



SNT

Interdisciplinary Centre
for Security, Reliability
and Trust

*Rethinking dependability
from ground up*

Marcus Völz



Rethinking Dependability from Ground Up



A380



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



Secondary: DSP Sharc (40 MHz)



Redundancy and Diversity



AurixTM TC4x

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

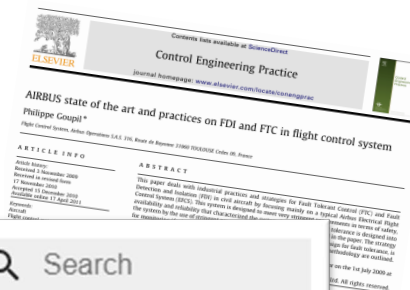
<https://www.infineon.com/assets/row/public/documents/10/156/infineon-tc4x-overview-productpresentation-en.pdf>

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

Rethinking Dependability from Ground Up



Primary: Power PC755 (66 MHz → 98 MHz)



Autoware Documentation latest ▾

Introduction Installation Tutorials How to guides Design Reference HW Contributing Datasets Support Competitions

Installation

Autoware

Docker installation

Source installation

Related tools

Additional settings for developers

Minimum hardware requirements

- CPU with 8 cores (amd64)
- 16GB RAM
- [Optional] NVIDIA GPU (4GB RAM)

Although GPU is not required to run basic functionality, it is mandatory to enable the following neural network related functions:

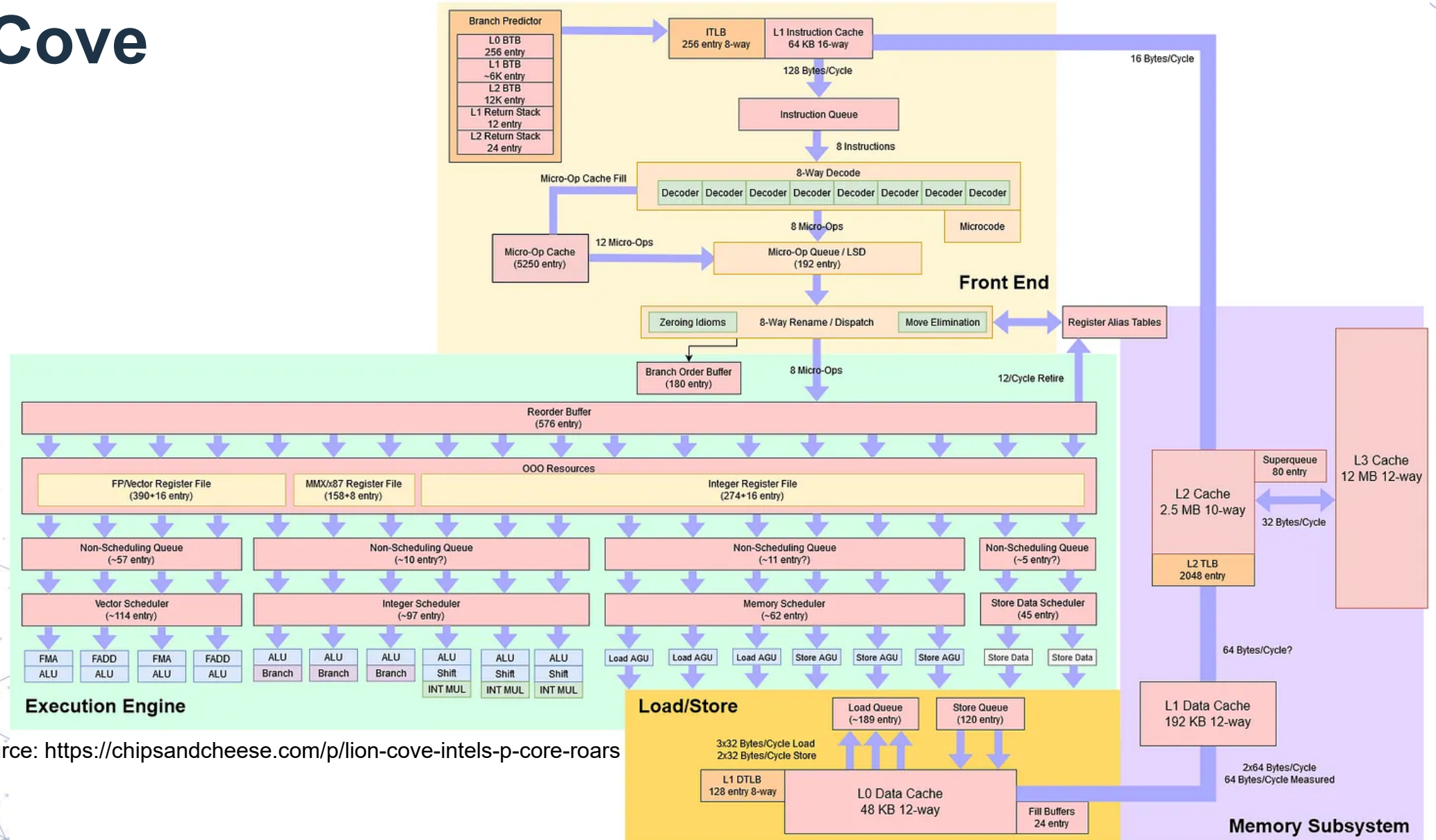
- LiDAR based object detection
- Camera based object detection
- Traffic light detection and classification

- Up to 24MB NVM

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

Lion Cove

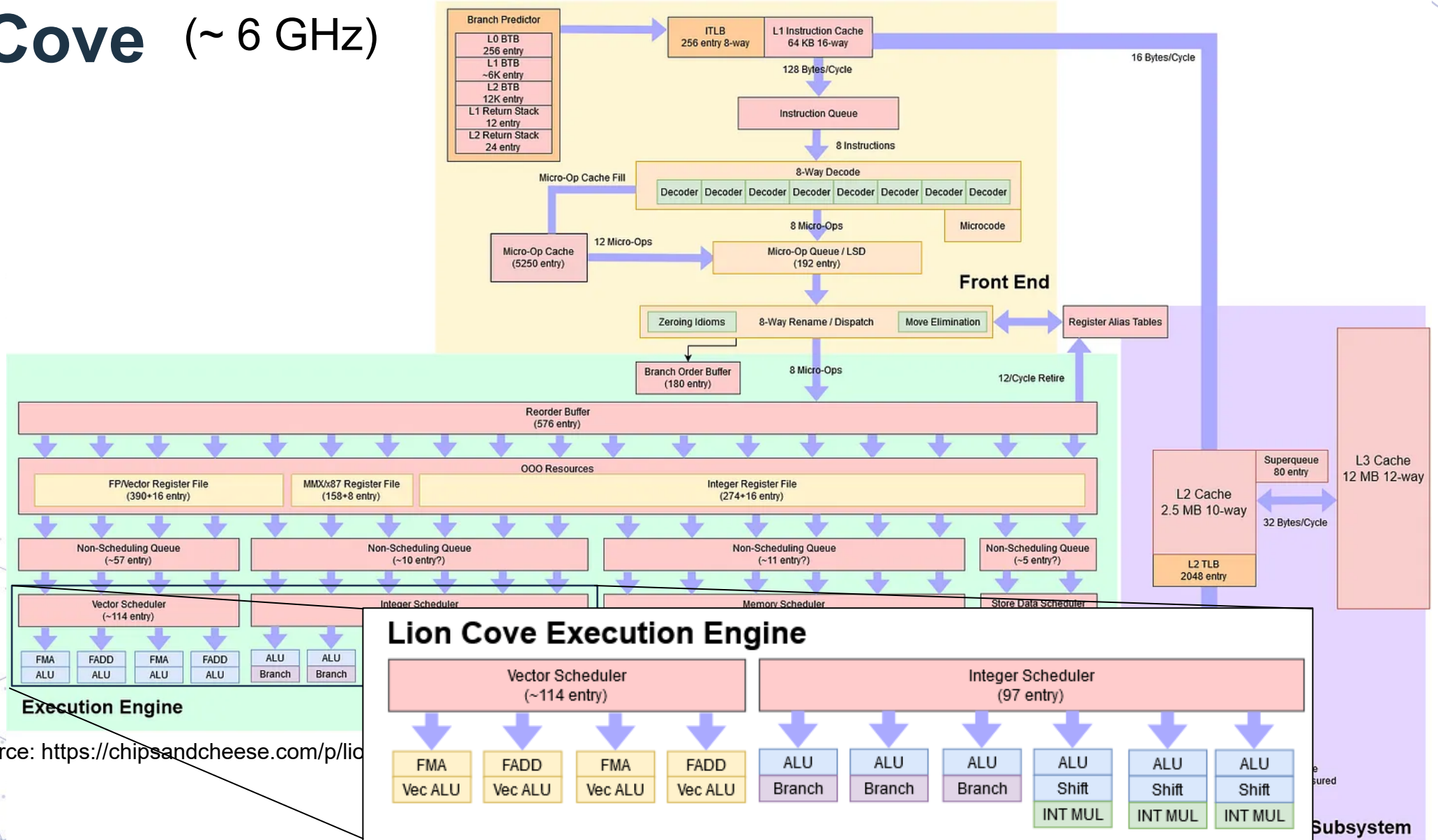
Lion Cove
Diagram By Clamchowder



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

Lion Cove (~ 6 GHz)

Lion Cove
Diagram By Clamchowder

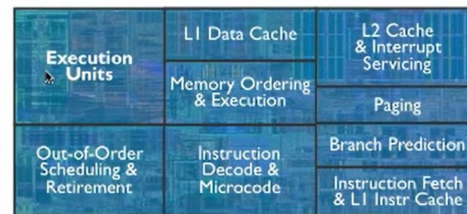
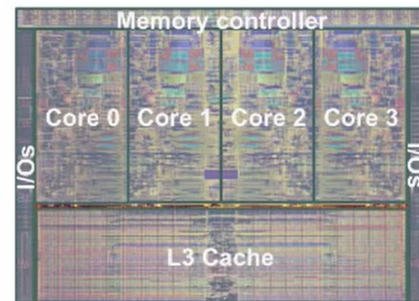


Source: <https://chipsandcheese.com/p/lic>

Chris Terman

Putting it all together: Intel Core i7 (Nehalem)

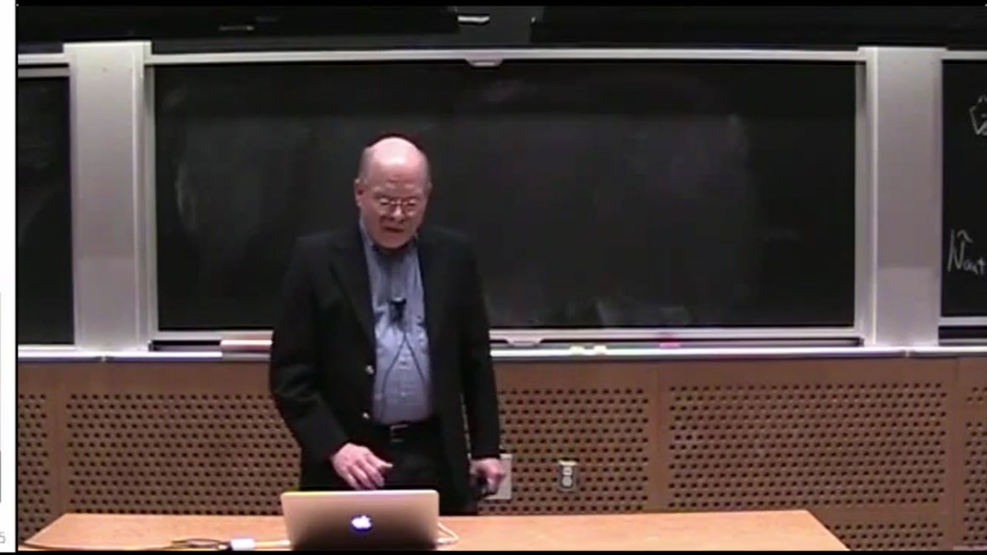
- 4 cores/chip, 2 threads/core
- 16 pipeline stages, ~3GHz
- 4-wide superscalar
- Out of order execution
- 2-level branch predictors
- Caches:
 - L1: 32KB I + 32KB D
 - L2: 256KB
 - L3: 8MB, shared
- Huge overheads vs simple, energy-optimized cores!



■ Beta

L18: Parallel Processing, Slide #15

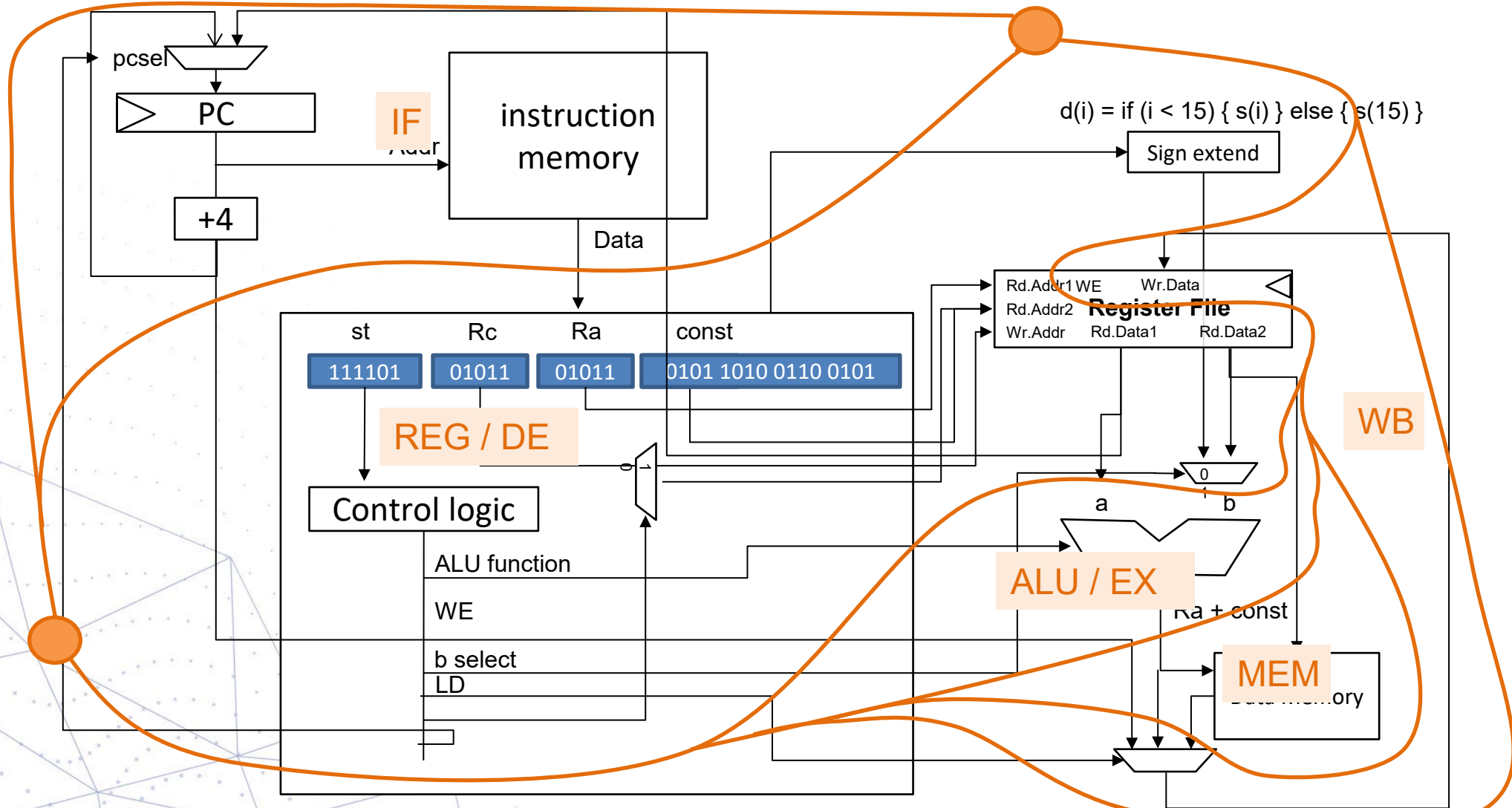
6.004 Spring 2015
L18: Parallel Processing



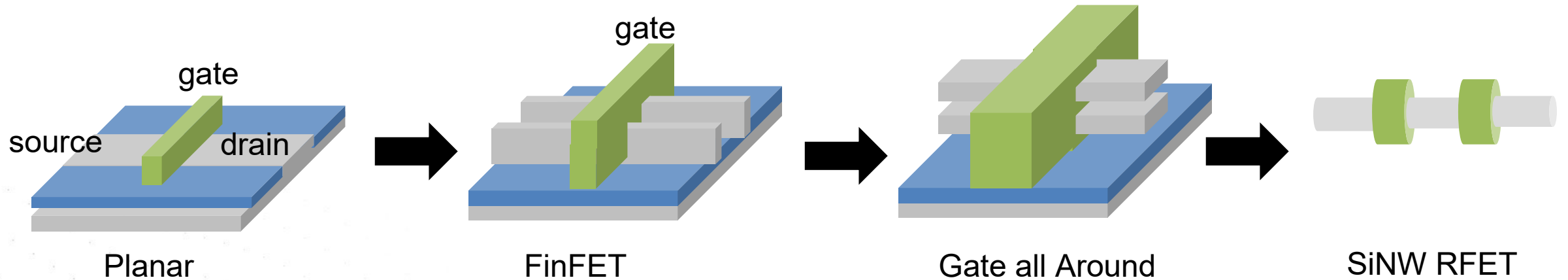
Playlist of 2017 course:

<https://www.youtube.com/watch?v=R0tFDXBZvKI&list=PLUI4u3cNGP62WVs95MNq3dQBqY2vGOtQ2>

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	Input type	Aggressor	Victim	Smooth	Rough
Out of phase	1 -> 0	0 -> 1	38 ns	47.22 ns	Out of phase	1 -> 0	0 -> 1	185.7 ns	3593 ns
In phase	1 -> 0	1 -> 0	3.04 ns	3.8 ns	In phase	1 -> 0	1 -> 0	11.03 ns	220 ns

13nm

Crosstalk delay

7nm

IEEE TRANSACTIONS ON COMPONENTS, PACKAGING AND MANUFACTURING TECHNOLOGY, VOL. 8, NO. 10, OCTOBER 2018

Sunil Pathania, Sameesh Kumar, Student Member, IEEE, and Rohit Sharma, Senior Member, IEEE

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

Abstract—Aggressive scaling of on-chip interconnects results in significantly higher coupling capacitance, which results in crosstalk effects. In this paper, we analyze the crosstalk effects in conductor lines that further exacerbate these crosstalk-induced effects. This article reports an extensive analysis of crosstalk-induced effects, considering interconnect surface roughness at current and future technology nodes (i.e., 13 and 7 nm), for analyzing global copper interconnects. The role of roughness in the architecture and FEM/CFEM based simulation is also analyzed. Our results show that surface roughness degrades delay product. At a 7-nm technology node, average worst case delay product is degraded by 17% and 8%, respectively, when compared to smooth interconnects. Similarly, global interconnects, FEM/CFEM based simulation, delay and eye width are reduced by 23% and 14%, respectively, in the worst case scenario for 7-nm global lines. Finally, we show that the role of repeater insertion in reducing performance degradation is improved by 8% and 9%, respectively, at a 7-nm node.

Index Terms—Bandwidth density (BWD), crosstalk, delay, global interconnects, repeater, surface roughness, technology node.

INTRODUCTION

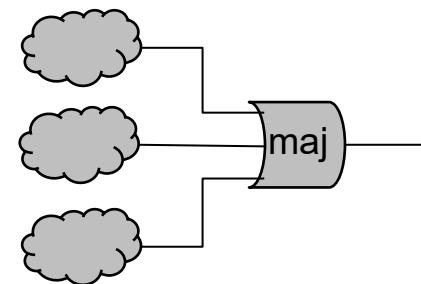
CROSSTALK has been a major signal integrity challenge in on-chip interconnects, which results in delay uncertainty and logic reliability issues. Interconnect pitch reduction with scaling that results in reduced lateral dimensions with almost unchanged vertical dimensions. This leads to a significant increase in capacitive coupling and crosstalk [1], [2]. On the other hand, we see that surface roughness in copper (Cu) interconnects increases as the technology scales down. Surface roughness is a random phenomenon, which is significantly higher during the fabrication process to increase adhesion between conductor surfaces and dielectric layers [3], [4]. Crosstalk is further increased due to grain size effects at reduced dimensions of the interconnects [4]. Thus, the combined phenomenon of surface roughness and aggressive scaling leads to severe penalty on signal reliability in coupled on-chip interconnects. Thus, for on-chip Cu interconnects at current and future technology nodes, it is imperative to study the effect of crosstalk in order to ensure superior signal integrity at the design stage. This article aims to analyze crosstalk effects at ultracalled technology nodes, considering distinct yet interrelated design issues in large mixing in Cu surface roughness in on-chip interconnects. To the best of our knowledge, a comprehensive study considering these two available literatures. This happens to be the main motivation for our present work.

For our analysis, a well-known aggressor-victim-aggressor (AVA) three-line bus architecture is used. The bus architecture chip interconnects (SI) in our approach, we have considered the roughness on all four surfaces of interconnect lines. However, crosstalk can be controlled to some degree using chemical mechanical polishing (CMP); it is the sidewall surface roughness that significantly contributes to the crosstalk effects in the AVA architecture with the theme of this article, we have specifically targeted 13 and 7-nm on-chip technology nodes. Repeater can be quite effective to mitigate the effect of crosstalk in on-chip interconnects. To that end, we have various technology nodes for rough Cu analytical model on rough Cu on-chip interconnects with and without repeaters. The results obtained for rough interconnects are compared with smooth interconnects. To find the practical surface roughness profile, we have fabricated this Cu interconnect with about thickness is equivalent to that of the corresponding technology node. Surface characterization of the fabricated Cu interconnect is done to extract roughness parameters (i.e., rms height and fractal dimension). The Mandelbrot-Wornatzen (MW) function, based on the fractal approach, is used to model the roughness profile of Cu interconnects [7], [8]. We also present the optimal number of repeaters to be used on on-chip interconnects to mitigate the effect of crosstalk. Based on this approach, we present the effect of

2156-3994 © 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Hardware Dependability

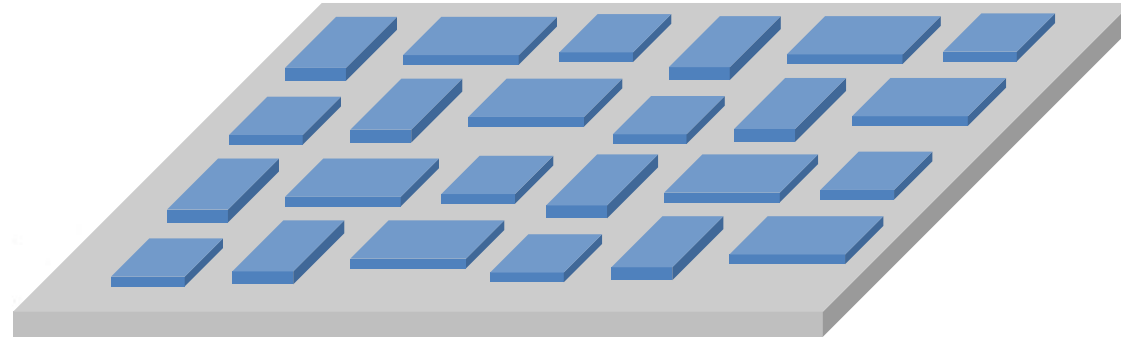
- Growing complexity to improve single thread instruction throughput
- Large part of complexity due to speculation
=> Transient execution attacks
- Crosstalk => Side channels
- Individual transistor reliability drops



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



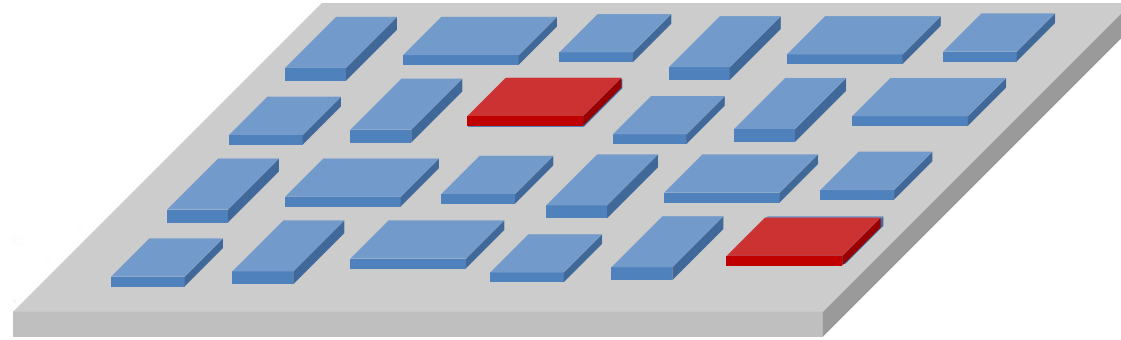
Chipllets to Counter Decreasing Yield



Trusted Execution Environments

~~NOT: whatever crap I put inside becomes trustworthy~~

Chipllets to Counter Decreasing Yield



Trusted Execution Environments

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

availability, dependability, ...

Why: same core? / same chipllet ?

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/S0967066110002704>
- **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/S0026271421000548>
- **Pale Blue Dot** – Nasa / JPL-Caltech
https://en.wikipedia.org/wiki/Pale_Blue_Dot#/media/File:PIA23645-Earth-PaleBlueDot-6Bkm-Voyager1-orig19900214-upd20200212.jpg