



**HAL**  
open science

## Covert Communications in Heterogeneous SoCs

Carlos Andres Lara-Nino, Lilian Bossuet

► **To cite this version:**

Carlos Andres Lara-Nino, Lilian Bossuet. Covert Communications in Heterogeneous SoCs. École d'hiver Francophone sur les Technologies de Conception des Systèmes Embarqués Hétérogènes (FETCH), Université Libre de Bruxelles, Feb 2024, Maillen, Belgium. hal-04467933

**HAL Id: hal-04467933**

**<https://hal.science/hal-04467933v1>**

Submitted on 20 Feb 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License



fεtCh 2024

## Communications cachées dans des SoC hétérogènes

---

Carlos Andres LARA-NINO

École d'hiver Francophone sur les Technologies de Conception des Systèmes Embarqués Hétérogènes (FETCH)

Maillen, Belgique

Février 7-9, 2024

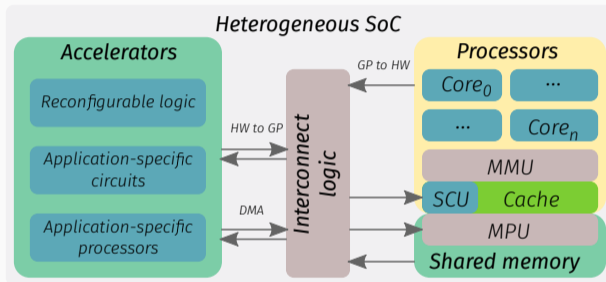
Université Jean Monnet Saint-Etienne, CNRS, Laboratoire Hubert Curien

UMR 5516, F-42023, SAINT-ETIENNE, France

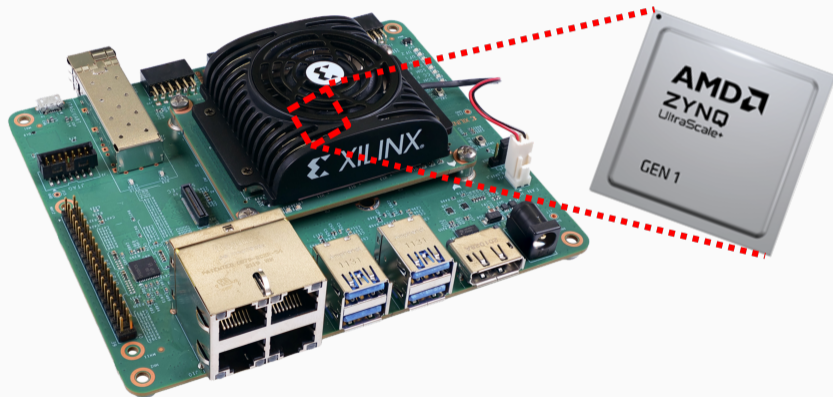


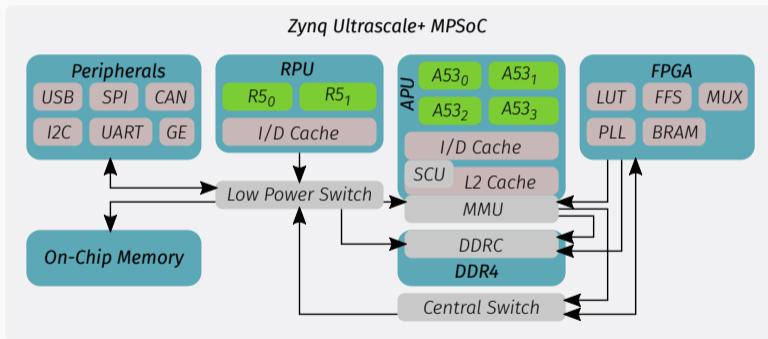
# System(s)-on-a-Chip

---



A **system-on-a-chip (SoC)** is a device which integrates multiple processing elements in the same die. An **heterogeneous SoC** may feature different processors, hardware accelerators, and even an FPGA.





## Intrinsic channels

---

The shared resources of the SoC may be leveraged to covertly transfer information.

## Attack goals

- Bypass isolation policies
- Change the nature of the channel<sup>1</sup>
- Enable more complex attacks<sup>2</sup>

---

<sup>1</sup> Benhani, E.M. & Bossuet, L. (2018). DVFS as a security failure of TrustZone-enabled heterogeneous SoC. In *25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)* (pp. 489-492). IEEE.

<sup>2</sup> Fellah-Touta, A., Bossuet, L., & Lara-Nino, C. A. (2023). Combined Internal Attacks on SoC-FPGAs. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 281-286). IEEE.



Require:  $k$ , an encryption key

Require:  $p$ , a plaintext to be encrypted

*covert\_bit\_set()*

AES( $p, k$ )

*covert\_bit\_clear()*

{Pull trigger}

{Release trigger}

**Require:**  $k$ , an encryption key

**Require:**  $p$ , a plaintext to be encrypted

**Require:**  $f, f'$ , two core frequencies

$\text{cpu\_freq} \leftarrow f'$

$\text{AES}(p, k)$

$\text{cpu\_freq} \leftarrow f$

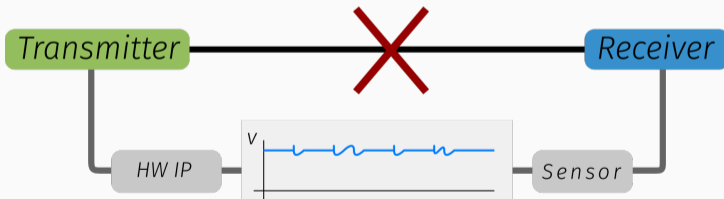
{Pull trigger}

{Release trigger}

















## Challenges

- Many intrinsic channels available
- Implementation strategies change from one platform to another
- Mitigating the attack, once discovered, is complicated

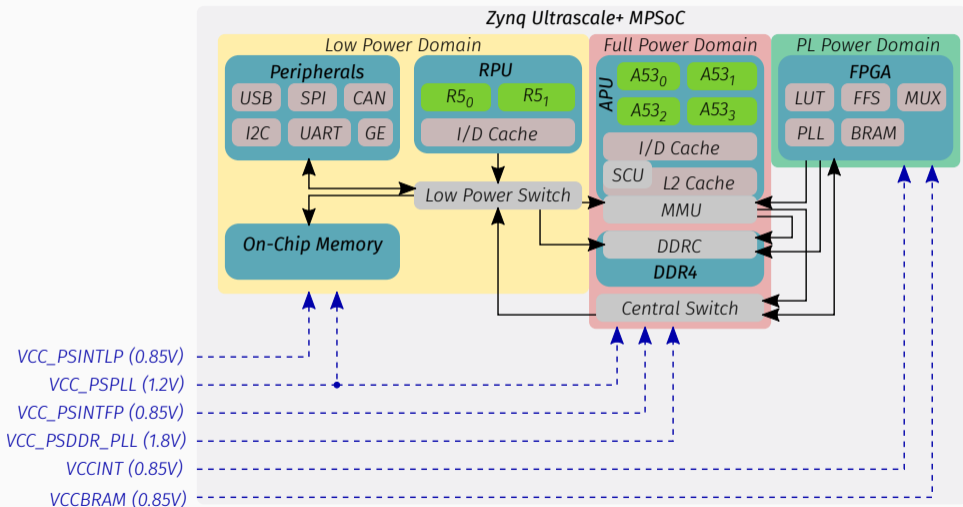


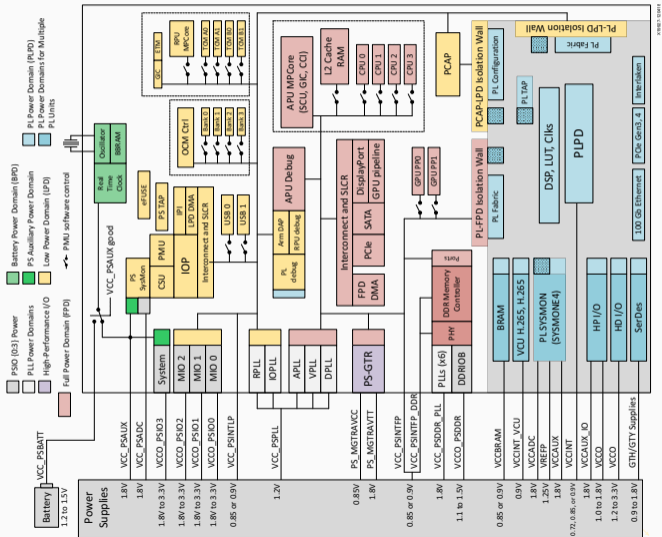
### Potential approaches

- Conventional study of architectural vulnerabilities
- Implementation of stricter isolation rules
- Use of pre-silicon tooling for the study of intrinsic channels

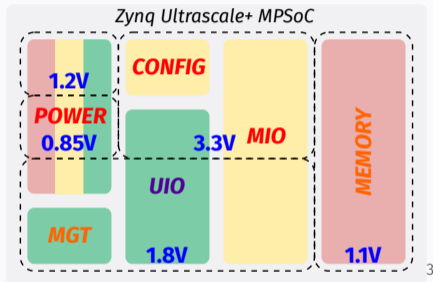
## Case studies

---

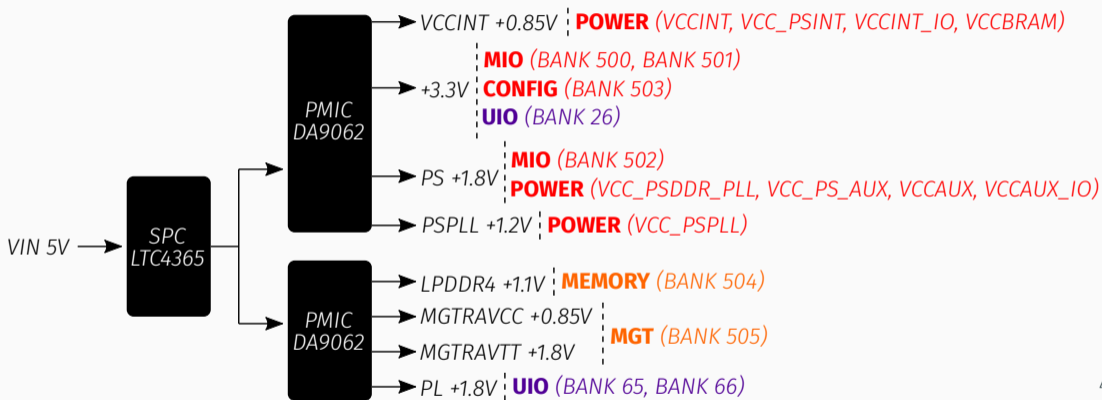




ARM 9001



<sup>3</sup> [https://shop.trenz-electronic.de/Download/?path=Trenz\\_Electronic/Development\\_Boards/TE0802/REV02/Documents](https://shop.trenz-electronic.de/Download/?path=Trenz_Electronic/Development_Boards/TE0802/REV02/Documents)



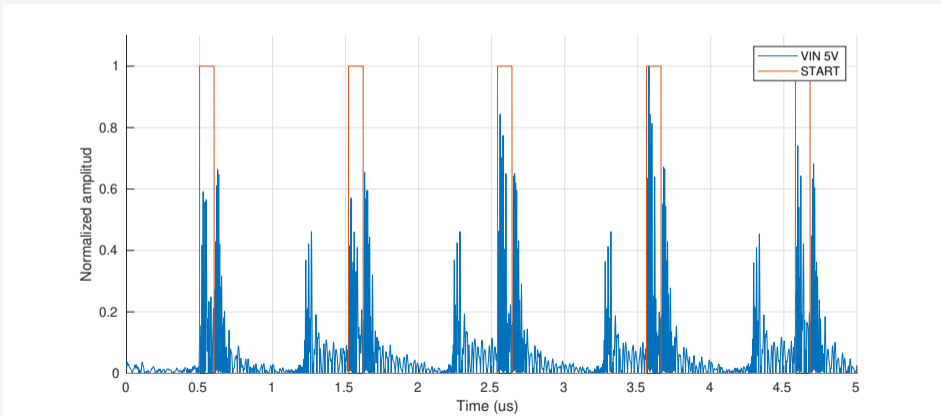
<sup>4</sup> [https://shop.trenz-electronic.de/Download/?path=Trenz\\_Electronic/Development\\_Boards/TE0802/REV02/Documents](https://shop.trenz-electronic.de/Download/?path=Trenz_Electronic/Development_Boards/TE0802/REV02/Documents)

## Considerations

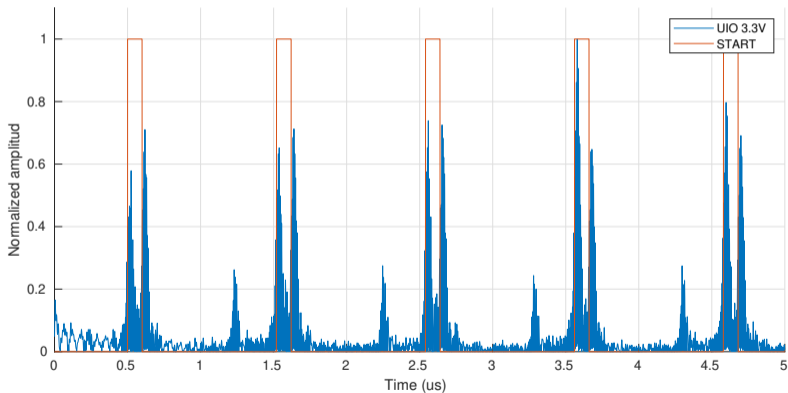
- Transmitter: Hardware accelerator in the FPGA
- Receiver: External
- Shared resource: **V\_PL**

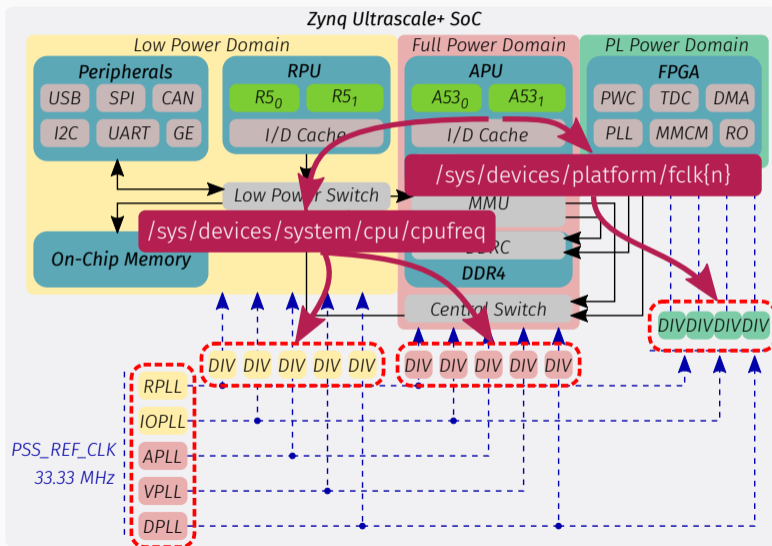


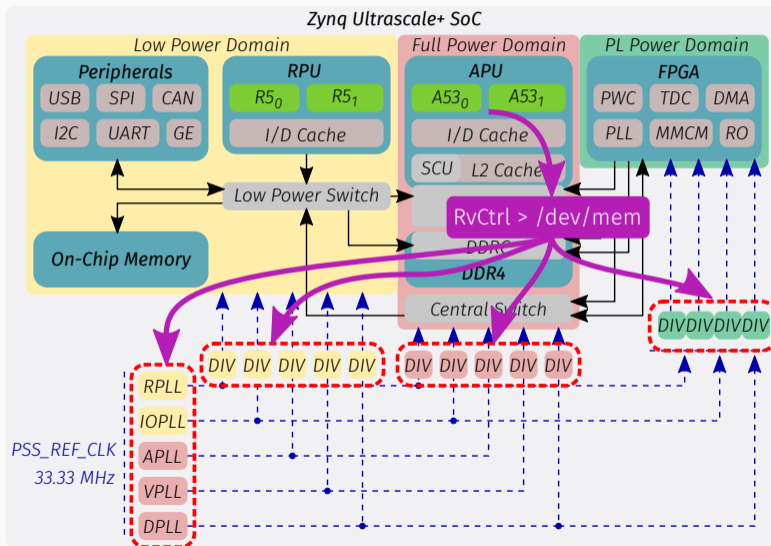
## PDN intrinsic channel



## PDN intrinsic channel



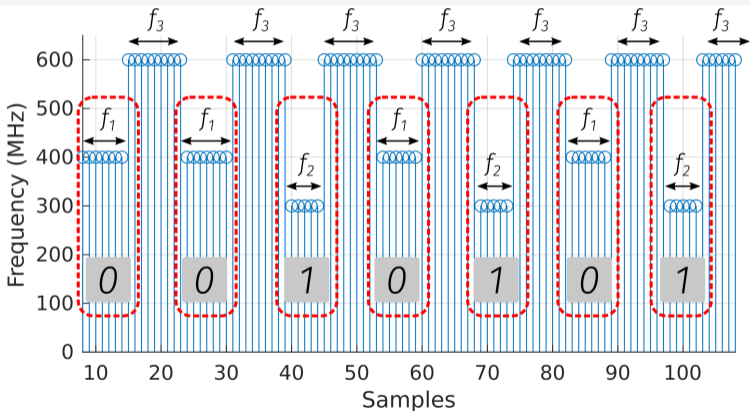




## Considerations

- Transmitter: User application coded in C
- Receiver: User application coded in C
- Shared resource: **cpufreq driver**

## DVFS intrinsic channel



## Final remarks

---

- Intrinsic channels have niche applications but are difficult to mitigate
- Their transmission rate is low, but the volume of information required is not high
- We need to rethink the design of SoC platforms to introduce more effective isolation strategies





This work has been supported by the French government in the framework of the *France 2030* initiative under project ARSENE (ANR-22-PECY-0004).

Thanks !

---