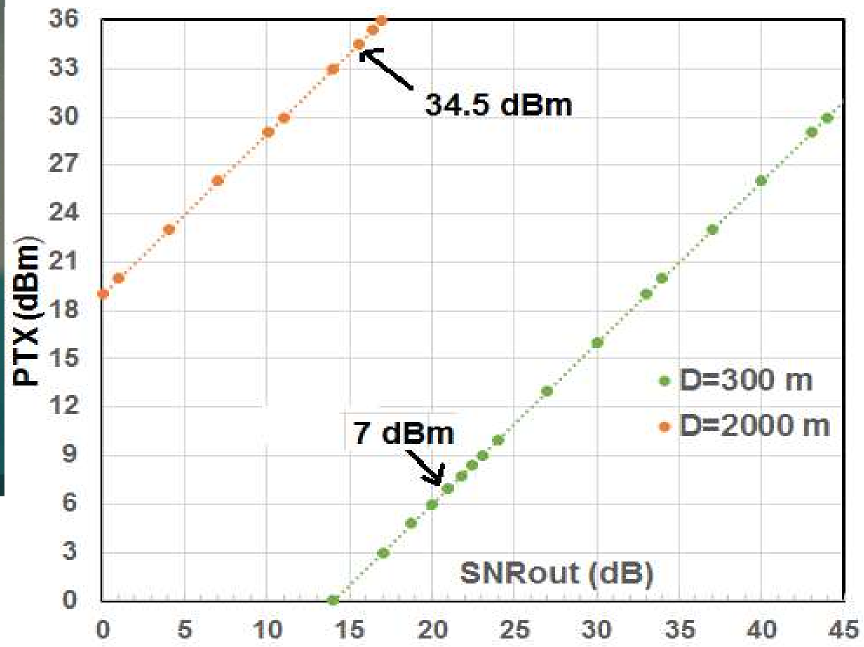
**X-band Radars for harbor surveillance information system & for railway-crossing and parking or road crossing safety**

- Detection & tracking of ships/yachts ingress/egress up to 1.5 km
- Obstacle detection on a railroad or urban road crossing up to 200 m
- Network of Radars for large port areas (increase the covered area)
- Up to 4 Radar nodes for high SIL (Safety Integrity Level) in automated railroad crossing
- 1 Tx + 3 Rx for speed, distance, angle estimation
- Custom microwave board for imaging sensor front-end in X-band
- Real-time DSP on FPGA for power efficiency/compact size

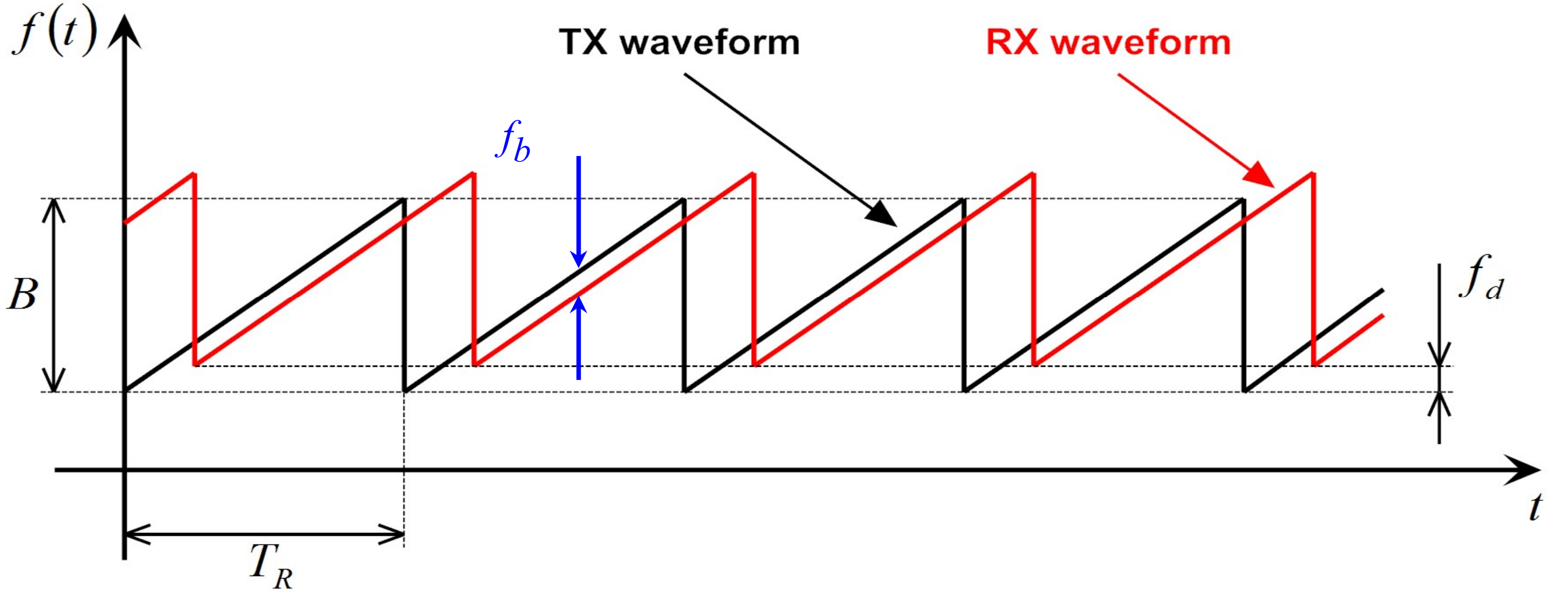
Collaboration with CNIT/RASS (Berizzi, Martorella, Lischi, Massini) & IDS

# Specification for a transport-surveillance Radar


| | |
|---|---|
| Max. distance coverage | *300 m, 2000 m* |
| Range resolution | *40 cm* |
| Max speed | *40 m/s* |
| Target RCS | *≈ $1 \div 10^4$ $m^2$* |
| SNR after DSP | *> 15 dB* |



# FMCW waveform: moving target




For a moving target:

$$R(t) \cong R_0 + v_r t$$

Doppler frequency: $$f_d = -\frac{2v_r}{\lambda_0}$$

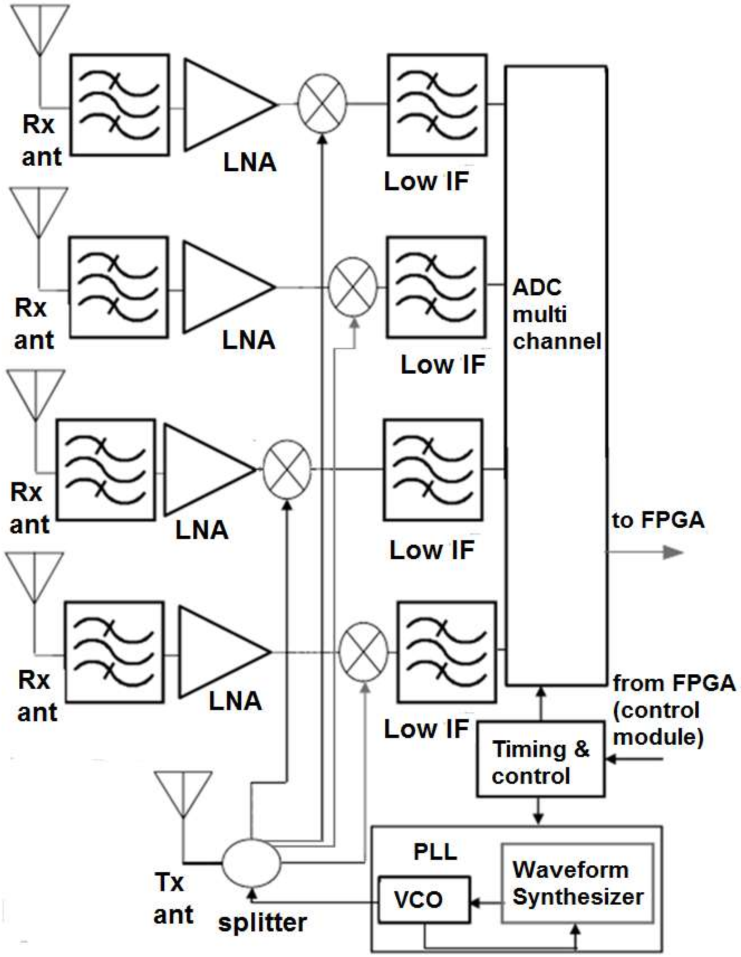
Range frequency: $$f_r = \alpha\tau = \frac{B}{T_R}\frac{2R_0}{c}$$

Beat frequency: $$f_b = f_r + f_d$$

Range-Doppler coupling effect

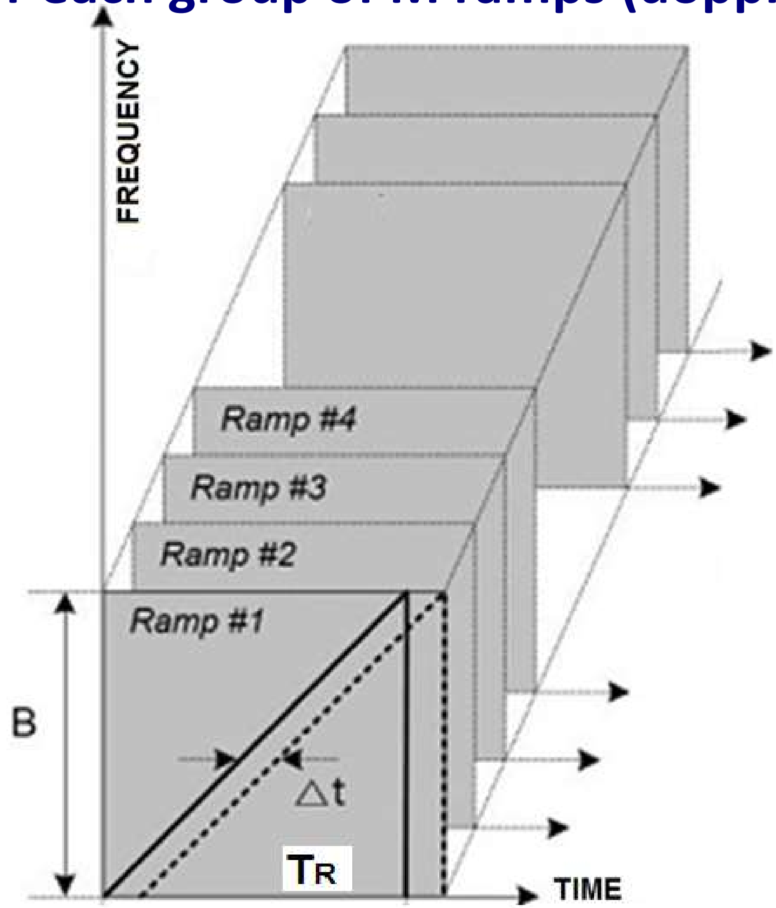
# X-band Radar transceiver architecture

**Scalable number of RX channels**




**2D FFT frequency analysis**

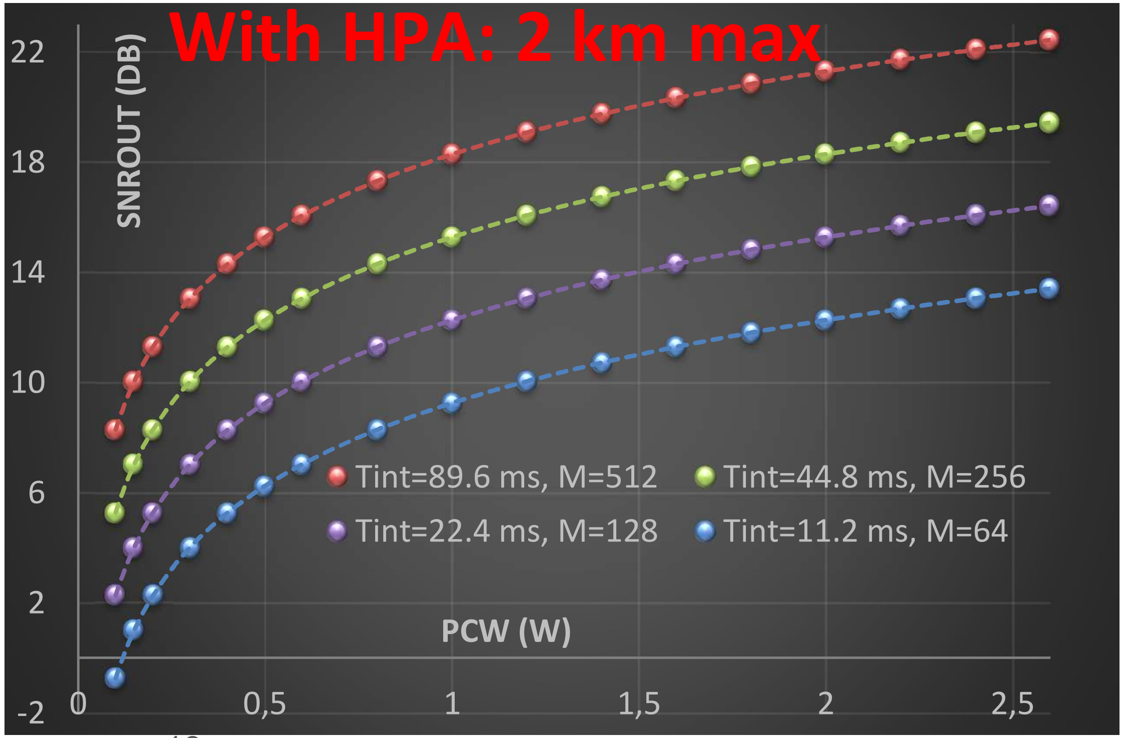
- for each sweep (range)
- for each group of M ramps (doppler)

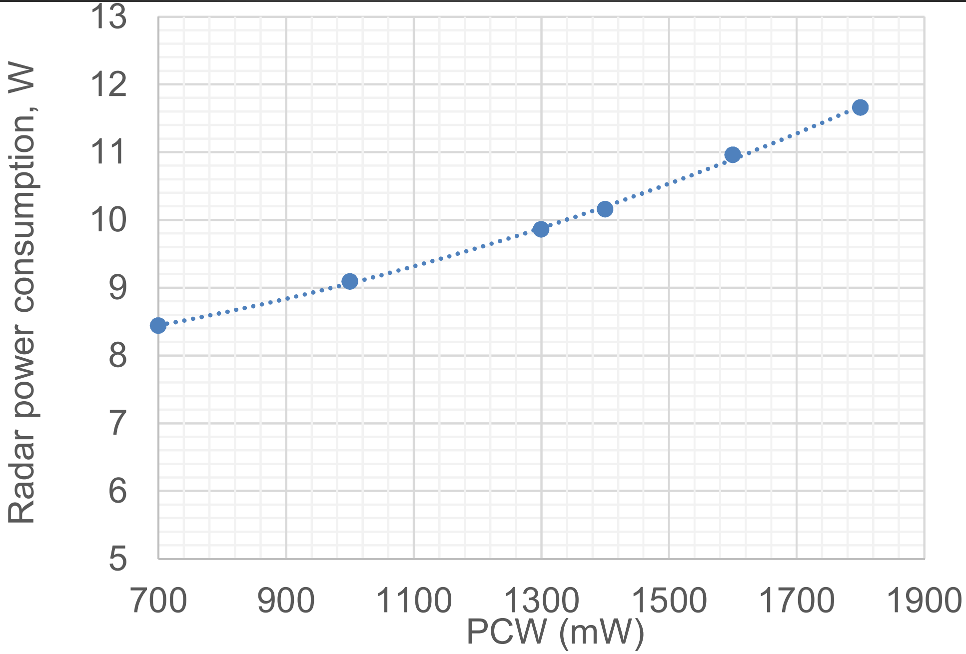


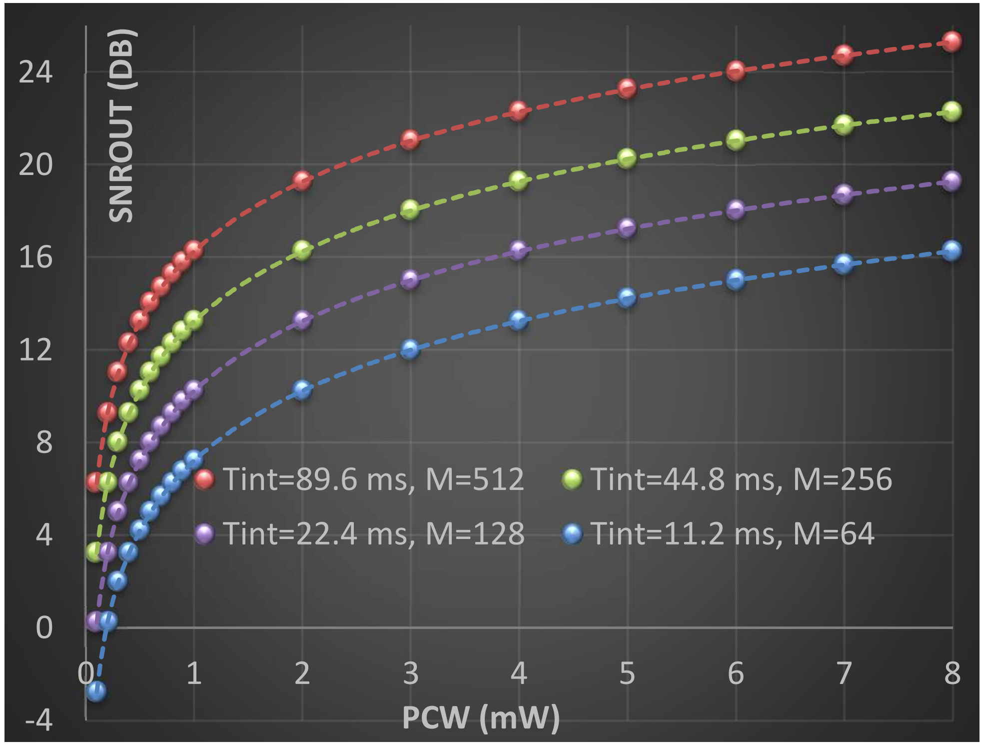

**High-power stage HPA (34.5 dBm Pcw) to reach 2 Km**

**HPA by-passed (7 dBm Pcw) for low-power applications with 300 m target**

# Received SNR vs. Pcw

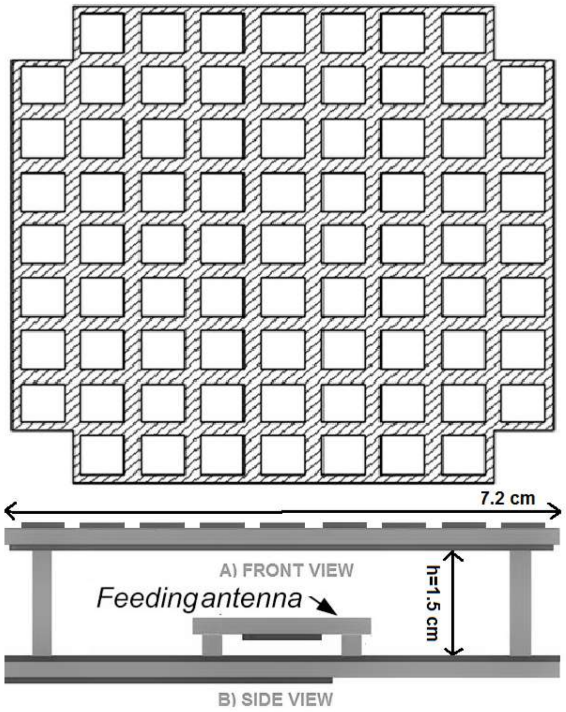


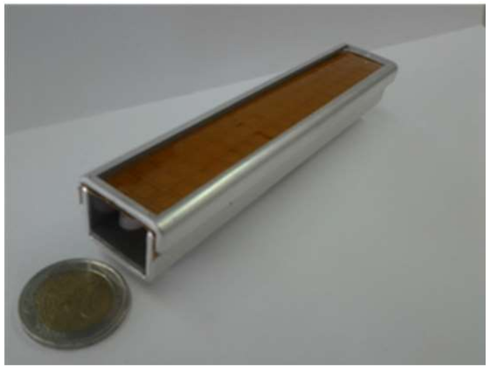




Without HPA: 300 m max

# Fabry-Perot resonating antenna

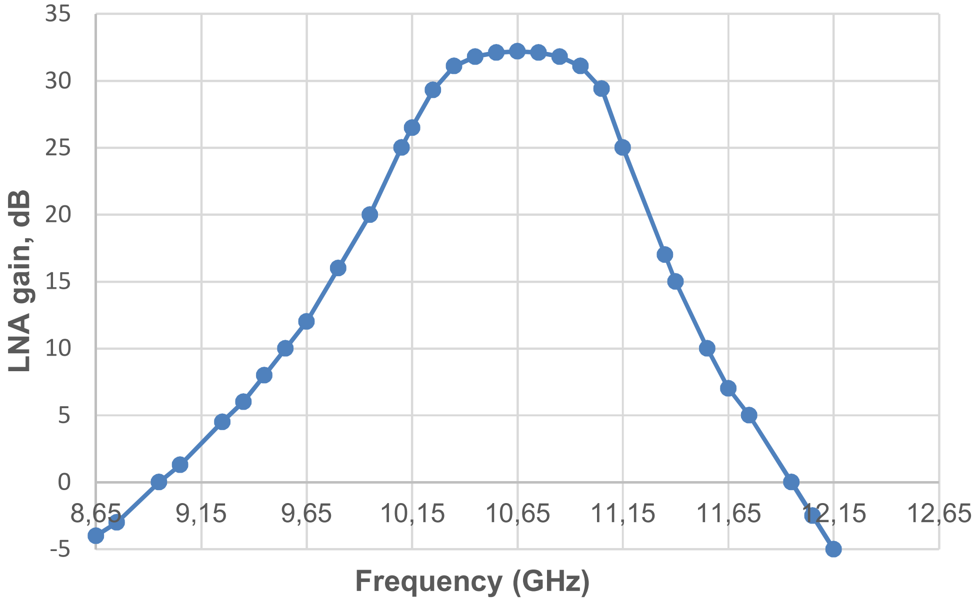



Prototype developed by the Electromagnetic fields and microwaves Lab. of the Department of Information Engineering of the University of Pisa.

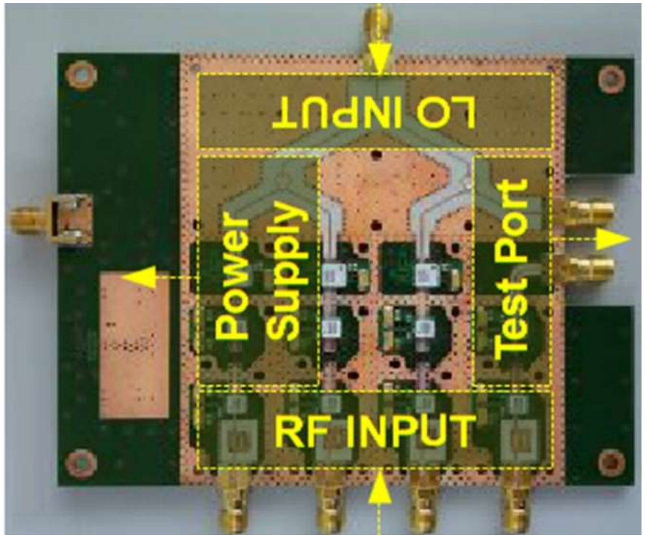


| | |
|---|---|
| Central frequency | 10.65 GHz |
| Bandwidth | 300 MHz-500 MHz |
| Transmitted power | up to 33 dBm |
| System losses | 8 dB |
| Noise figure | 4.2 dB |
| SFDR | 65 dBc |
| Sampling frequency | Up to 46 MS/s |
| ADC resolution | 12 bit/14 bit |
| Antenna technology | Fabry-Perot resonator |
| Antenna polarization | H-linear |
| Antenna azimuth HPBW | 60° |
| Antenna elevation HPBW | 20° |
| Antenna gain | 13 dBi |
| Receiving channels | 1 to 4 |

# Receiver with COTS LNA (from Hittite, now Analog Devices) & Microwave Board




Gain (S21) of the LNA and input filter

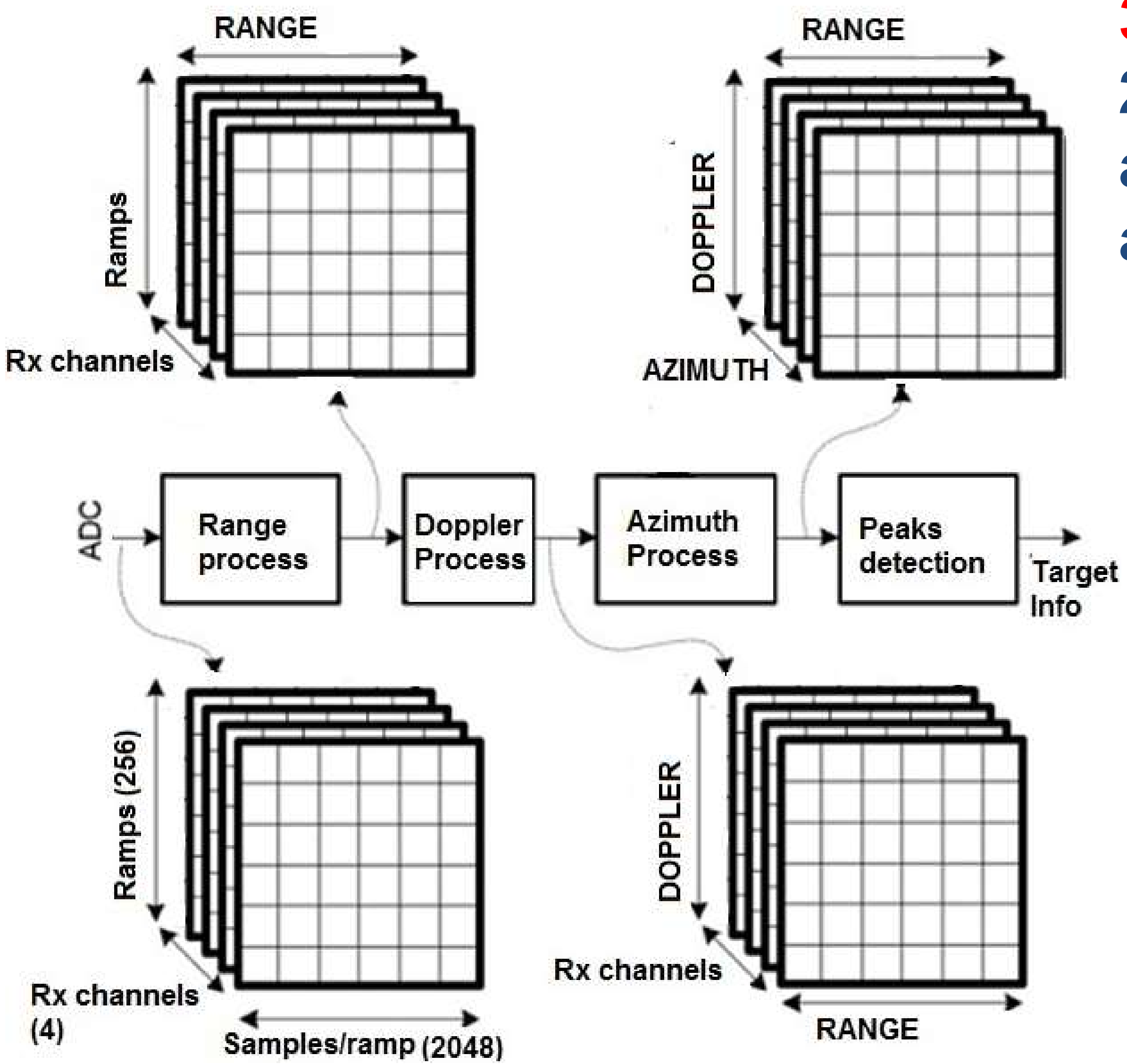



Measurement range R affected by channel impairments, HW performance, target cross-section; resolution $d_R$ depends on sweep band B (4 cm for 77-81 GHz LRR)

$$R=\sqrt[4]{\frac{P_{CW}\lambda^2 G_{ant}^{\;2}}{(4\pi)^3}\frac{1}{L}\frac{\sigma}{SNR_{dig}}\frac{1}{k_B T N_F \Delta f}}$$

$$d_R = {}^{c}\!/_{2B}$$

# FPGA-based signal processing

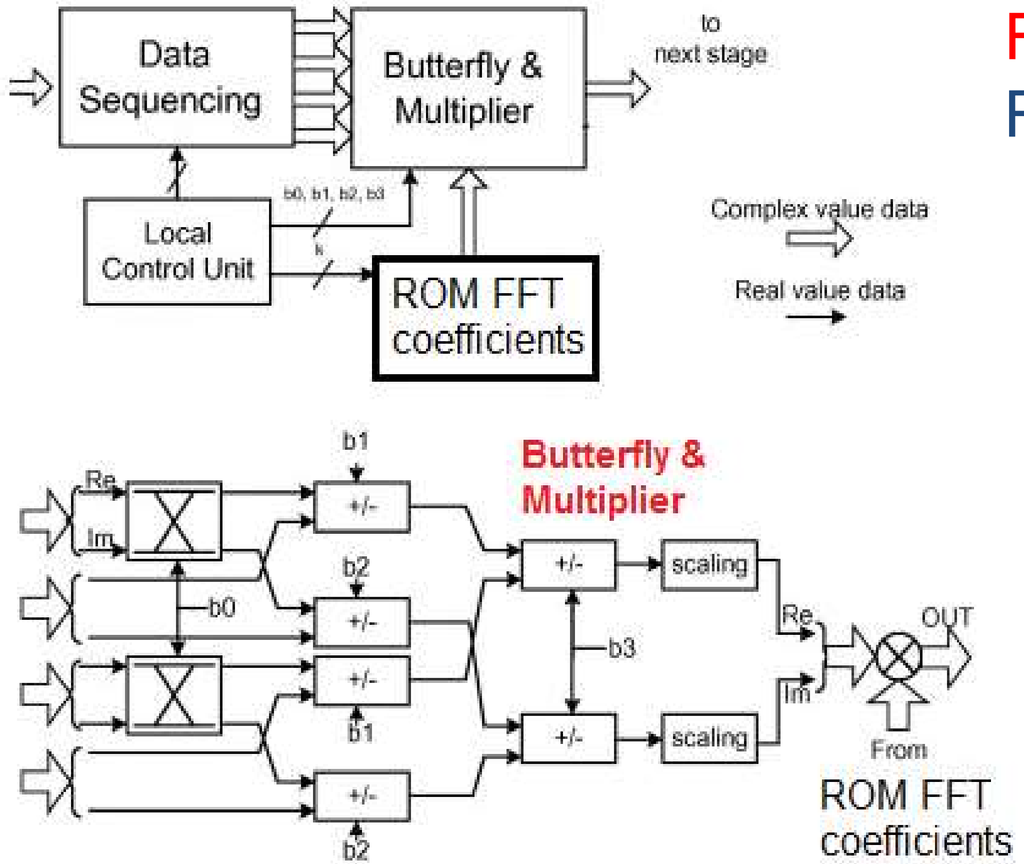



**3D FFT range-Doppler:** 2D FFT processing + 3rd FFT along the 4 RX channels for azimuth and peak estimation

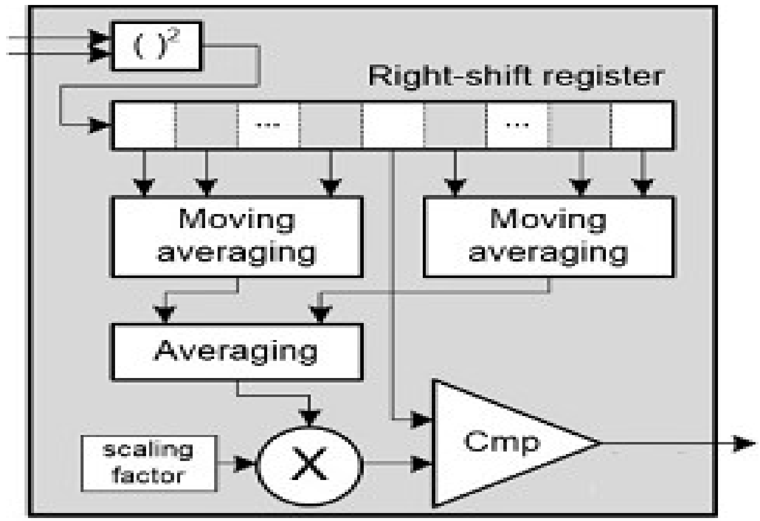
**Memory storage:** 2M words of 24 bits (12 bits Re & Im data)

**Memory buffering** since data transfer & storage may become the bottleneck

# HDL blocks for FPGA-based signal processing




FFT core based on a multi Radix-4 stages

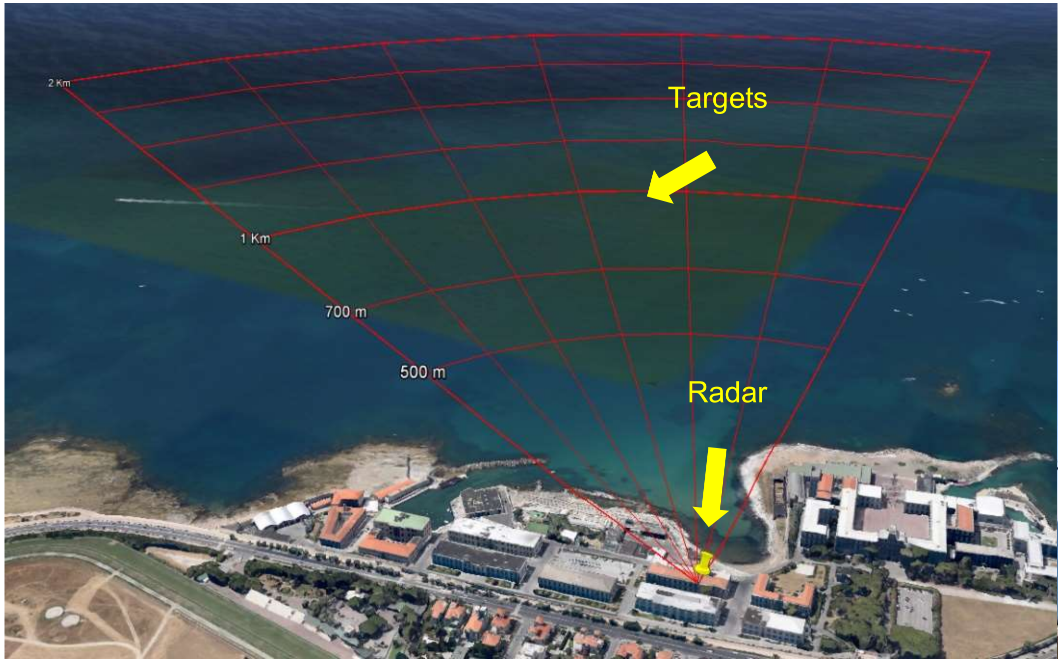



CA-CFAR HDL circuit

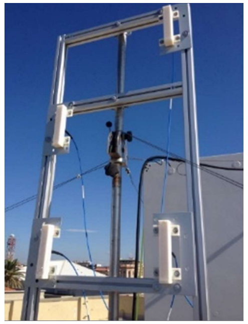
| Device | FF | DSPslice | LUTs | Mem block | RX Channels |
|---|---|---|---|---|---|
| XA7A100T | 32.4% | 88.3% | 35.6% | 96% | 4 |
| Zynq-XA7Z020 | 40.9% | 93.7% | 45.7% | 93% | 4 |

# Artix-7 FPGA and Zynq FPSoC

# Experimental setup and Measurements



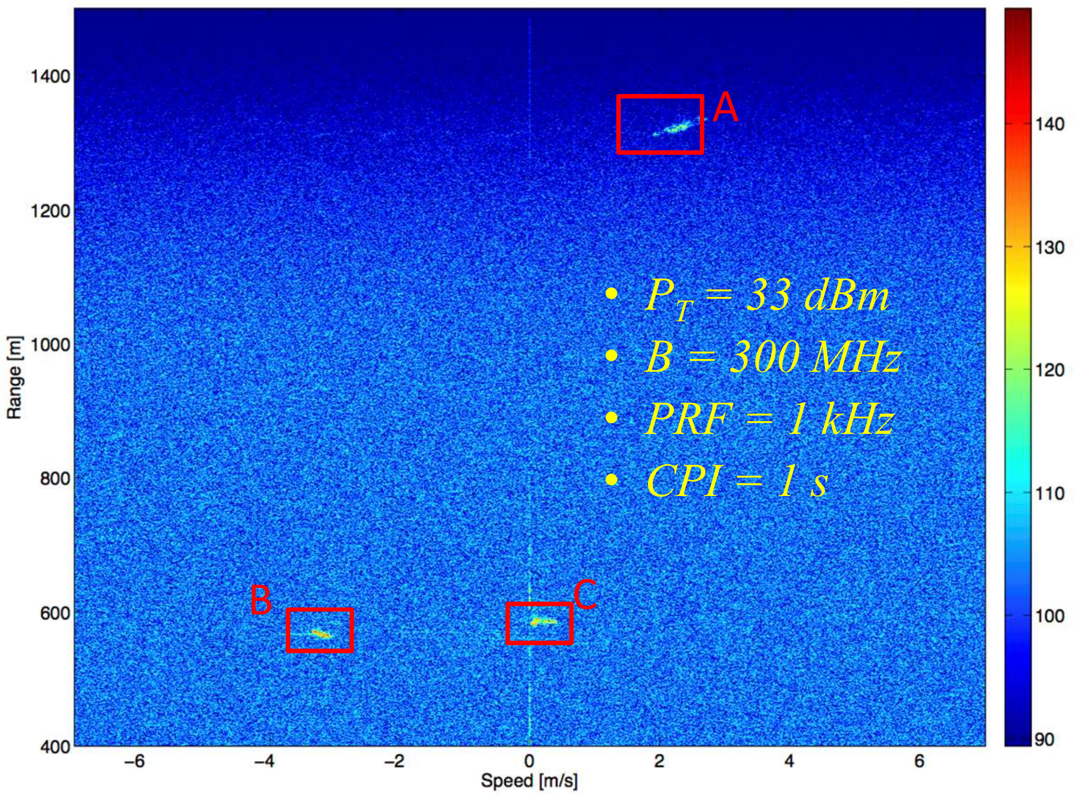

Experimental setup for the NATO-SET196 trials, Istituto Vallauri, Livorno, Italy.



| | | |
|---|---|---|
|  |  |  |
| A. Length: 32.5m, Width: 6.47m<br>• Material: wood and iron | B. Length: 8.5m, Width: 2.3m<br>• Material: fiberglass and iron | C. Length: 13.20m, Height: 13m<br>• Material: wood |

# Targets & Range-Doppler map

| | Freq, GHz | Type | Power cost | Range, Output power | Channels |
|---|---|---|---|---|---|
| **This work** | 10.3-10.8 | FMCW | < 8 W | 300 m@5 mW, 1.5 km@2W | 5 |
| **IEEE TBSC** | 3.1-10.6 | Pulsed UWB | 73 mW | <1 m, 7 pJ/pulse | 2 |
| **MOTL 2013** | 22-26 | Pulsed UWB | N/A | N/A, 2 mW | 2 |
| **TERMA2015** | 9.375 | Pulsed | N/A | 45 km @ 32 kW | N/A |
| **EURAD2014** | 10.5-10.8 | FMCW | >100 W | 1.2 km@2 W | 3 |
| **IEEETIM 2014** | 2.48 - 2.56 | FMCW | N/A | 20-100m @ 100 mW | N/A |
| **AMS2013** | 9.4 | FMCW | 650 W | 50 km@100W | 1 |




Radar sensor signal acquisition and multi-dimensional FFT processing for surveillance applications in transport systems, IEEE Trans IM 2017

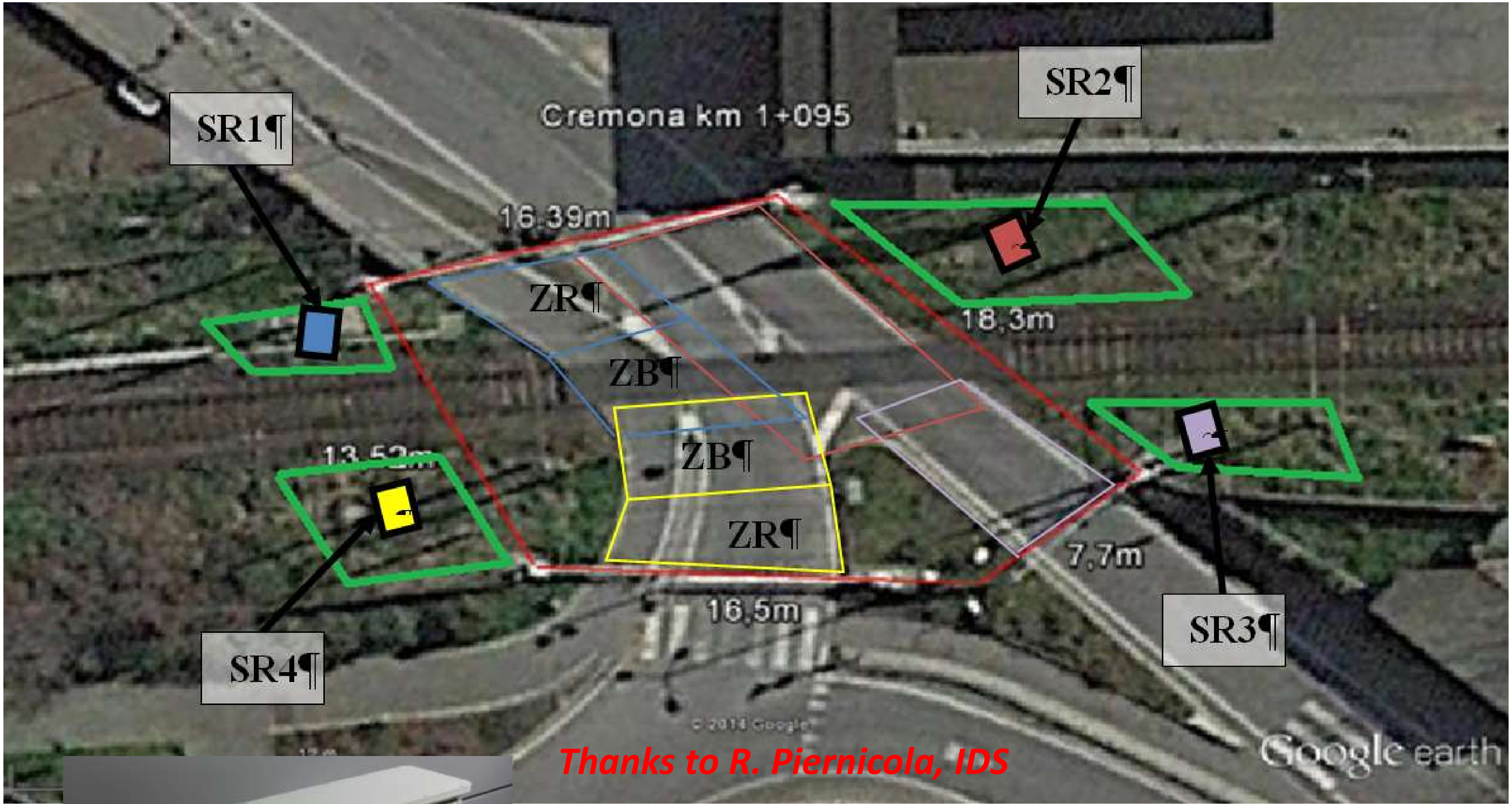
Design of compact and low-power X-band Radar for mobility surveillance applications, Computer and Electr,. Engineering, 2016

Hardware accelerator IP cores for real-time Radar and camera-based ADAS", Journal RT Image Proc. 2020

Detected targets appear like an oval due to the target physical size and to Radar resolution limits in distance and speed

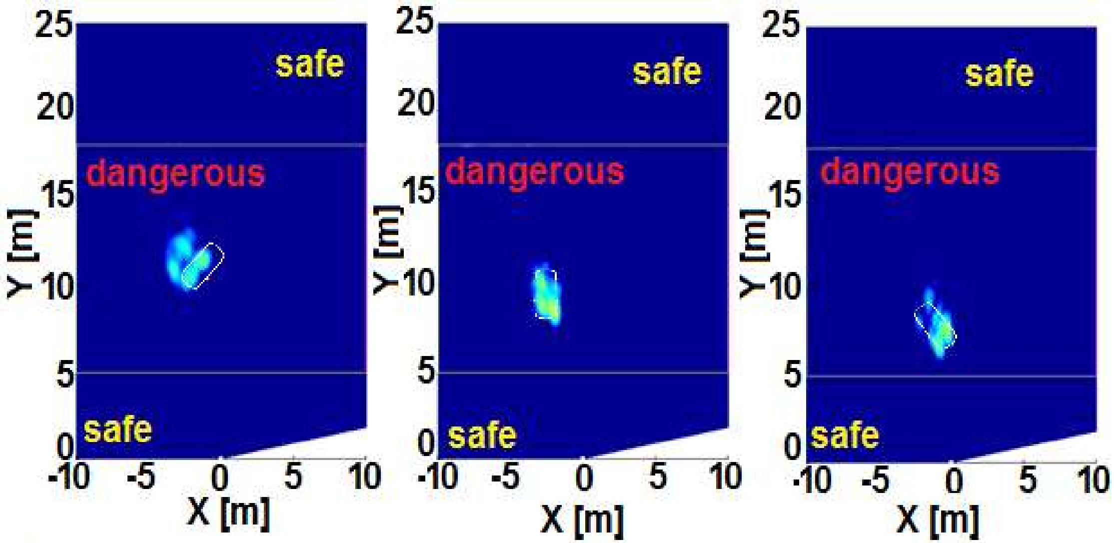
A post-processing step on the range-doppler image allows extracting size along radial axis and speed

# Example of installation on a roadcrossing

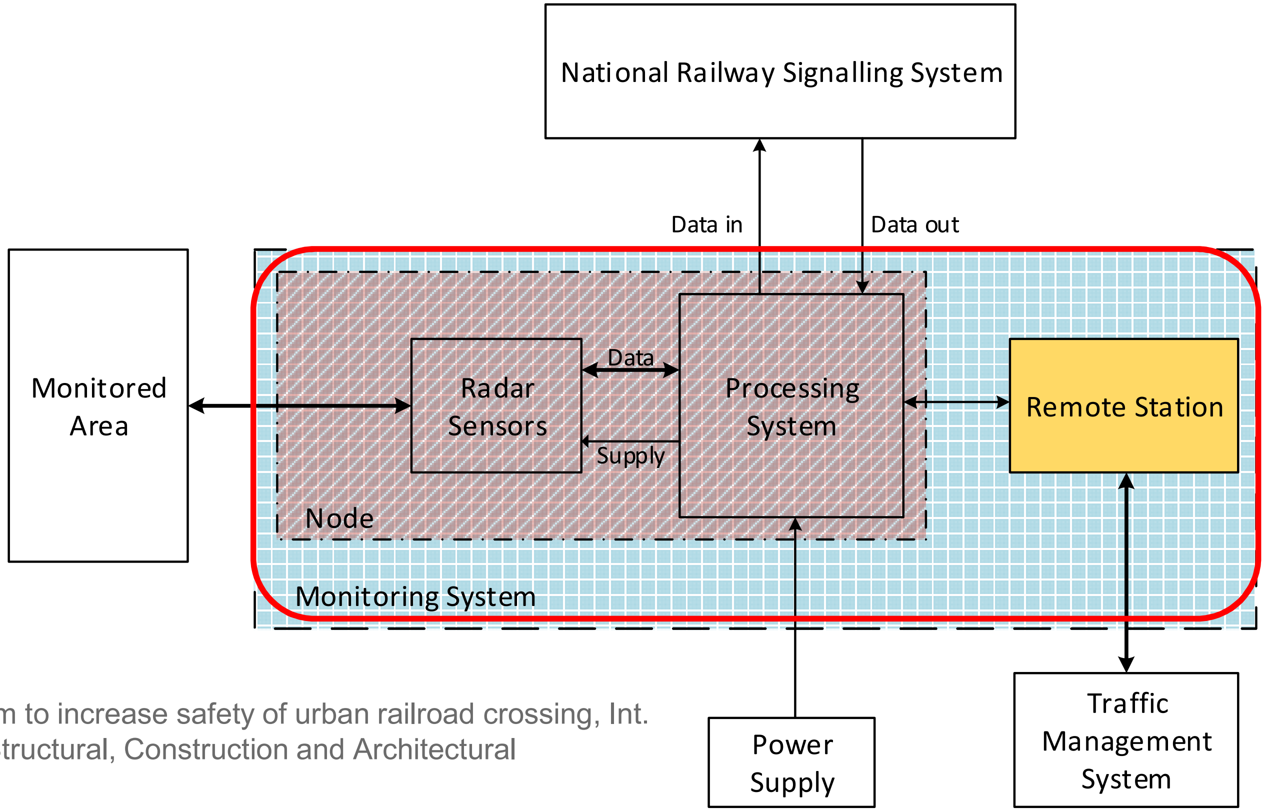



**Safety Integrity Level SIL4**

# Railway surveillance-radar configuration




*Thanks to*
*R. Piernicola, IDS*



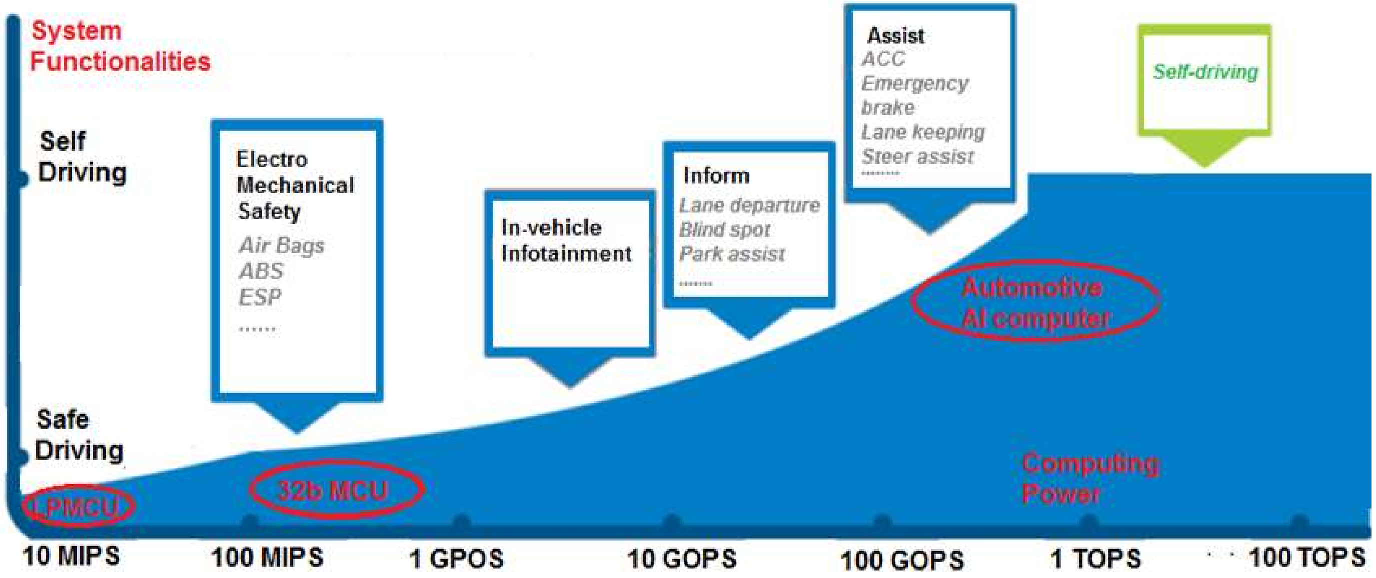

Networked radar system to increase safety of urban railroad crossing, Int. Journal of Civil, Env., Structural, Construction and Architectural Engineering, 2015

# Outline

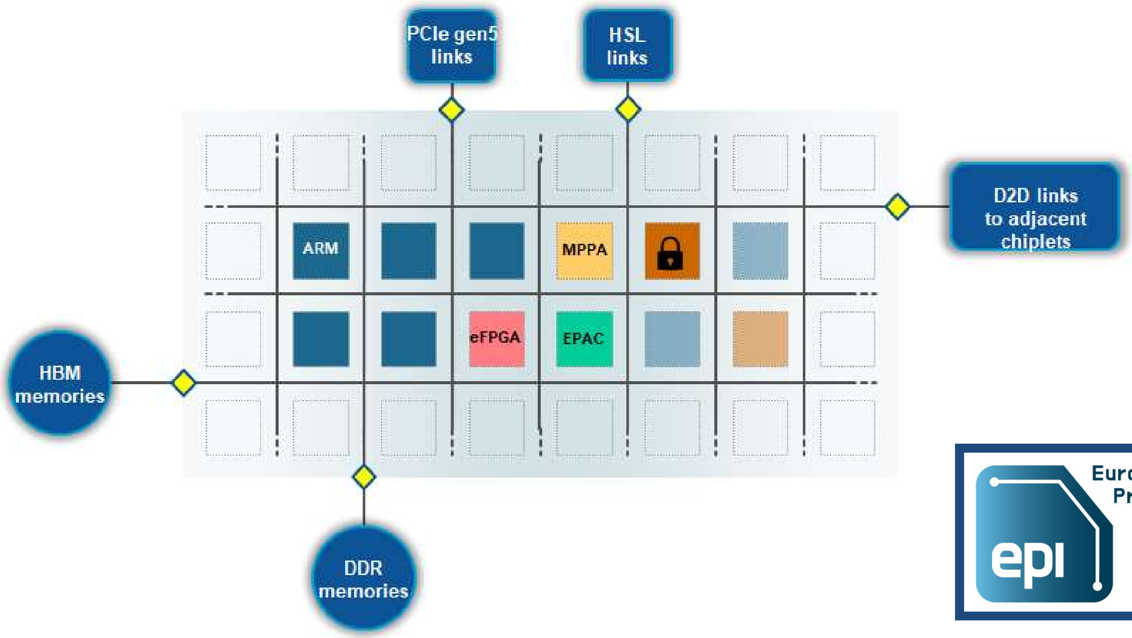
- Trends in smart vehicles & intelligent transport systems (ITS) and impact for society/economy
- University pillars: opportunities for continuous education, R&D, and technology transfer in Electronics
- Example R&D case studies:
  - Integrated Power Converters for 48 V micro/mild-hybrid vehicles
  - ITS surveillance X-band Radar
  - Cybersecurity acceleration

# ADAS needs eHPC

Recent advances and trends in on-board embedded and networked automotive systems, IEEE Transactions Industrial Informatics, 2018




NVIDIA Xavier claims 30 TOPS, Drive AGX Pegasus 160 TOPS, Tesla FSD 144 TOPS




- EPAC - EPI Accelerator
- MPPA - Multi-Purpose Processing Array
- eFPGA - embedded FPGA
- Cryptographic HW & SW (EU Sovereignty)

European Processor Initiative

***EPI RHEA chip (Multi-core ARM64b with SVE in 6 nm technology)***

# EPI partners & HW/SW eco-system

**Full HPC Environment for the Reference Platform**

**Co-design exploration space**

**Automotive eHPC software support**

**Programming tools & Libraries: LLVM/GCC with OpenMP; OpenMPI; FFTW; BLIS; OpenBLAS, …**

**Security, Low-level software, power management**

**Linux Operating System**

**EPI Processor**

**EPI Reference Hardware**

# Automotive cybersecurity: a real challenge


WIRED | Hackers Remotely
BUSINESS | CULTURE | DESIGN
ANDY GREENBERG SECURITY 07.21.15 06:00 AM
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT


Exposure to attacks: Vehicle hack, Data tampering, Denial of Service

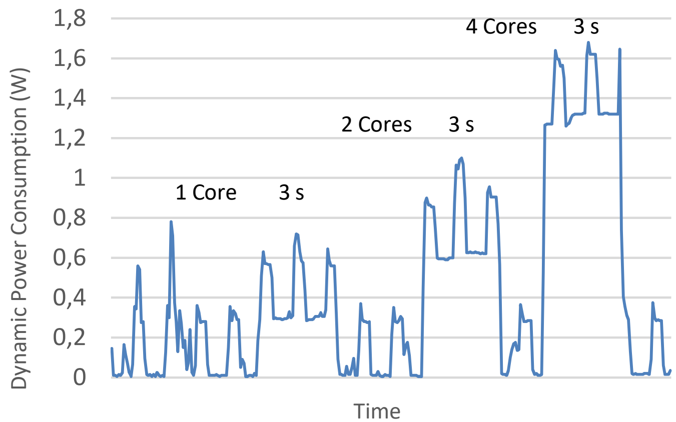
SW computing of crypto functions slow and power demanding

Performances data for SHA-2 256 and ECDSA SW implementation (Open SSL library on 4-core 64b Cortex-A53 Broadcom MPSoC)

Crypto accelerators for power-efficient and real-time on-chip implementation of secure algorithms“, IEEE ICECS 2019

| Number of core | Exec. time (s) | D (Mb) | TH (Mbps) | P (mW) | E (mJ/Mb) |
|---|---|---|---|---|---|
| 1 | 3 | 917.4 | 305.80 | 300 | 0.98 |
| 2 | 3 | 1812.8 | 604.27 | 600 | 0.99 |
| 4 | 3 | 3628 | 1209.33 | 1300 | 1.07 |

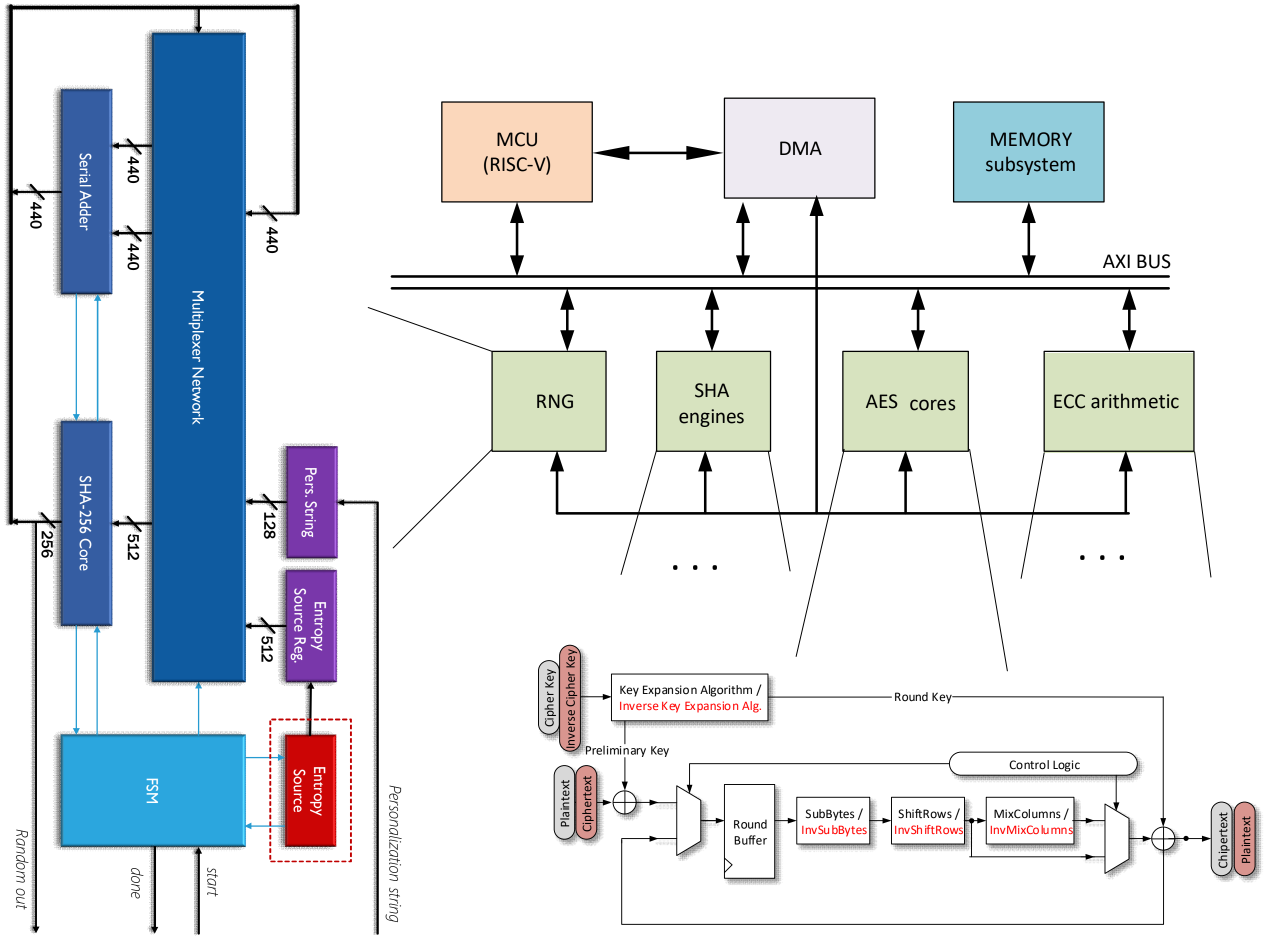
| Number of core | Exec. time (s) | D (Op) | TH (Op/s) | P (mW) | E (mJ/Op) |
|---|---|---|---|---|---|
| 1 | 10 | 282.4 | 28.24 | 310 | 10.98 |
| 2 | 10 | 560 | 56 | 620 | 11.07 |
| 4 | 10 | 1085 | 108.5 | 1330 | 12.26 |




3 orders of magnitude in speed/power improvement with HW acceleration

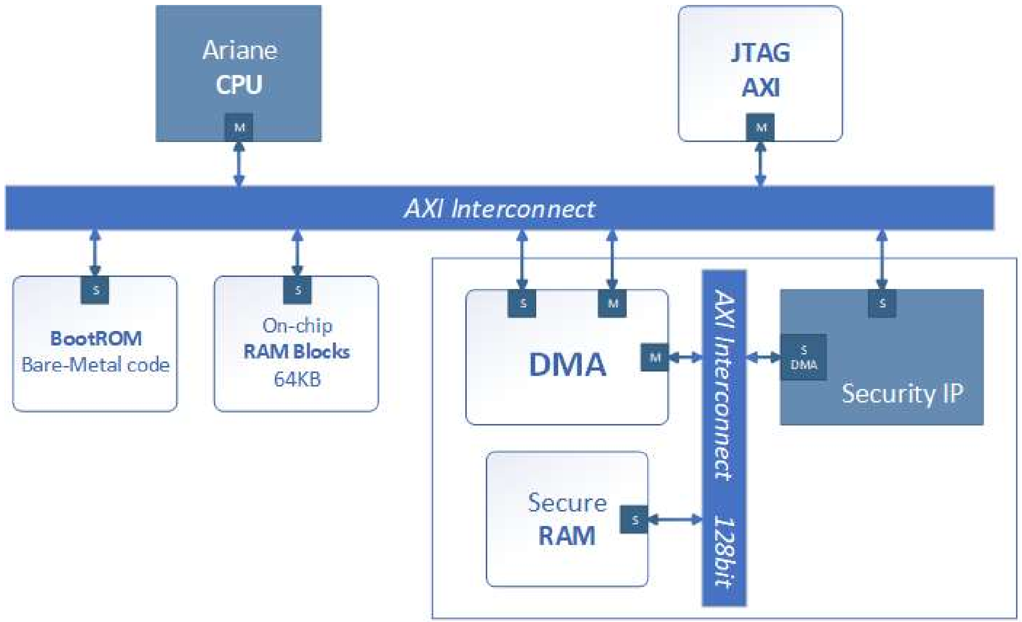
# HW-based Root of trust

- Definition of the HW and SW architecture of the Secure Element (SE) that will be the root of a trusted chain to avoid that malicious SW runs on EPI multi-cores
- The multi-core on-chip system divided in secure zones (quadrants) each with a secure MCU
- Focus on a secure boot sequence and on the relation between secure elements and power manager
- SE trustiness by proper HW/SW partitioning including: OTP/e-fuse integration, RNG for seed generation, acceleration for advanced and complex crypto functions, programmability (e.g. RISC-V plus DMA capability)



# Configurable HW crypto IPs

- Up to 300 Gbps AES XTS encryption/decryption in 7 nm
- Support core security functions needed for diffused security standard such as SHE, MACSec or WAVE, EVITA full compliant
- Design of accelerator IPs for embedded cybersecurity
  - AES 128/256 with configurable modes (ECB, CBC, CTR, OFB, CFB, CCM, CMAC, GCM, XTS) compliant with NIST SP800-38XX
  - SHA2 & SHA3, 256 and 512 bits compliant with FIPS-180/FIPS-202
  - Configurable ECC-based public key accelerator modes (ECDSA, ECIES, ECDH,..) and curves (NIST-P 256, 521) compliant with FIPS 186-3,…
  - TRNG & CSPRNG verified vs NIST SP800-90B, SP800-22




| XCZU7EV (ZCU106) | CLB LUTs | CLB Reg |
|---|---|---|
| ARIANE+AES | 75696 | 66710 |
| ECC | 77983 | 47925 |
| SHA | 16419 | 20071 |
| RNG | 10689 | 7374 |
| Misc | 6000 | 2500 |
| **Tot** | **186787** | **144580** |
| | | |
| **Available** | **230400** | **460800** |
| **Util [%]** | **81%** | **31%** |

# More than just an HW IP core

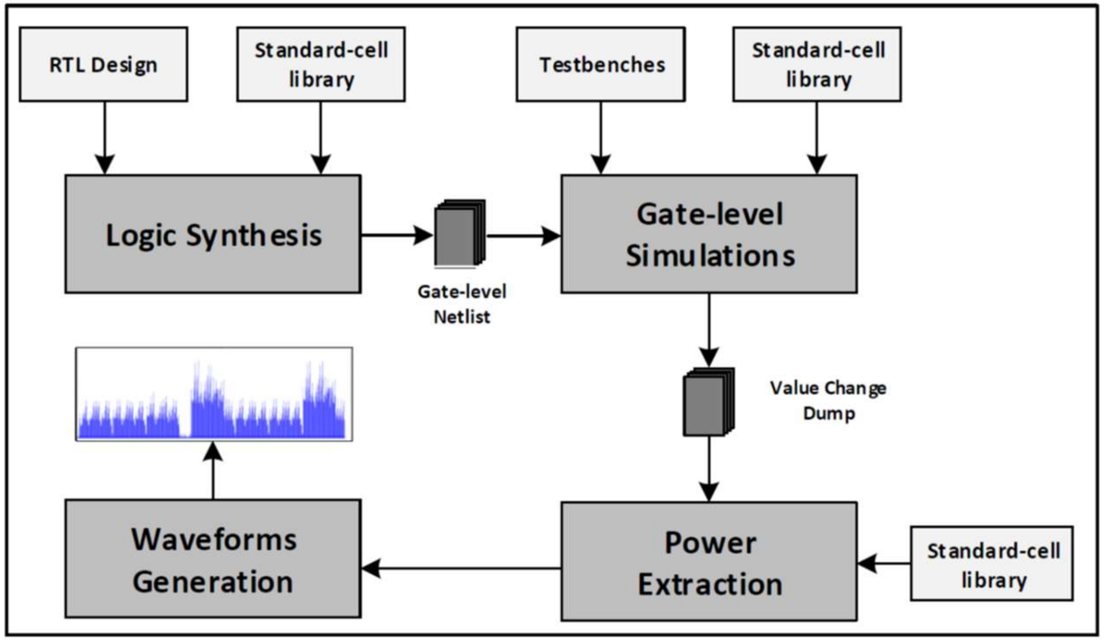
Secure management policy of keys/certificates embedded in HW, enabling advanced SW services

- Enforce good practice in sensitive data management at HW level
- Provide mechanisms at HW level to enforce usage of cryptographic algorithm and associated keys (key management interface and internal secure storage)
- Provide necessary robustness to detect and limit impact of SW bugs and attacks by enforcing strict usage rules of the crypto processor interface
  - need to know, data separation per usage, and state machine approaches
- Help to architecture the SW for high security and safety, with the concept of SW islands: simple and restricted functionality, by isolating the different operations when manipulating sensitive data; limiting access to associated sensitive data to each part
- Ease the certification of the HW/SW by using concept of independent island when dealing with the configuration of the crypto processor (locking mechanism, CPU privilege restrictions, …)
- Crypto-processor configuration and operation management

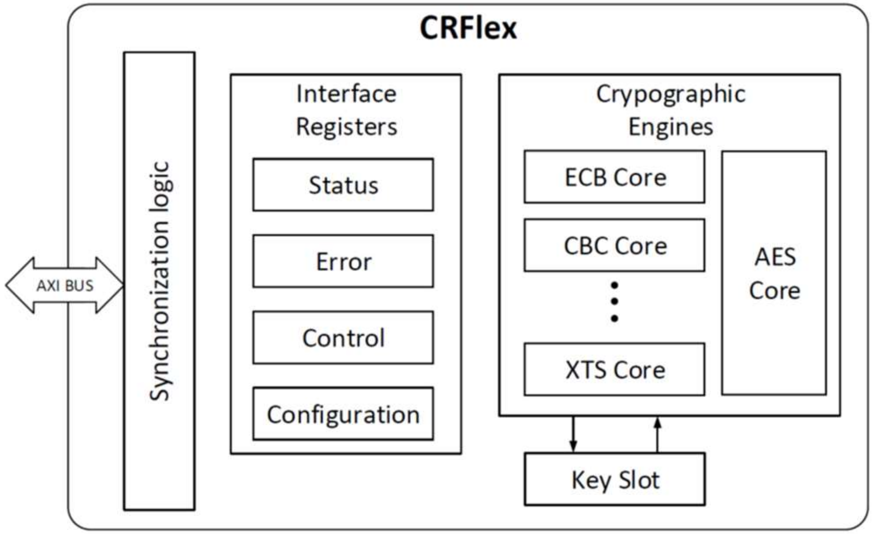
# More than just an HW IP core

Design being aware of side-channel attacks:

- Simulating (and measuring) power and EM information leakage
- Design-style to have flat power and EM profiles, particularly during safety critical operations



# AES IP design & complexity results




| CRFlex module | Slice LUT usage | Slice Register usage |
|---|---|---|
| AES Core | 23 % | 17 % |
| ECB Core | 0.2 % | 0.4 % |
| CBC Core | 0.3 % | 7 % |
| CFB Core | 1 % | 7 % |
| OFB Core | 0.3 % | 0.6 % |
| CTR Core | 0.2 % | 4 % |
| CMAC Core | 2 % | 4 % |
| GCM Core | 43 % | 17 % |
| CCM Core | 10 % | 8 % |
| XTS Core | 3 % | 2 % |
| Interface registers | 9 % | 8 % |
| Synchronization logic | 8 % | 25 % |

Slice LUTs and Registers occupation for each CRFlex sub-module on Xilinx Zynq-7000.

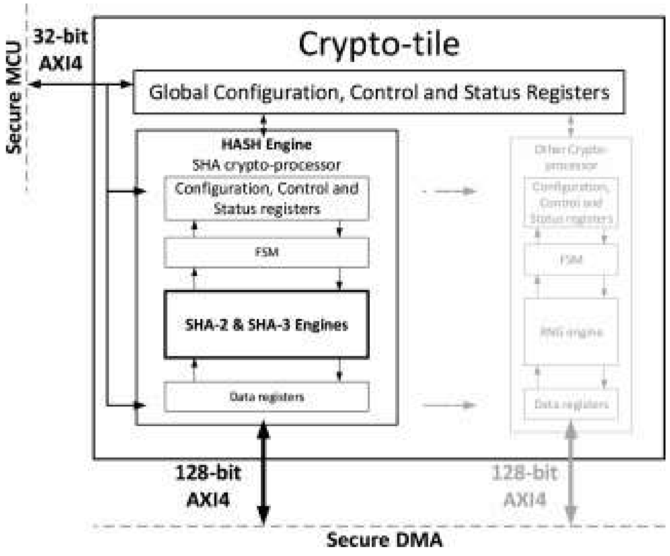
| Cipher Mode | Confidentiality | Integrity | Authenticity |
|---|---|---|---|
| AES-ECB | ✓ | ✗ | ✗ |
| AES-CBC | ✓ | ✗ | ✗ |
| AES-OFB | ✓ | ✗ | ✗ |
| AES-CFB | ✓ | ✗ | ✗ |
| AES-CTR | ✓ | ✗ | ✗ |
| AES-CMAC | ✗ | ✓ | ✗ |
| AES-GCM | ✓ | ✓ | ✓ |
| AES-CCM | ✓ | ✓ | ✓ |
| AES-XTS | ✓ | ✗ | ✗ |

7 nm ASIC at 0.75 V 85 °C

| AES-ECB-256 | | |
|---|---|---|
| # Stage(s) | Logic Usage | Throughput |
| 1 Stage | 28 kGE | 27.4 Gbps |
| 2 Stages | 55.7 kGE | 55 Gbps |
| 7 Stages | 195 kGE | 192 Gbps |
| 14 Stages | 370 kGE | 384 Gbps |

# SHA3/SHA-2 IP engine

*SHA2 and SHA-3 accelerator design in a 7 nm technology within the European Processor Initiative*, Microprocessors and Microsystems, 2020

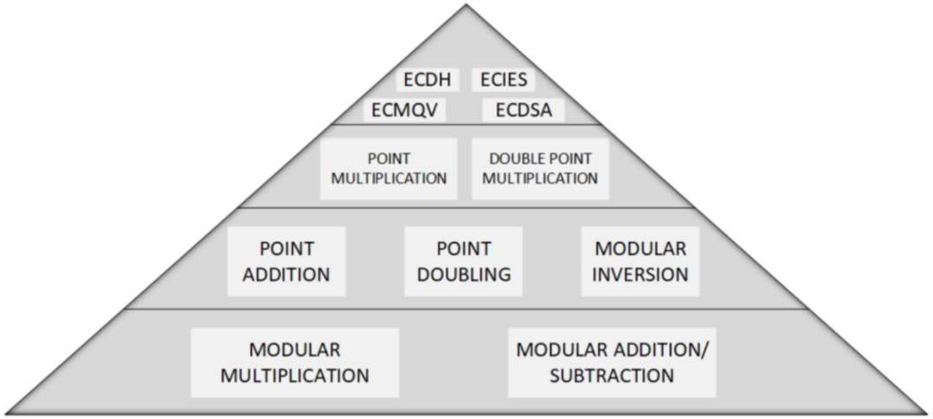


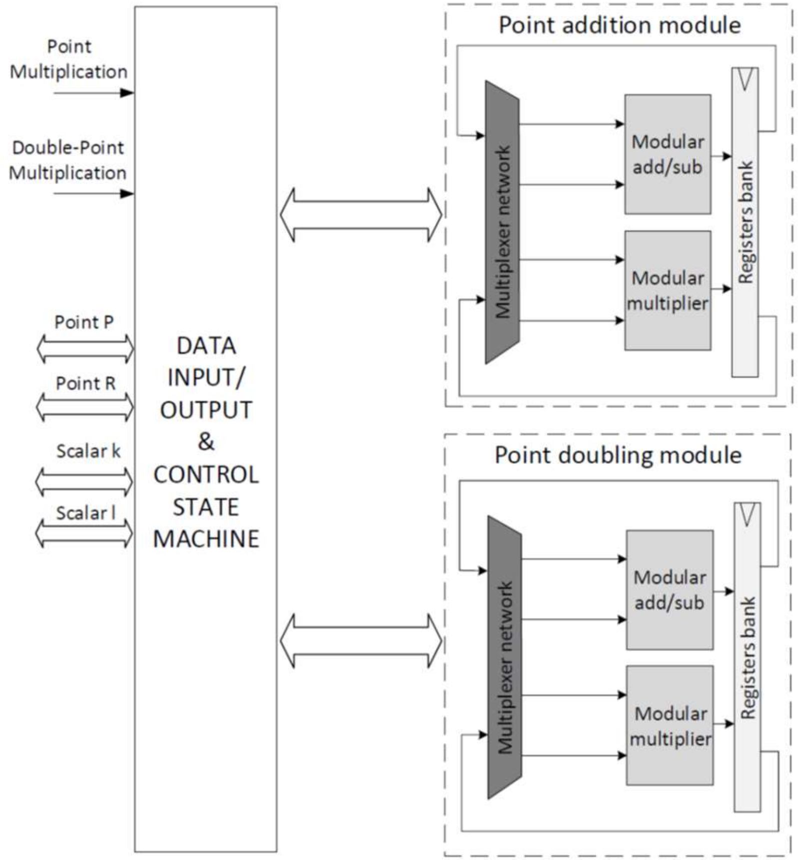

SHA-3/SHA2 in 7 nm ASIC 0.75 V 85 °C (SHA-3 @ max 5GHz, SHA2 @ max 4.35 GHz)

| Operation | Latency [Clk cycles] | Throughput [Gbps] |
|---|---|---|
| SHA2 224 | 67 | 33.24 |
| SHA2 256 | 67 | 33.24 |
| SHA2 384 | 83 | 53.67 |
| SHA2 512 | 83 | 53.67 |
| SHA-3 224 | 25 | 230.40 |
| SHA-3 256 | 25 | 217.60 |
| SHA-3 384 | 25 | 166.40 |
| SHA-3 512 | 25 | 115.20 |

| Operation | Area, kGE SHA-3 | Area, kGE SHA2 | Power, mW SHA-3 | Power, mW SHA2 |
|---|---|---|---|---|
| 224 | 31.27 | 15.43 | 24.96 | 13.43 |
| 256 | 31.55 | 15.45 | 25.29 | 13.45 |
| 384 | 31.36 | 28.28 | 25.07 | 22.56 |
| 512 | 30.74 | 29.93 | 25.67 | 24.66 |
| 256-224 | 31.65 | 15.47 | 25.19 | 13.47 |
| 384-256 | 31.93 | 31.33 | 24.03 | 21.47 |
| 384-224 | 32.47 | 31.14 | 24.80 | 21.67 |
| 512-384 | 32.17 | 30.32 | 27.54 | 24.97 |
| 512-256 | 31.85 | 31.26 | 26.18 | 21.47 |
| 512-224 | 32.11 | 31.35 | 25.73 | 21.44 |
| 384-256-224 | 32.21 | 31.19 | 25.41 | 21.46 |
| 512-256-224 | 32.33 | 31.42 | 26.33 | 21.51 |
| 512-384-224 | 32.21 | 31.62 | 25.58 | 21.68 |
| 512-384-256 | 33.07 | 31.92 | 23.18 | 21.69 |
| 512-384-256-224 | 33.43 | 31.79 | 25.29 | 21.70 |

# ECC IP engine



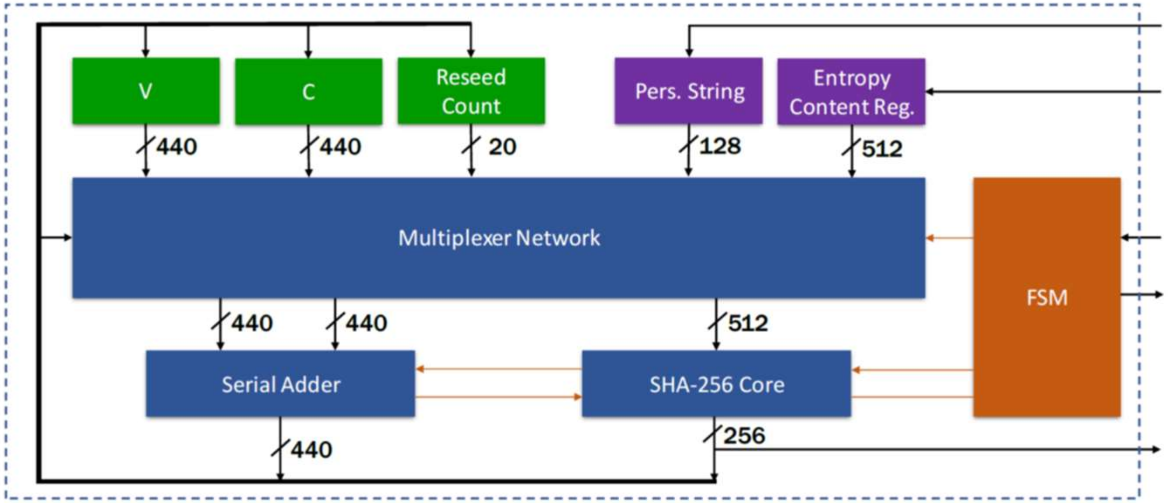

*Fast and configurable elliptic curve crypto-processor on 7 nm technology*, Microprocessors and Microsystems, 2021

7 nm ASIC at 0.75 V 85 °C

| Configuration | Technology | Gate counts (kGE) | Kcycles | Freq. (MHz) | T($us$) |
|---|---|---|---|---|---|
| **P-256 only** | 45 nm | 281 | 36.390 | 400 | 90.975 |
| **P-521 only** | 45 nm | 407 | 254.456 | 375 | 686.54 |
| **P-256/-521** | 45 nm | 447 | 36.390/257.456 | 375 | 97.04/686.54 |
| **P-256 only** | 7 nm | 279 | 36.390 | 1820 | 19.99 |
| **P-521 only** | 7 nm | 405 | 257.456 | 1650 | 156.03 |
| **P-256/-521** | 7 nm | 445 | 36.39/257.456 | 1650 | 22.05/156.03 |

# CSPNRG IP engine

the 7 nm Artisan ASIC standard-cell reaches a throughput value of 19.67 Gbps, given a maximum clock frequency of 5.15 GHz, requiring an overall complexity of 46.56 kGE.




Two Entropy seed options:
- external seed
- on-chip TRNG made of a mix of Fibonacci and Galois digital Ring-Oscillators

| Test | Block/Template Length | Pass Rate |
|---|---|---|
| Frequency (Monobit) | - | 0.9924 |
| Frequency Within a Block | 256 | 0.9876 |
| Runs | - | 0.9901 |
| Longest-Run-of-Ones in a Block | - | 0.9878 |
| Binary Matrix Rank | - | 0.9901 |
| Discrete Fourier Transform (Spectral) | - | 0.9874 |
| Non-overlapping Template Matching | 10 | [0.9801–0.9974] |
| Overlapping Template Matching | 10 | 0.9848 |
| Maurer's Universal Statistical | - | 0.9901 |
| Linear Complexity | 1024 | 0.9900 |
| Serial | 16 | 0.9825, 0.9876 |
| Approximate Entropy | 10 | 0.9901 |
| Cumulative Sums (Cusums) | - | 0.9901 |
| Random Excursions | - | [0.9826–0.9947] |
| Random Excursions Variant | - | [0.9875–0.9975] |

NIST Statistical Test Suite parameters and results

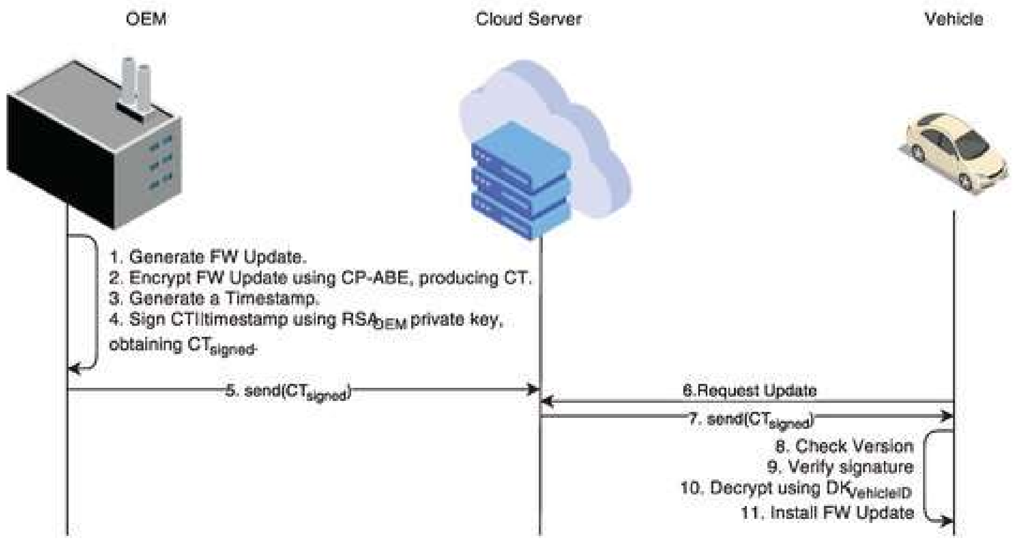


Cryptographically Secure Pseudo-Random Number Generator IP-Core Based on SHA2 Algorithm, Sensors 2020

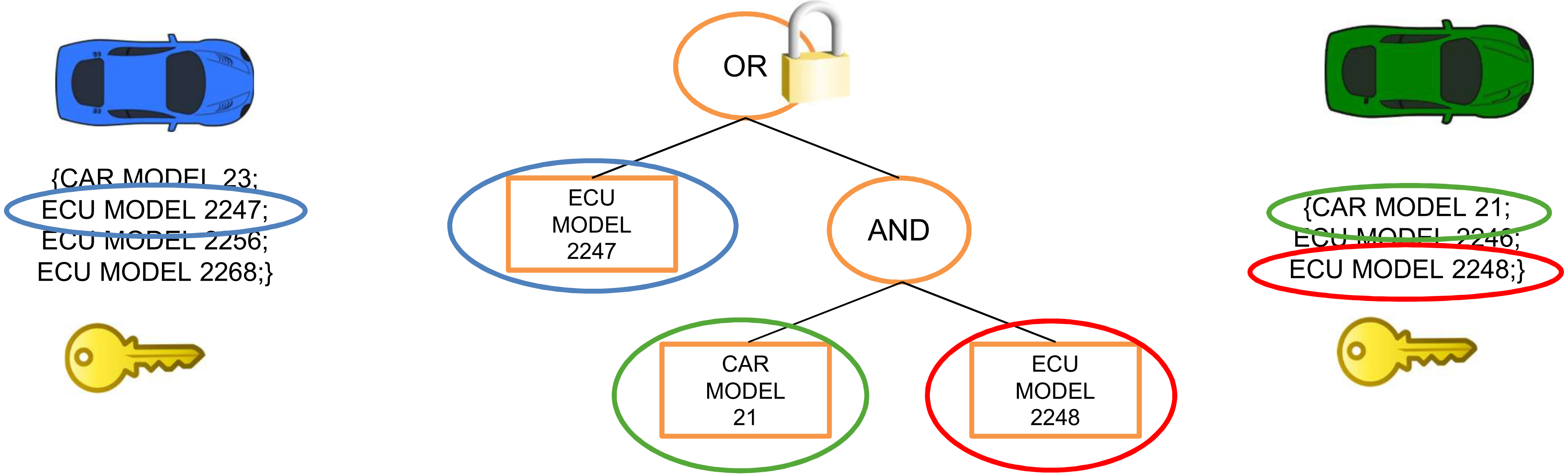
True Random Number Generator Based on Fibonacci-Galois Ring Oscillators for FPGA, Applied Sciences 2021

# ABE Over The Air (OTA) SW/FW UPDATE

Attribute Based Encryption (ABE) is an asymmetric key encryption scheme that allows one to embed an Access Control Mechanism inside a ciphertext by means of a Policy, which is a Boolean expression upon some values, called attributes



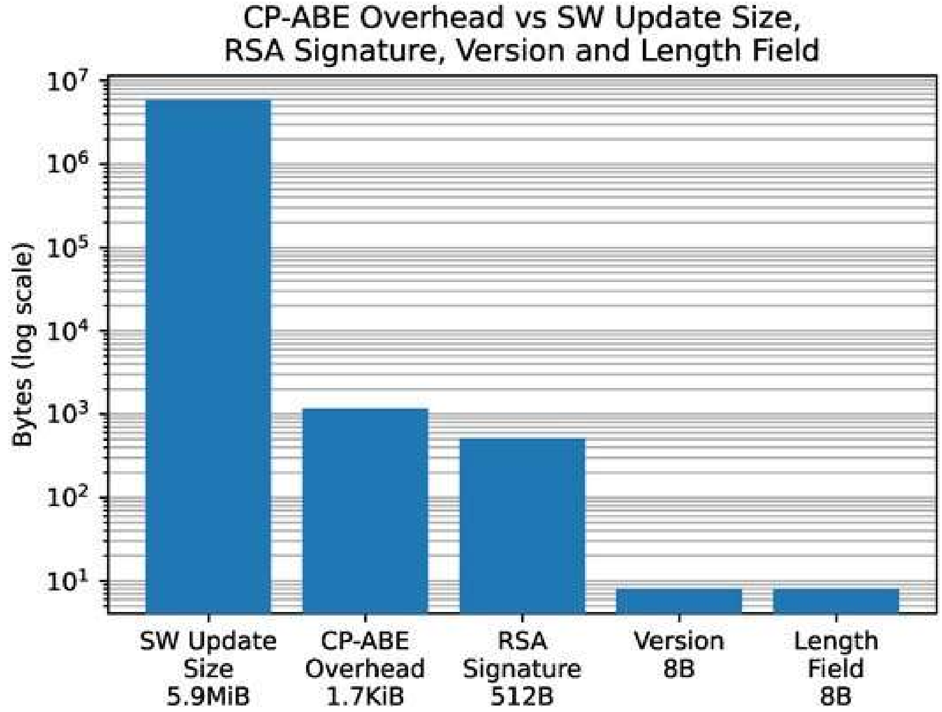

«The more attribute you *need* to decrypt a ciphertext, the more operations you must perform»

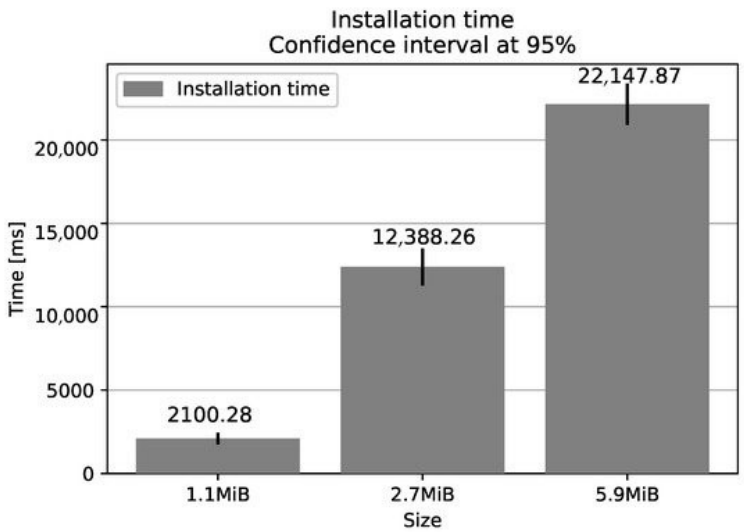


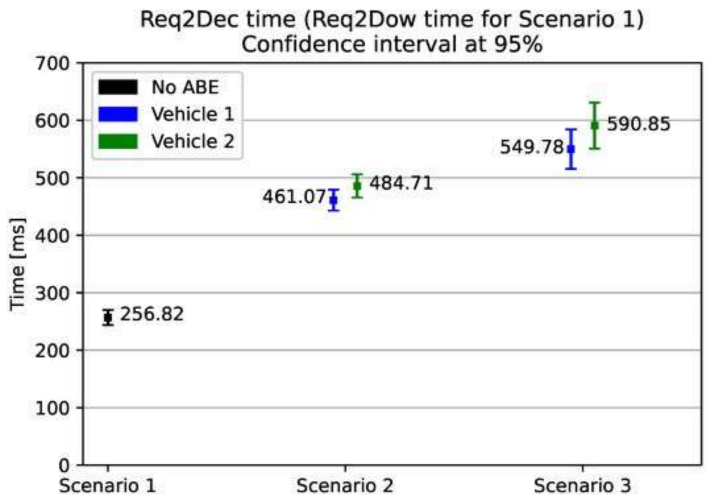

IDEA: FW/SW updates are encrypted in such a way only authorized ECUs can decrypt them
ADVANTAGE: encrypted FW/SW updates can transit or rest on untrusted cloud servers

# ABE OTA overhead

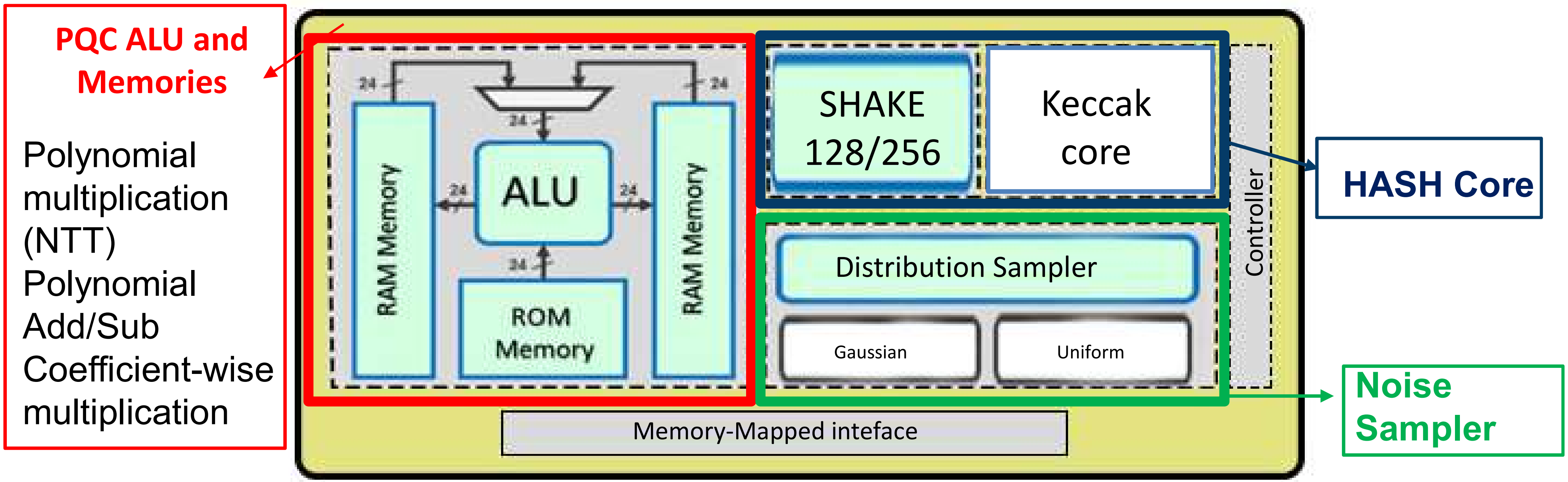
Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update, Sensors 2021



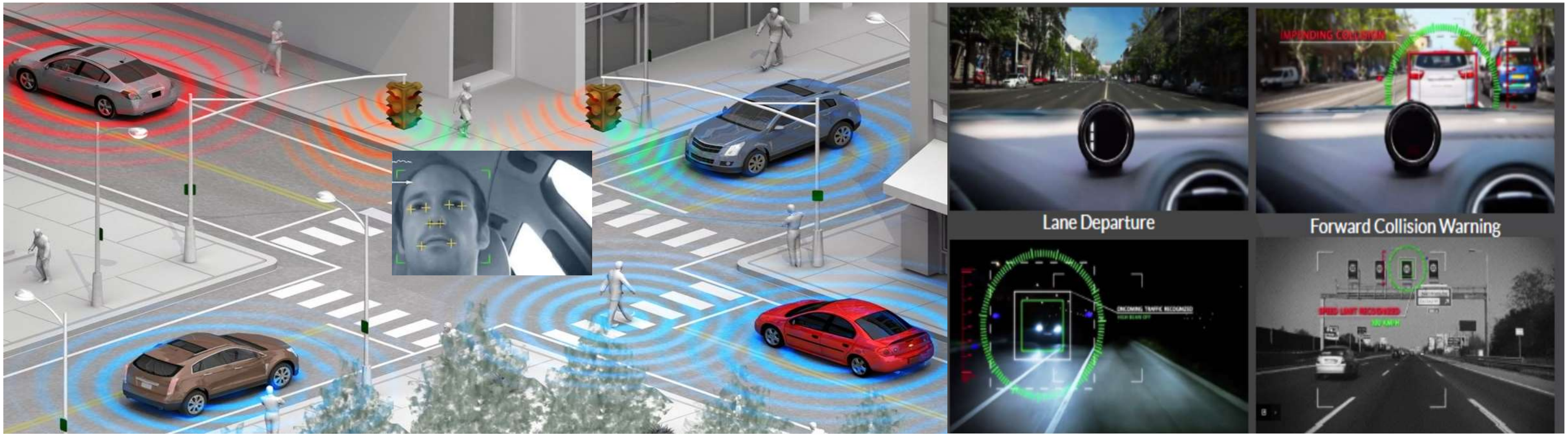
# PQC Lattice Hardware accelerator




**HW acceleration allows x 300 gain vs SW solution**
**Prototype and test on ZCU106**
**70 kGE + 1 MB and 0.6 GHz in 45nm**

| Block name | Max freq | CLB LUTs | CLB reg | BRAM | DSP |
|---|---|---|---|---|---|
| ALU+Memories | 300 MHz | 1882 | 4399 | 14,5 | 8 |
| NOISE SAMPLER | 370 MHz | 227 | 532 | 0 | 4 |
| SHAKE | 750 MHz | 5642 | 2969 | 0 | 0 |
| TOTAL | 300 MHz | 8627 | 4713 | 14,5 | 12 |

# Conclusions




- Vehicular electronics: high impact on society and fast growing trends in digital and electrified vehicles & intelligent transport systems (ITS)
- Opportunities from reskilling needs (continuous learning), upgrade of Electronics University teaching offer
- Huge scientific R&D field (Horizon Europe, PNRR)
- Technology transfer and consulting opportunities
- Spin-off in related fields (robotics, energies, avionics, …)
- Challenge: effort to go beyond the classic EE comfort zone

# Thanks for your attention

Prof. Ing. Sergio Saponara
+39 3468790937

**sergio.saponara@unipi.it,**
**https://www.linkedin.com/in/sergio-saponara-3031431/**

https://www.youtube.com/watch?v=Bg8zw1SWiJA&feature=youtu.be
Sistemi elettronici per mobilità intelligente

https://www.youtube.com/watch?v=2Y7uLbpehcQ&list=PL13CyHsHfOt1GC19RsPv-FvITnbbnd2e0&index=7
Integrated Serializer and High-speed driver for mulTi-gbps And Rad-Hard links