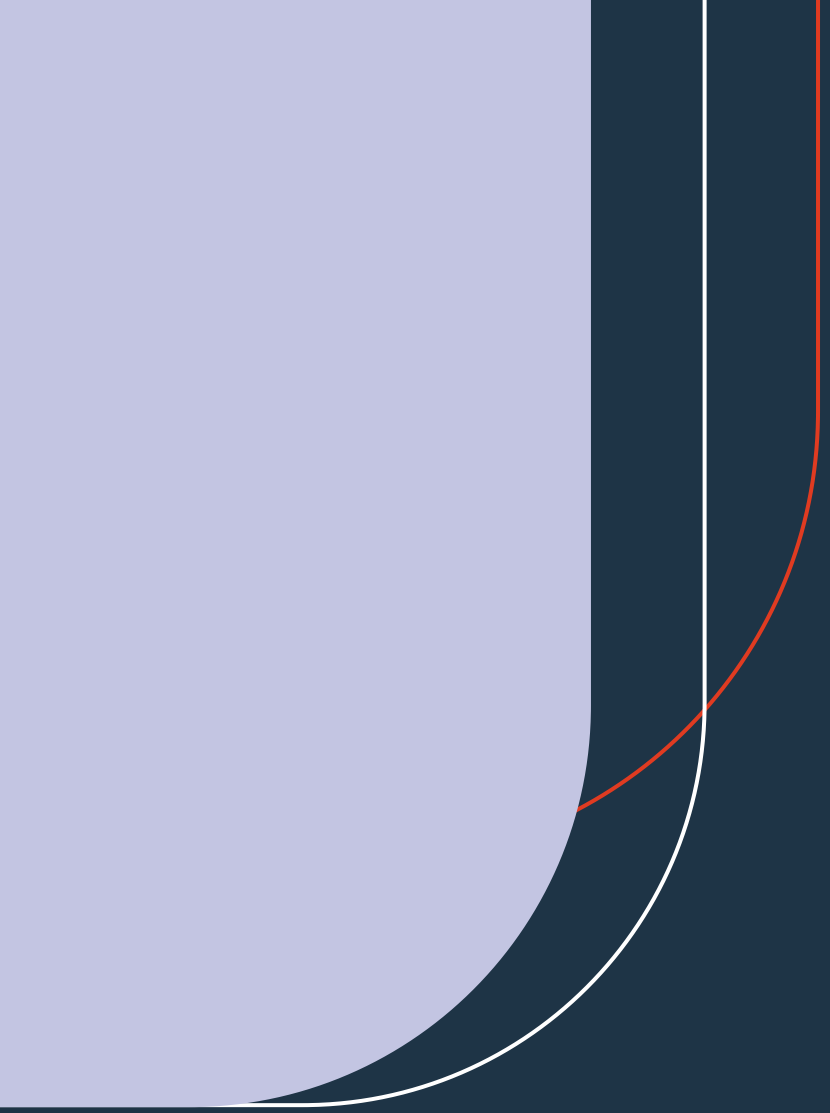


SnT

Interdisciplinary Centre for Security, Reliabilty and Trust

Rethinking dependability from ground up

Marcus Völp

uni.lu

Rethinking Dependability from Ground Up

A380

Primary: Power PC755 (66 MHz → 98 MHz)
(Flight Control & Guidance)

Secondary: DSP Sharc (40 MHz)

Control Engineering Practice

AIRBUS state of the art and practices on FDI and FTC in flight control system

Philippe Goupil *

P. Goupil AIRBUS state of the art and practices on FDI and FTC in flight control system

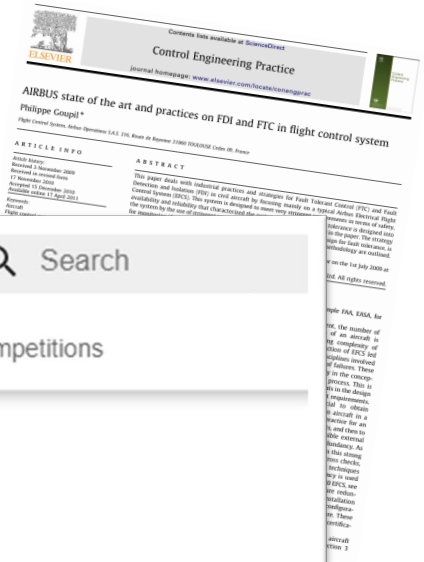
Redundancy and Diversity

AurixTM TC4x

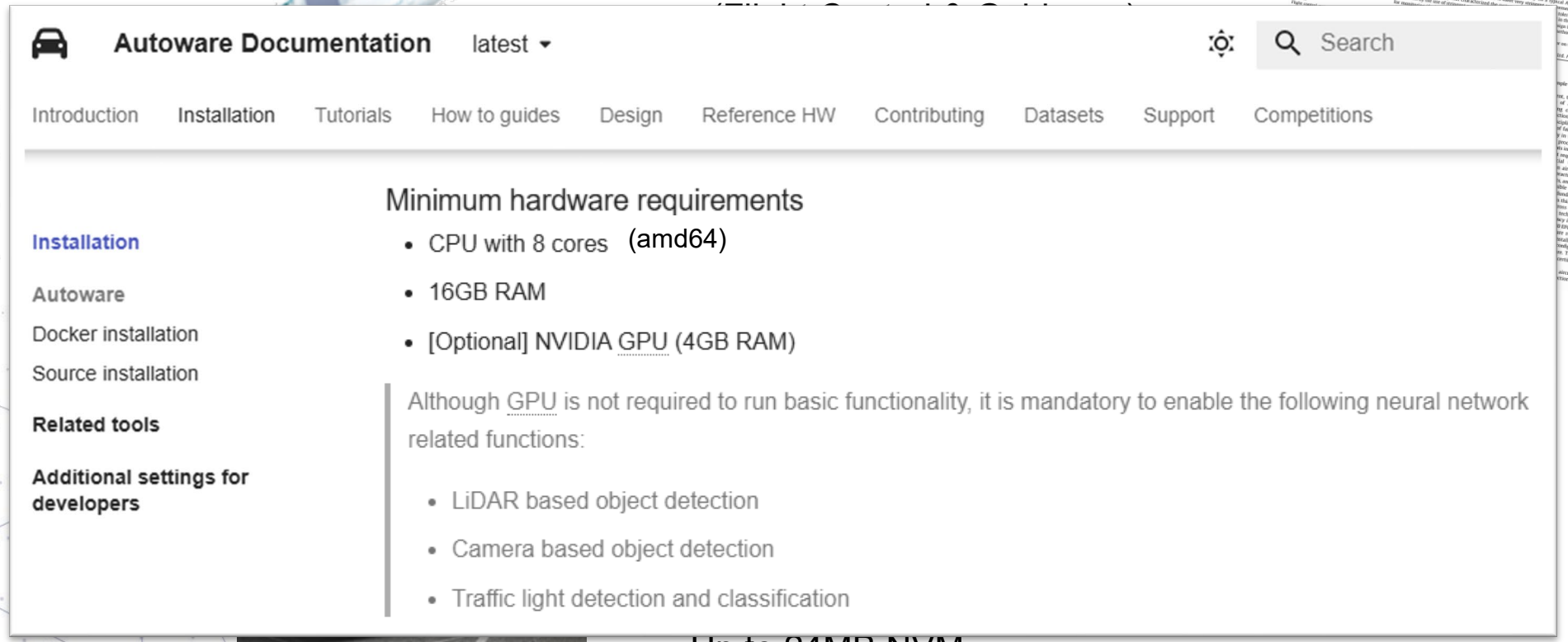
- Up to 6x Tricore™1.8 (500MHz)
- ISO26262 ASIL-D + ISO 21434 certification
- Up to 24MB NVM

https://www.infineon.com/assets/row/public/documents/10/156/infineon-tc4x-overview-productpresentation-en.pdf

Rethinking Dependability from Ground Up



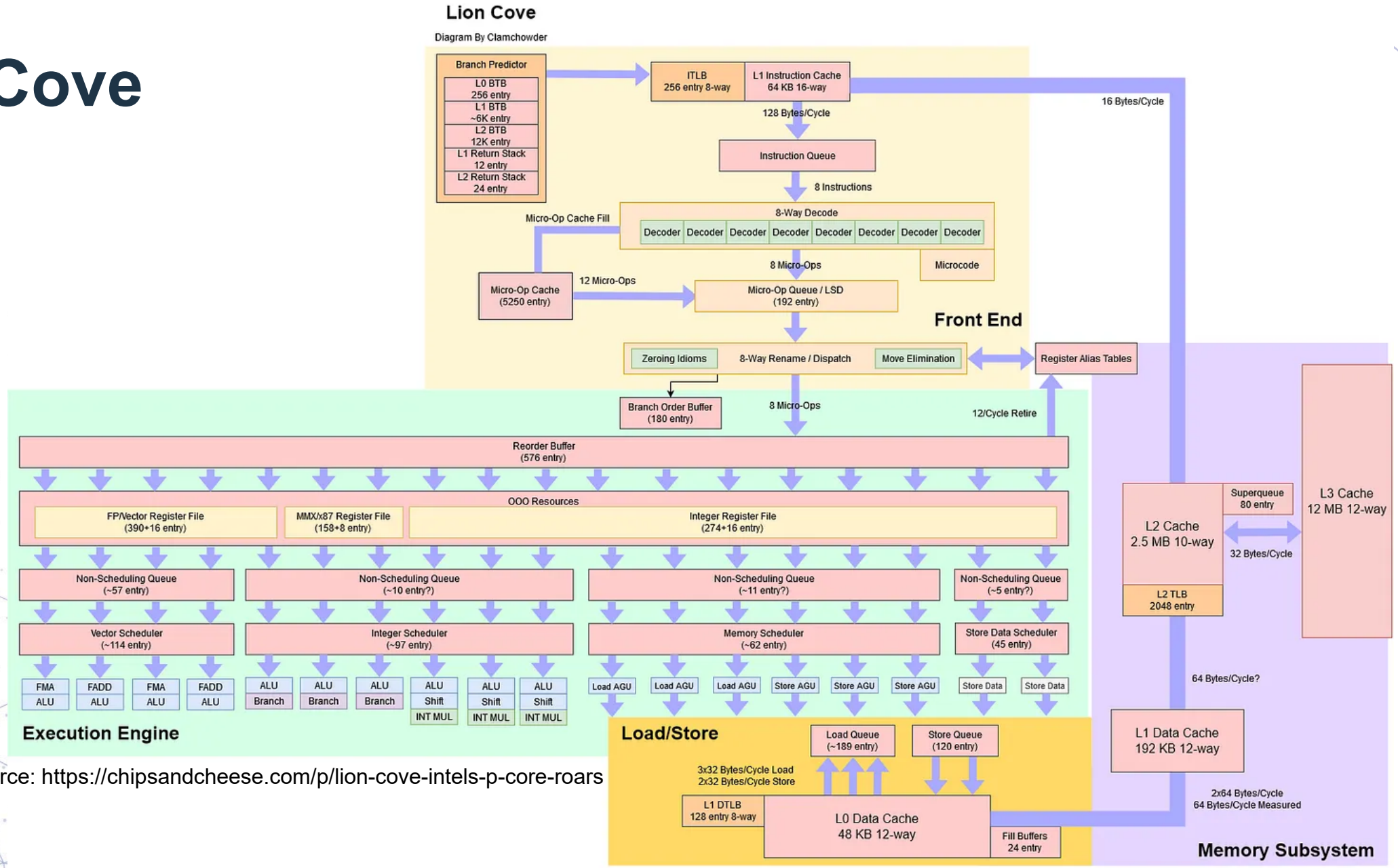
Primary: Power PC755 (66 MHz → 98 MHz)



- Up to 24MB NVM

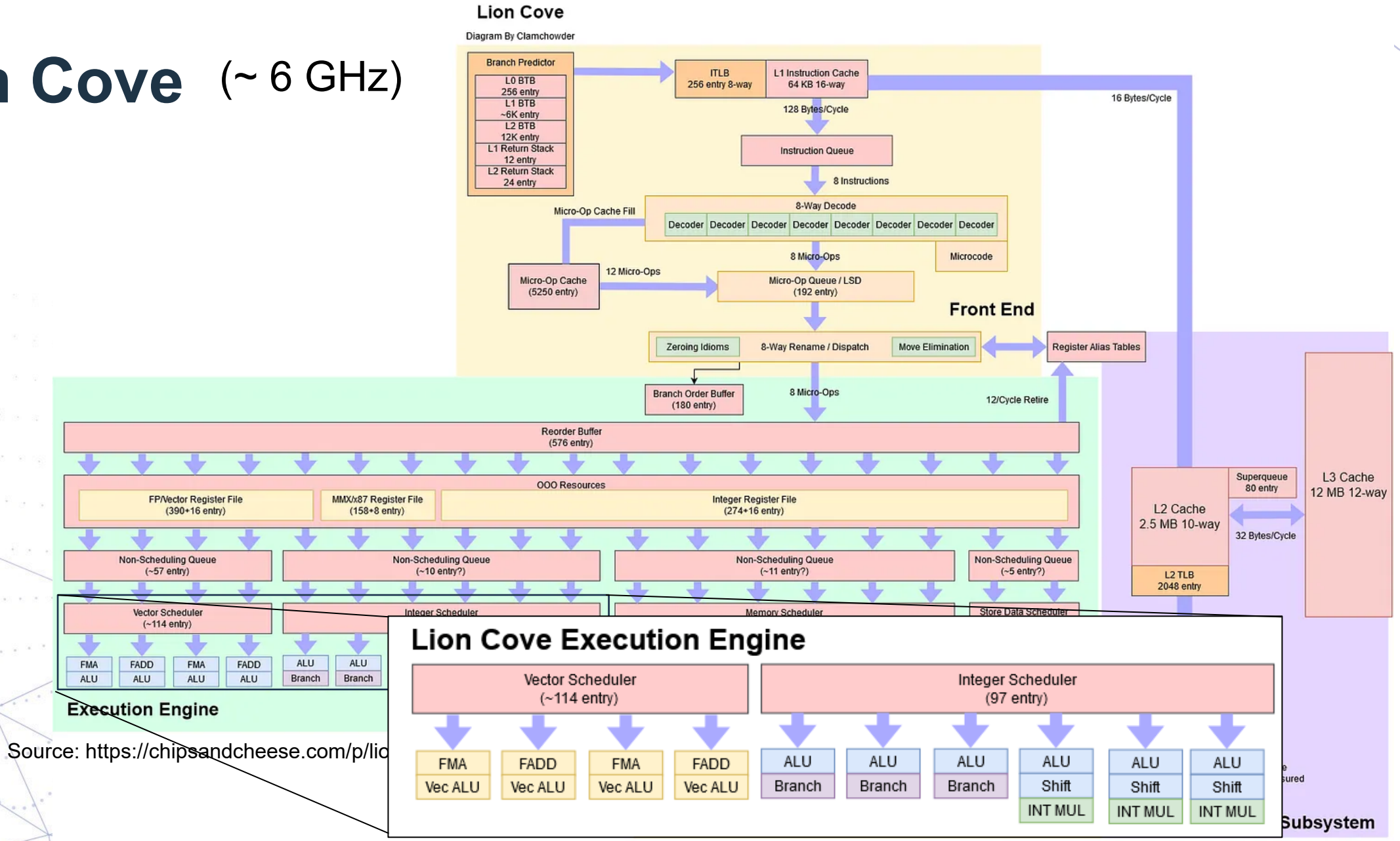
https://www.infineon.com/assets/row/public/documents/10/156/infineon-tc4x-overview-productpresentation-en.pdf

Lion Cove



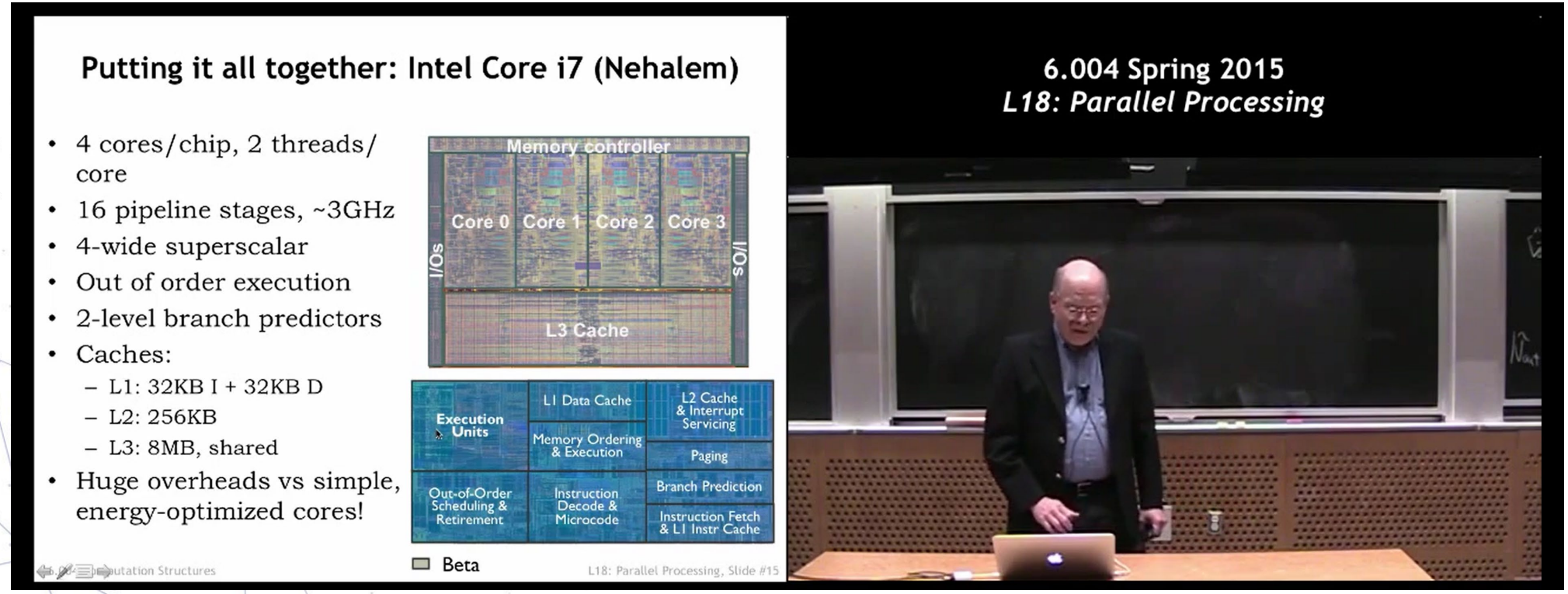
Source: https://chipsandcheese.com/p/lion-cove-intels-p-core-roars

Lion Cove (~ 6 GHz)



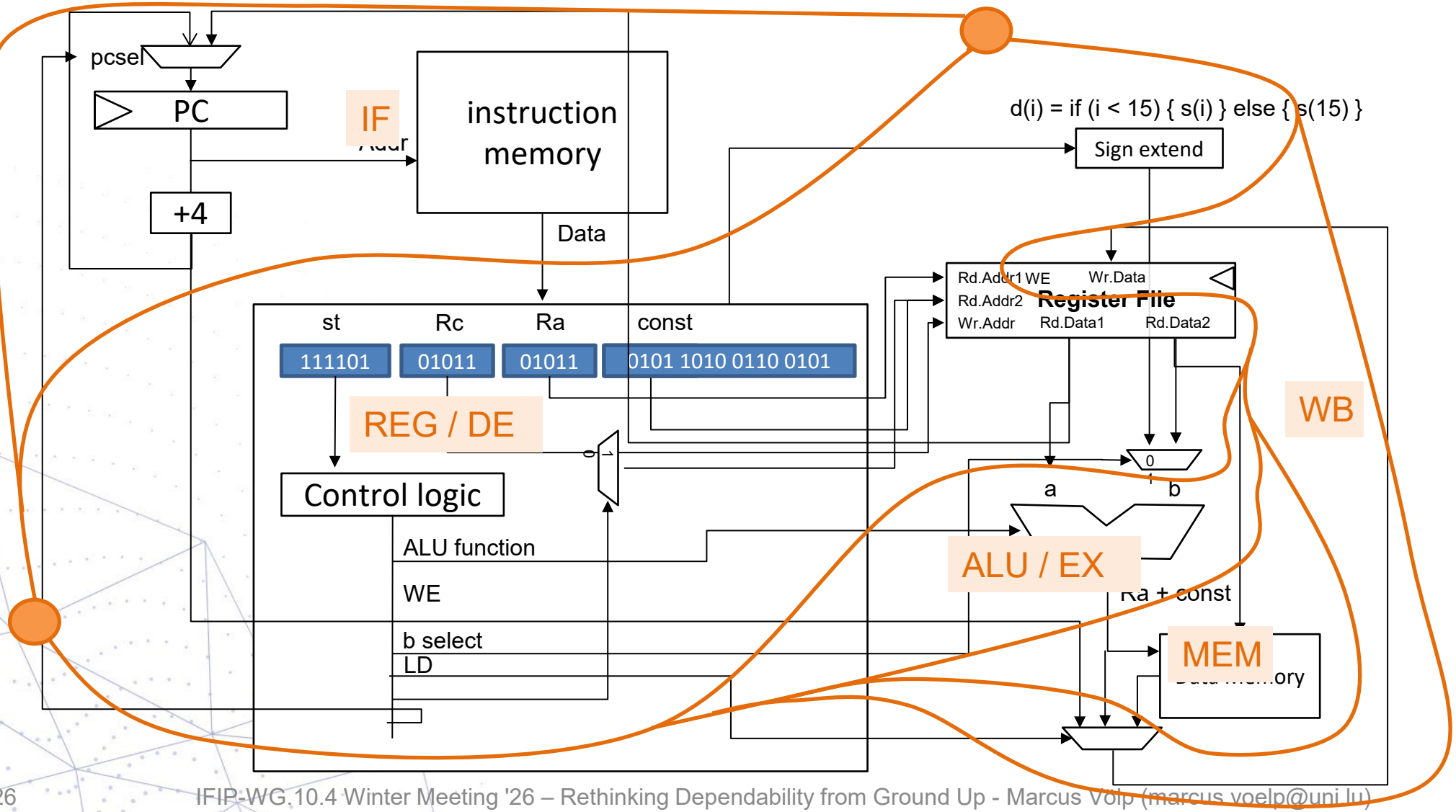
Source: https://chipsandcheese.com/p/lic

Chris Terman

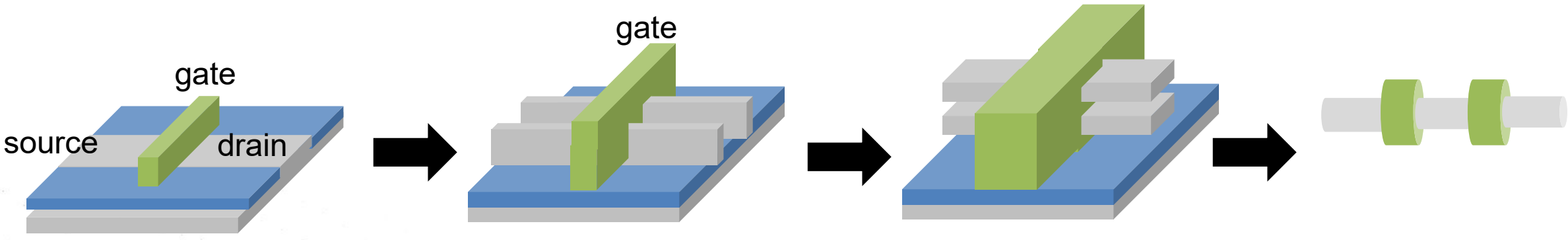


Playlist of 2017 course:
https://www.youtube.com/watch?v=R0tFDXBZvKI&list=PLUl4u3cNGP62WVs95MNq3dQBqY2vGOtQ2

A simple pipelined processor



Problems of Continuous Scale



Sunil Pathania et al.
Analyzing Crosstalk-Induced Effects in Rough On-Chip Copper Interconnects

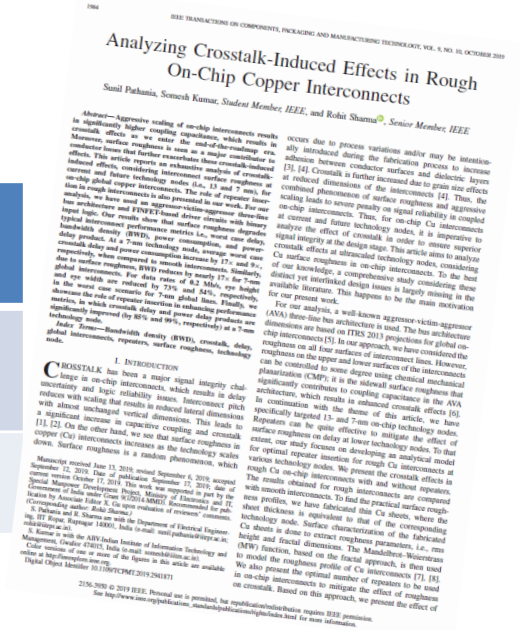
Input type	Aggressor	Victim	Smooth	Rough
Out of phase	1 -> 0	0 -> 1	38 ns	47.22 ns
In phase	1 -> 0	1 -> 0	3.04 ns	3.8 ns

13nm

Input type	Aggressor	Victim	Smooth	Rough
Out of phase	1 -> 0	0 -> 1	185.7 ns	3593 ns
In phase	1 -> 0	1 -> 0	11.03 ns	220 ns

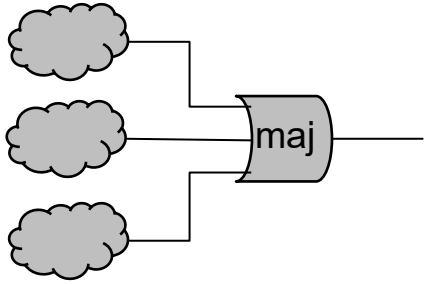
7nm

Crosstalk delay


Analyzing Crosstalk-Induced Effects in Rough On-Chip Copper Interconnects

Hardware Dependability

- Growing complexity to improve single thread instruction throughput



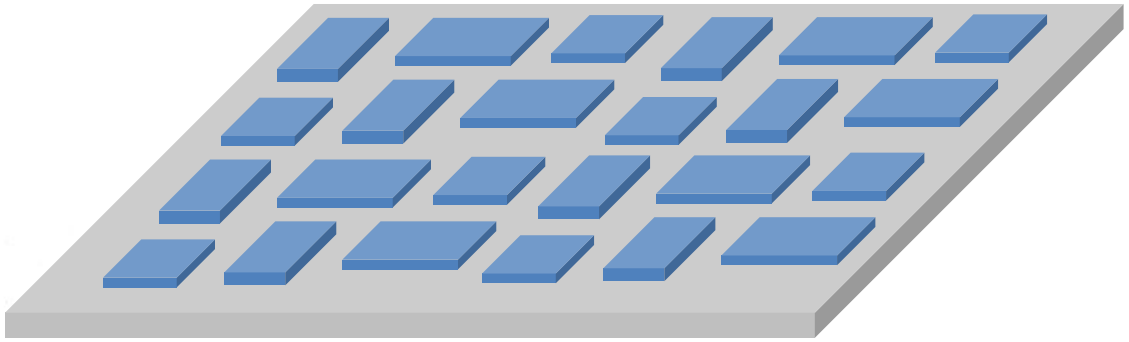
- Large part of complexity due to speculation
  => Transient execution attacks

Dür, Függer, Steininger, *Generation of a fault-tolerant clock through redundant crystal oscillators*

- Crosstalk => Side channels

- Individual transistor reliability drops

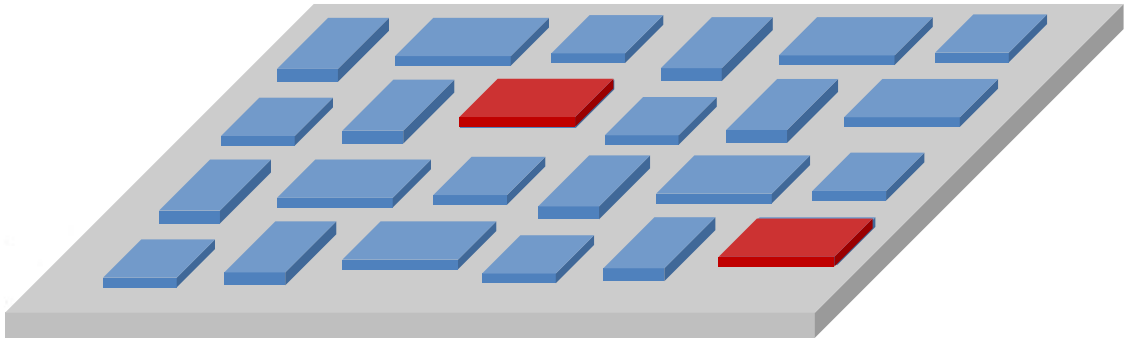
Chiplets to Counter Decreasing Yield



Trusted Execution Environments

NOT: whatever crap I put inside becomes trustworthy

Chiplets to Counter Decreasing Yield



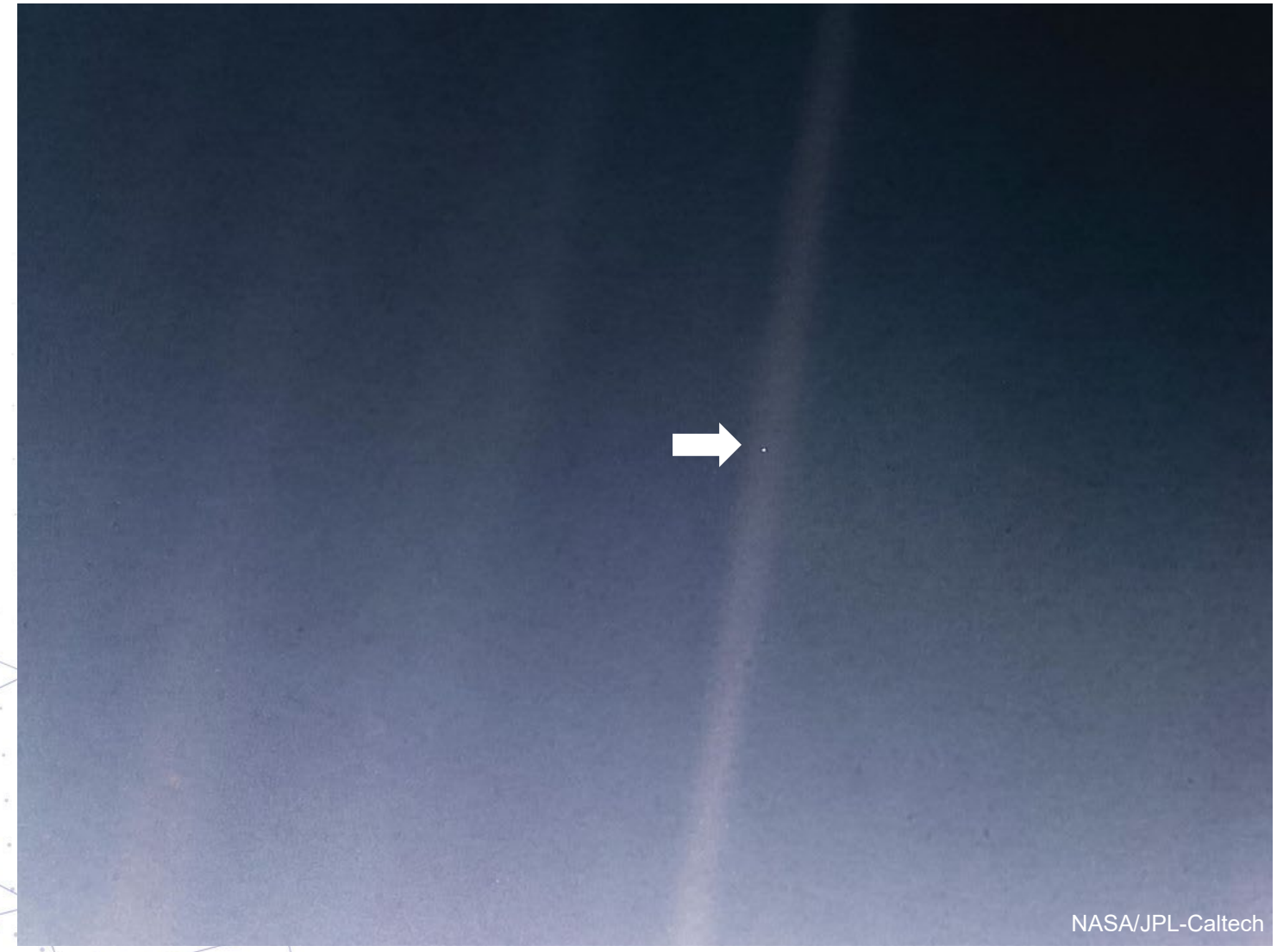
Trusted Execution Environments

Trusted so that whatever runs inside, it **cannot** be **interfere**d with from what is **outside** as far as ***integrity*** and ***confidentiality*** are concerned

availability, dependability, …

Why: same core? / same chiplet ?

Pale Blue Dot



Insights and Questions

- Multicore / Manycore / *PUs / … **are** distributed systems on a chip
- Hardware people will continue to provide us the illusion of **digital fault-free systems**, at significantly increasing costs
- Isolation (e.g., as required to implement TEEs or fault containment domains) becomes increasingly difficult within the same core.

➢ What should be the granularity at which we implement fault and intrusion tolerance and resilience in the future? (node, chiplet, core, …)

➢ How can fixed function trusted components help reduce the trust in cores and the software they run?

➢ How can we build systems that survive up to **49** years on earth, without requiring replacement, while still contributing to tomorrow‘s workload

References

- P. Goupil et al. **AIRBUS state of the art and practices on FDI and FTC in flight control system**
  https://www.sciencedirect.com/science/article/pii/S096706611000270 4
- **Infineon Aurix TC4x**
  https://www.infineon.com/assets/row/public/documents/10/156/infineon-tc4x-overview-productpresentation-en.pdf
- **Autoware**
  https://tier4.github.io/autoware-documentation/latest/
- **Intel Lion Cove Microarchitecture**
  https://chipsandcheese.com/p/lion-cove-intels-p-core-roars
- Dür, Függer, Steininger, ***Generation of a fault-tolerant clock through redundant crystal oscillators***
  https://www.sciencedirect.com/science/article/pii/S002627142100054 8
- ***Pale Blue Dot*** – *Nasa / JPL-Caltech*
  https://en.wikipedia.org/wiki/Pale_Blue_Dot#/media/File:PIA23645-Earth-PaleBlueDot-6Bkm-Voyager1-orig19900214-upd20200212.jpg