SAFETY-CRITICAL HETEROGENEOUS COMPUTING FOR AEROSPACE

JUAN VALVERDE
PRINCIPAL INVESTIGATOR EMBEDDED SYSTEMS

EMBEDDED SYSTEMS
UTRC-IRELAND
JANUARY 2020

United Technologies Research Center

UNITED TECHNOLOGIES CORPORATION

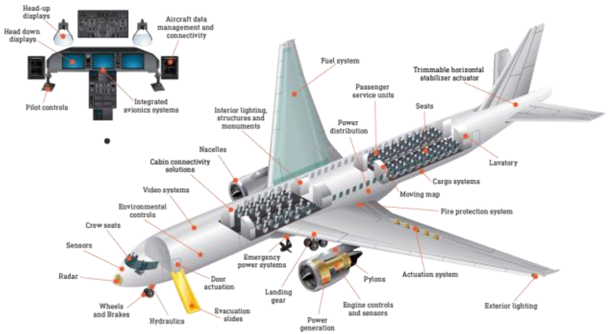
AEROSPACE PORTFOLIO

United Technologies

Collins Aerospace
A United Technologies Company

NET SALES $23 BILLION*

* 2017 pro-forma



United Technologies Research Center

Collins Aerospace

Pratt & Whitney
A United Technologies Company

NET SALES $16.2 BILLION

DOUBLE DIGIT REDUCTION IN FUEL CONSUMPTION

UP TO 75% REDUCTION IN NOISE FOOTPRINT

UP TO 50% REDUCTION IN NO_x EMISSIONS FROM CAEP/6

AIRCRAFT:
Airbus A320NEO
Airbus A220
Embraer E-Jets
Mitsubishi MRJ
Irkut MC21

PRATT & WHITNEY GTF

Global Research

>600 Employees

89% Advanced Degrees

United Technologies Research Center

United Technologies Research Centre, Ireland
Established in 2010, included capabilities in Controls, Decision Support, Networks & Embedded Systems, System Modelling & Optimization, Power Electronics, and System Analysis & Assurance

Berkeley, CA
Established in 2009, focuses on cyber physical systems and embedded intelligence

East Hartford, CT
Founded in 1929, focuses on a broad range of system engineering, thermal, fluid, material, and informational sciences

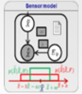
United Technologies Research Centre, Italy
Joined UTC in 2012, focuses on model-based design and embedded systems engineering.

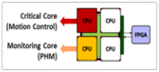
UTRC IRELAND

EUROPEAN HUB

Networks & Embedded Systems

- Hardware embedded systems
- IoT and communications systems
- Software systems
- Sensor technologies
- Autonomous systems



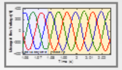



Control & Decision Support

- Model-based control design
- Optimization-based control
- Decentralized / distributed control
- Data analytics / machine learning
- Data- and physics-based diagnostics
- Computer vision

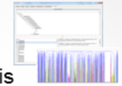
Power Electronics

- EMI modelling and filter design
- Power converter hardware design
- Distributed electrical systems
- Motor drives and converter controls
- HiL, Rapid control prototyping



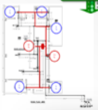

System Analysis & Assurance

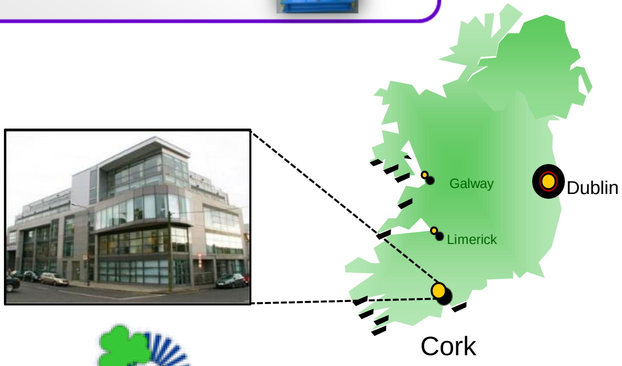
- SW/HW Cyber-security
- Formal analysis and Verification
- Model based design of CPS
- Cyber-Physical Systems analysis and Co-simulation


System Modeling & Optimization

- Aircraft systems modeling
- Building systems modeling
- Design Exploration and Optimization
- Thermal modeling and simulation
- Constraint programming and discrete optimization

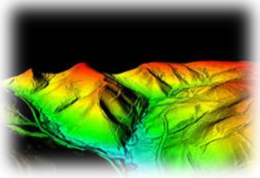
SAFETY CRITICAL APPLICATIONS AT UTC

UTC IS ONE OF THE LARGEST SUPPLIERS OF AEROSPACE SYSTEMS

- Safety-of-life operation is a critical technology differentiator in UTC.
- From Avionics to Engine PHM, Embedded Systems are a critical part of our products.

e.g. Vehicle Management Computer for rotorcraft, fixed-wing and UAS

- Will feature triple multi-core processors, high-speed communications and open architecture for use in high-redundancy flight critical applications.
- Higher processing capability will enable fly-by-wire and autonomous flight.



e.g. Situational awareness for autonomous operations

- Heavy use of image processing and sensor fusion for 3D environment reconstruction, obstacle detection, etc.
- More autonomy, more criticality!

e.g. Run-Time PHM of Engines

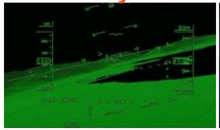
- Monitoring is critical.
- Instrumentation limited by physical constraints: space, temperature, etc.

SAFETY CRITICAL & COMPUTING INTENSIVE

COLLINS AEROSPACE

https://www.collinsaerospace.com

Vision Systems




- Head Up Displays
- Head Worn Displays
- Helmet mount Displays
- Enhanced Vision Systems
- Synthetic Vision Systems
- Combined Vision Systems

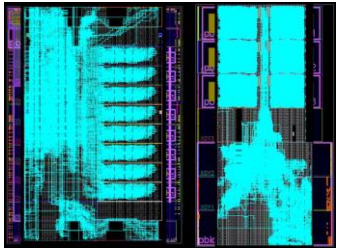
Flight & Mission Controls


- Configurable FCC
- Fly-by-wire
- Auto-throttle
- Flight Control Computers
- Mission Computers
- Vehicle Management Computers

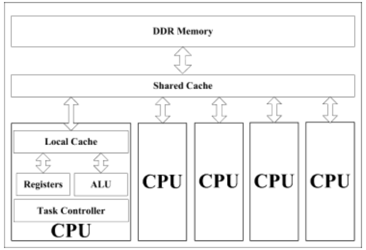
Autonomous Operations


- Auto-Pilot
- Auto-Taxiing
- Auto-Landing
- Situational awareness
- Assured AI
- UAV Modes

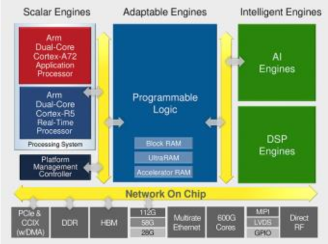
Embedded GPUs



FPGAs



Multicore Platforms



MPSoCs

United Technologies Research Center

CURRENT SOLUTIONS FOR SAFETY-CRITICAL ES

MOST SOLUTIONS ARE EITHER COTS-BASED OR DOMAIN SPECIFIC

- E.g. Vehicle Management Computer for rotorcraft, fixed-wing and UAS: 3 asymmetric commercial multicores, with different HALs.
- E.g. Motor Control Systems for actuation very frequently use dedicated Flash-based FPGAs with dedicated control architectures, redundant or not.
- E.g. Display controls include commercial GPUs and SoCs but the level of criticality is not maximum, if so, they are supported by co-processors like FPGAs.

but…

… for instance a standalone GPU performing a critical task is difficult… kernel co-scheduling?

… how do you ensure time determinism in a COTS multicore? How do you enforce it?

… how long does it take to fully design your system in an FPGA? Who does that?

… which is the best programing model for heterogeneous solutions?

… how can we decrease V&V overhead as complexity increases?

COTS

MULTICORE CERTIFICATION

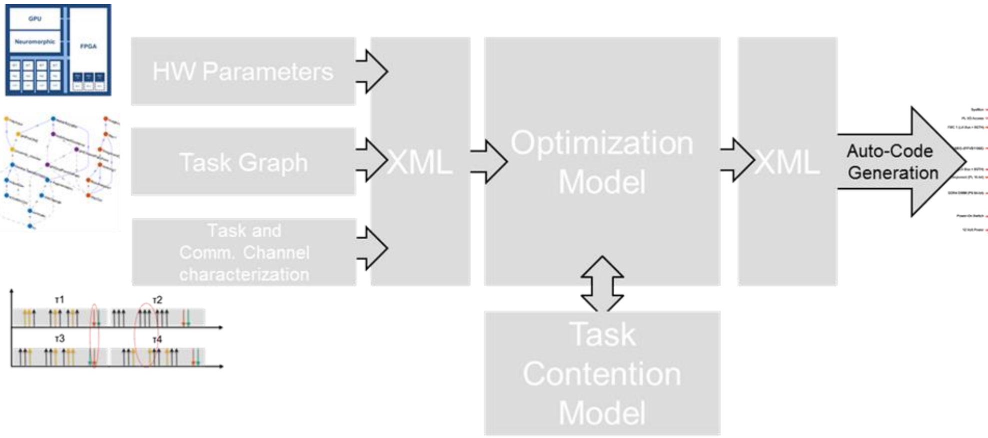
COLLINS AEROSPACE ALREADY SUBMITTED MC ARTEFACTS TO FAA

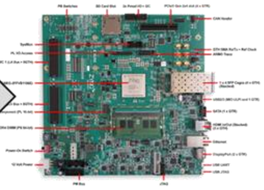
- Timing analysis to bound **WCET** is extremely **difficult**.
- **Interference analysis** is very **time consuming** and offer certification guarantees is challenging.
- **Platform Usage Domains** limit platform **performance** enormously: hyper threading, cache disabling, etc.
- **SW architectures** tend to **replicate single core** operations in multicore platforms with huge performance losses.

MASTECS

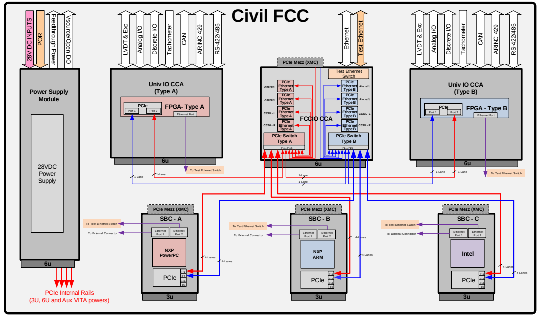
Barcelona Supercomputing Center – Centro Nacional de Supercomputación · RAPITA SYSTEMS · MARELLI · United Technologies Research Center

- Fast Track to innovation (FTI)
- **M**ulticore **A**nalysis **S**ervice and **T**ools for **E**mbedded **C**ritical **S**ystems





LYNX MOSA.ic™ · SYSGO EMBEDDING INNOVATIONS



Civil Certified Vehicle Management Computer

United Technologies Research Center

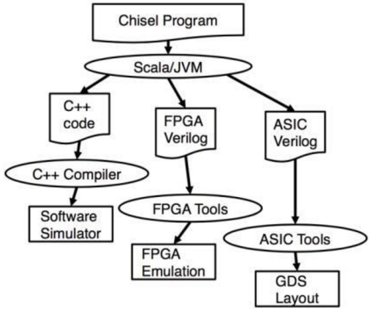
https://utcaerospacesystems.com/utc-aerospace-systems-developing-next-gen-vehicle-management-computer-to-support-autonomous-flight
https://blogs.windriver.com/wind_river_blog/2019/12/first-ascent-field-updates-from-wind-river-and-collins-aerospace/

RISC-V BASED ARCHITECTURES

Custom

ARCHITECTURES FOR SAFETY-CRITICAL DOMAINS

- **Collins Aerospace** is a **Silver** Member of the **RISC-V Foundation.**
- **Verification** from the very beginning: **Formal** specs for RISC-V (**Kami**, **Sail**, etc.)
- Specifically tailored **instruction extensions**: IO, crypto, monitors, etc.
- **Safety** and **Security** enhancements: redundancies, anomaly detectors, SCA protection, etc.
- **Reusable** building blocks.
- **Customizable Performance Counters** for full observability.

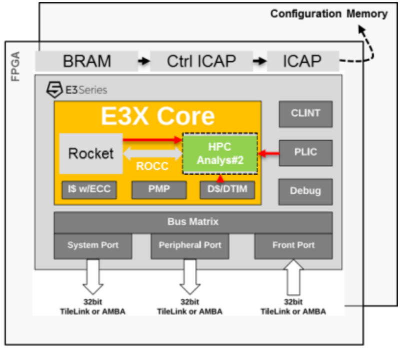


Toolchain Rocket Chip Generator and Chipyard

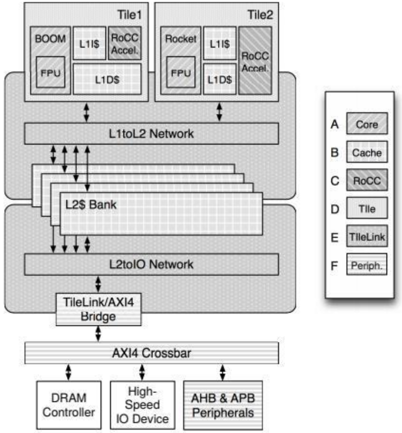
```
// app.c
Instruction #1
Instruction #2
Instruction #3
Instruction #4
Instruction #5
CUSTOMX() // returns HPC analysis
and launch reconfiguration
Instruction #6
Instruction #7
Instruction #8
CUSTOMX()
Instruction #9
Instruction #10
CUSTOMX()
```

Machine Hardware Performance Monitor Event Register	
Instruction Commit Events, mhpeventX[7:0] = 0	
Bits	**Meaning**
8	Exception taken
9	Integer load instruction retired
10	Integer store instruction retired
11	Atomic memory operation retired
12	System instruction retired
13	Integer arithmetic instruction retired
14	Conditional branch retired
15	JAL instruction retired
16	JALR instruction retired
17	Integer multiplication instruction retired
18	Integer division instruction retired
Microarchitectural Events , mhpeventX[7:0] = 1	
Bits	**Meaning**
8	Load-use interlock
9	Long-latency interlock
10	CSR read interlock
11	Instruction cache/ITIM busy
12	Data cache/DTIM busy
13	Branch direction misprediction
14	Branch/jump target misprediction
15	Pipeline flush from CSR write
16	Pipeline flush from other event
17	Integer multiplication interlock
Memory System Events, mhpeventX[7:0] = 2	
Bits	**Meaning**
8	Instruction cache miss
9	Memory-mapped I/O access

Hardware Performance Counter Registers



System Schematic



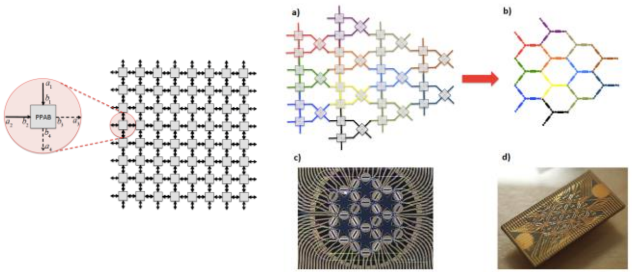
Rocket Chip Generator (Berkeley)

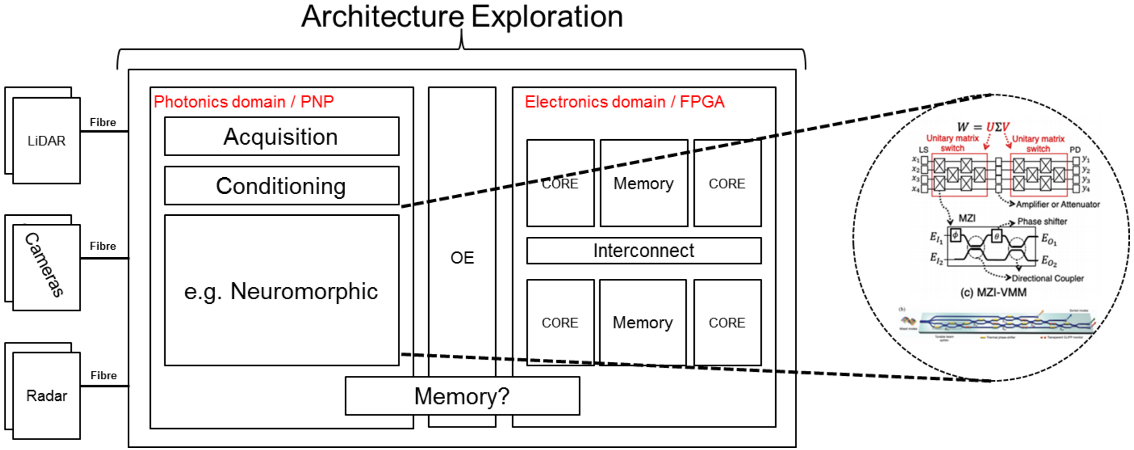
https://utcaerospacesystems.com/utc-aerospace-systems-developing-next-gen-vehicle-management-computer-to-support-autonomous-flight
https://blogs.windriver.com/wind_river_blog/2019/12/first-ascent-field-updates-from-wind-river-and-collins-aerospace/

PHOTONIC COMPUTING

TOWARDS MORE HYBRID PROCESSING ARCHITECTURES

- Prepare for **limitations in conventional electronics**. Death of Moore’s Law, etc.
- Optical **sensing** and **communications** are **already used** in commercial products, a **more computing** approach is necessary.
- Programmable Nano-Photonic Processors (**PNPs**) and Field Programmable Photonic Arrays (**FPPAs**) are already a reality.
- It is proven that photonic circuits can improve **speed** and **energy** consumption although they currently have **limitations** in terms of **scalability**.
- Execution paradigms can change if **photonic memories** or photonic links can be used to alter the **memory hierarchy limitations**.





Field-programmable photonic arrays DANIEL PÉREZ, IVANA GASULLA, AND JOSE CAPMANY

CONCLUSIONS

- **Embedded Systems** are **key** elements of most of our systems: need to **accelerate design**!
- **Certification** still very **expensive** and aerospace is very conservative.
- Aircrafts looking for more **autonomy**, require more intelligence at the edge…. but **assured intelligence**.
- More electric aircraft, fly by wire, WAIC, IMA architectures, run-time monitoring, etc. require **more and more SW for critical functionalities**.
- **COTS** or **custom** architectures?
- Complex **SoCs** are already here, but mostly relying on architectural **redundancies** to be part of critical systems.
- What is **beyond** pure **electronics**?

United Technologies Research Center

THANK YOU.

Juan Valverde
valverj@utrc.utc.com

Networks & Embedded Systems,
UTRC Ireland