Designing a Fail-operational motor controller for Space

Aloïs Wolff – 2023/03/15

Space FPGA Users Workshop, ESTEC

Presentation Outline

- How to build a Failure-Operational equipment for Space?

I. Project & Environmental constraints

II. Techniques to ensure system consistency

III. Verification & Validation

IV. Conclusion/Lessons learnt

Presentation Outline

- How to build a Failure-Operational equipment for Space?

I. **Project & Environmental constraints**

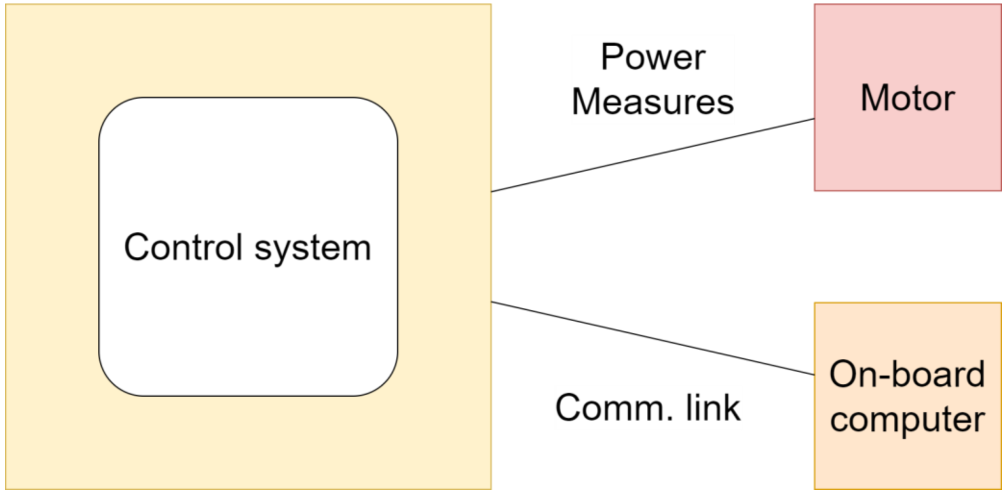
II. Techniques to ensure system consistency

III. Verification & Validation

IV. Conclusion/Lessons learnt

Project Context

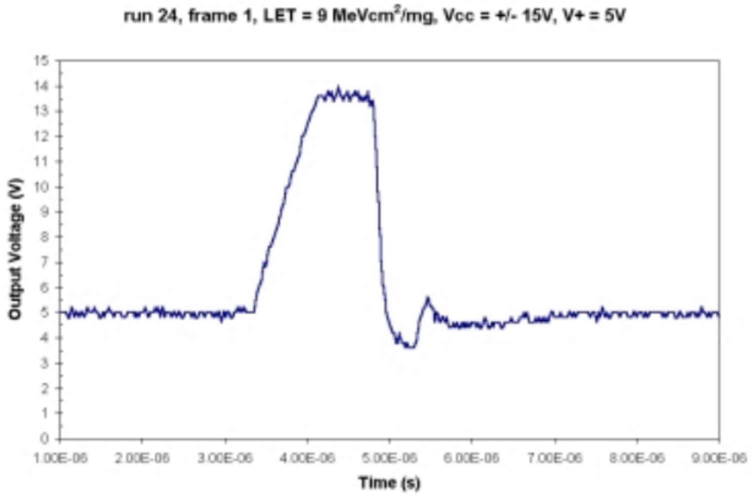
- Launcher second-stage equipment
- Fault-tolerant motor control for:
  - TVC
  - Thruster valves
  - Pumps, etc.
- Self-monitoring/Embedded FDIR

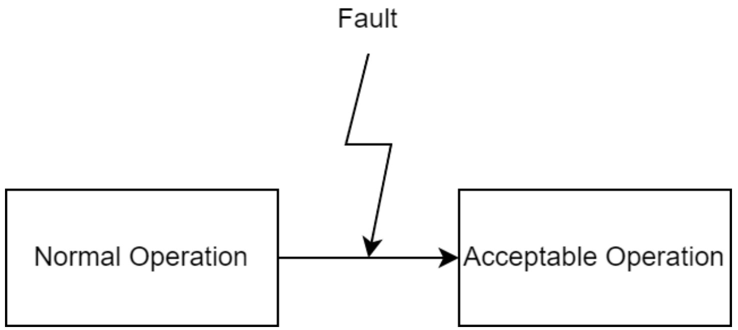


Environmental Constraints

- Launcher environment:
  - Vibrations
  - Some radiation: SEU/SETs, dose ignored
  - “Short” lifespan
  - Very high reliability
  - Vacuum (hopefully)

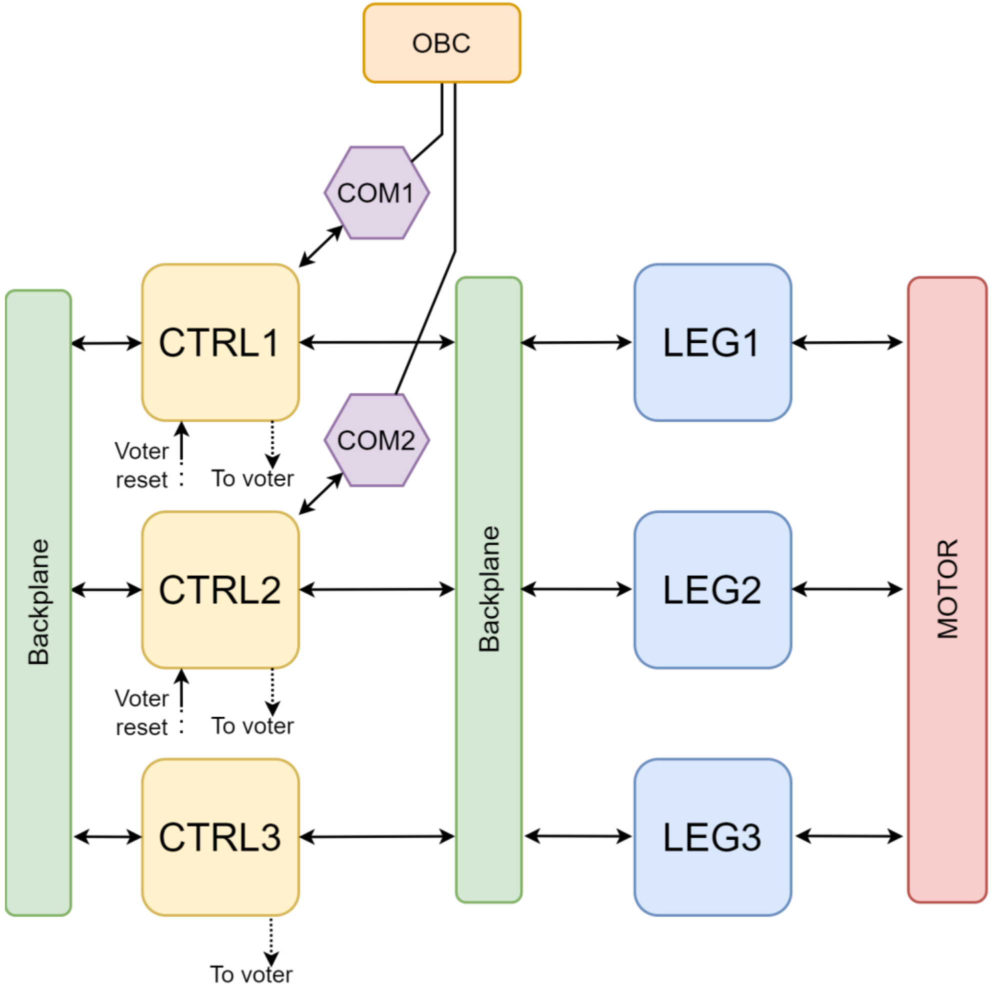
- 1-FO: Remain 1-Failure-operational
  - Graceful degradation
  - Fault detection & Isolation
  - Avoiding SPOFs
- Hard Real-time system



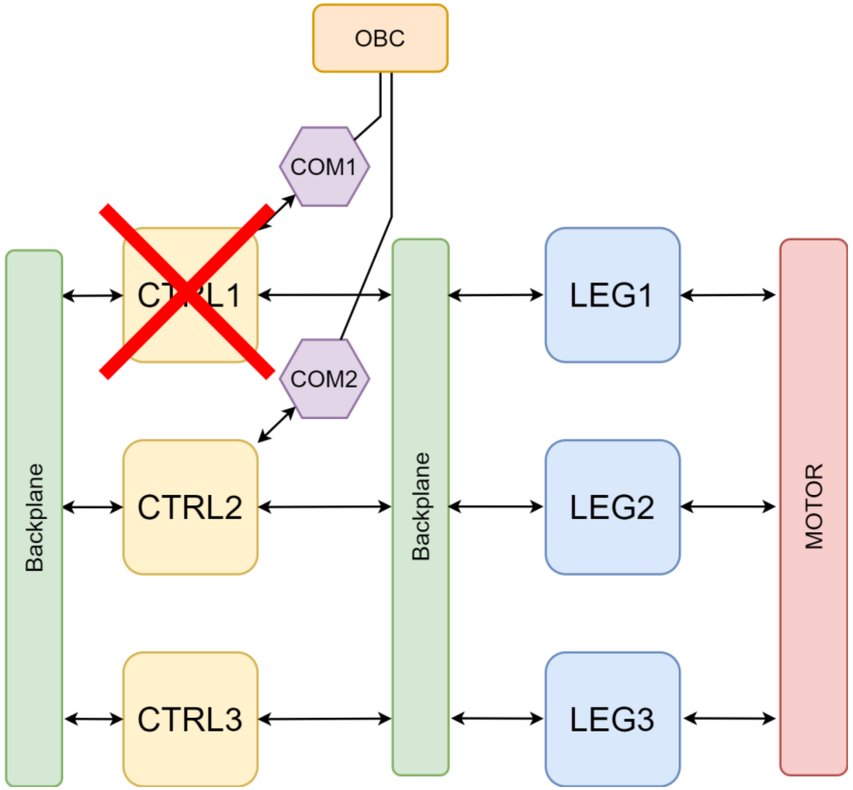


A Distributed System

- 3 Equivalent CTRLs : System-level TMR
- Not entirely symmetric: 2 players & a tie-breaker
  - 2/3 communication links
  - 2/3 motor control
  - 1 voter
- Build consensus and decide
- Failure? Reset the controller



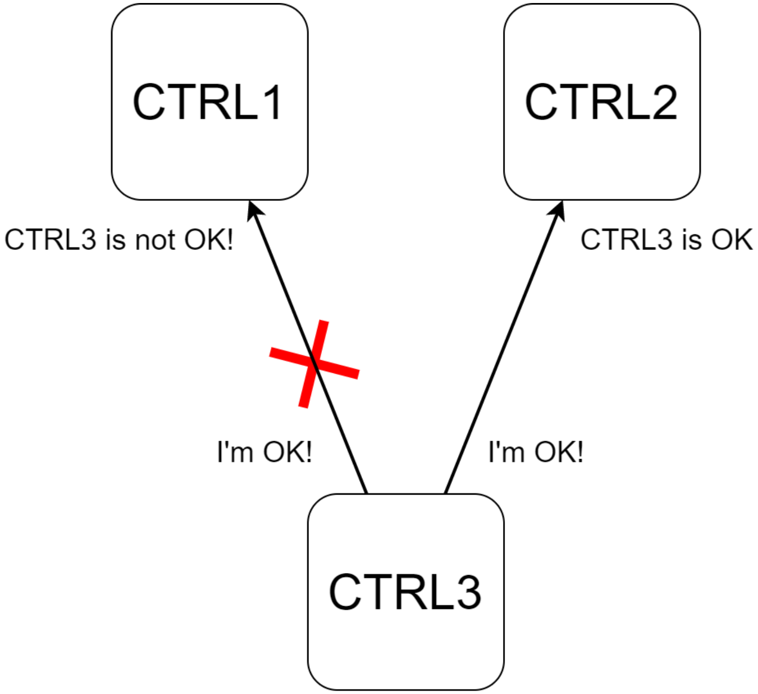
Expected Fault model



- SEUs: microtriplication & FPGA technology
- SETs:
  - input filtering on slow signals
  - error tolerance on fast signals
- Permanent failure/Already ejected
- But also…

Byzantine Generals problem

Byzantine Faults



- System must agree on **concerted strategy**
- Imperfect information on system state
- System may appear failed and not failed
- Voting law must be robust to that

Presentation Outline

- How to build a Failure-Operational equipment for Space?

I. Project & Environmental constraints

II. Techniques to ensure system consistency

III. Verification & Validation

IV. Conclusion/Lessons learnt

Presentation Outline

- How to build a Failure-Operational equipment for Space?

I. Project & Environmental constraints

II. Techniques to ensure system consistency

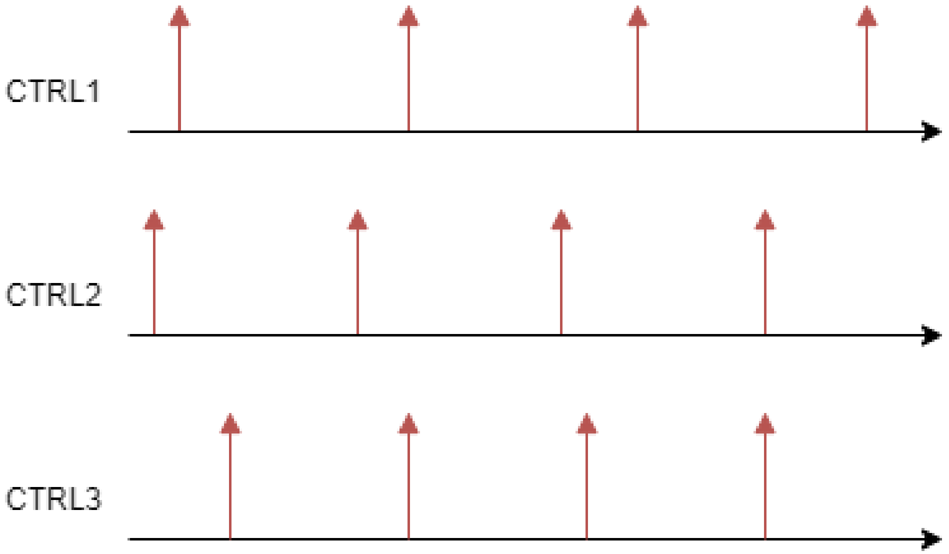
  I. Agree on a shared timebase

III. Verification & Validation

IV. Conclusion/Lessons learnt

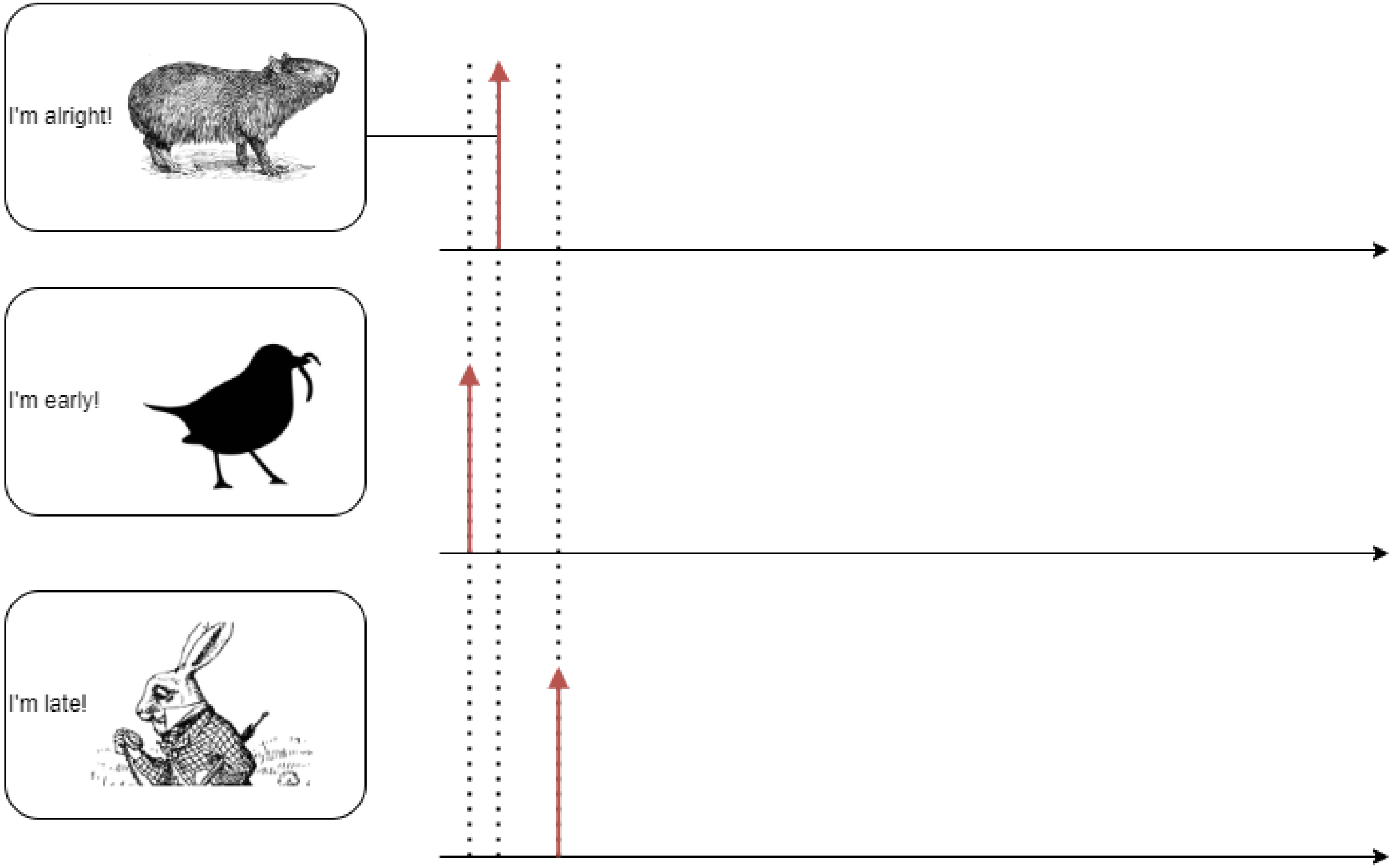
Time consensus

- 3 boards, so 3-time bases
  - Different phase
  - Different frequency (slightly)
- How can we agree on specific instants?
- How can we maintain that agreement?



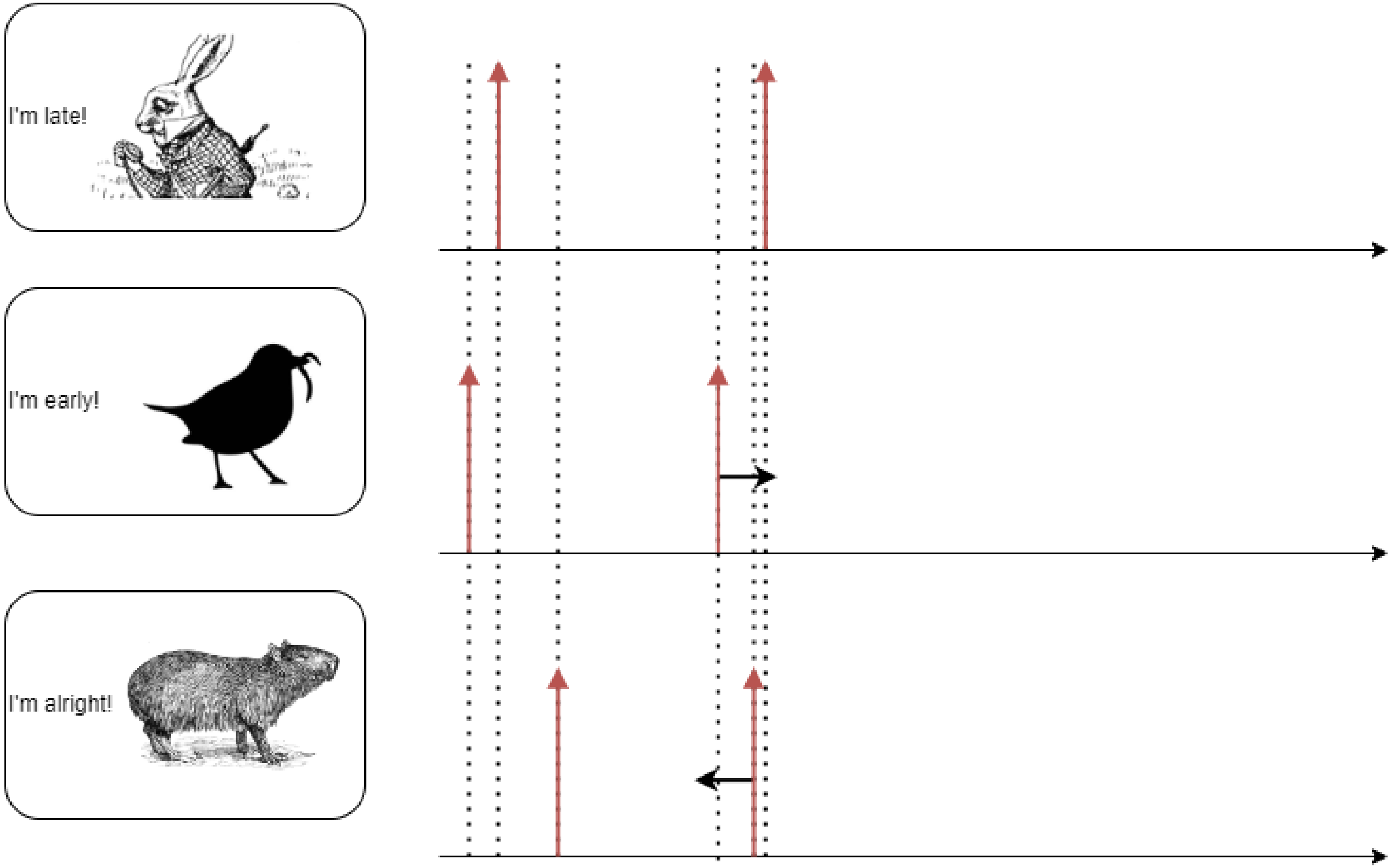
Time consensus: closed loop

- Exchange the info
- Is this likely?
- Adjust your own clock



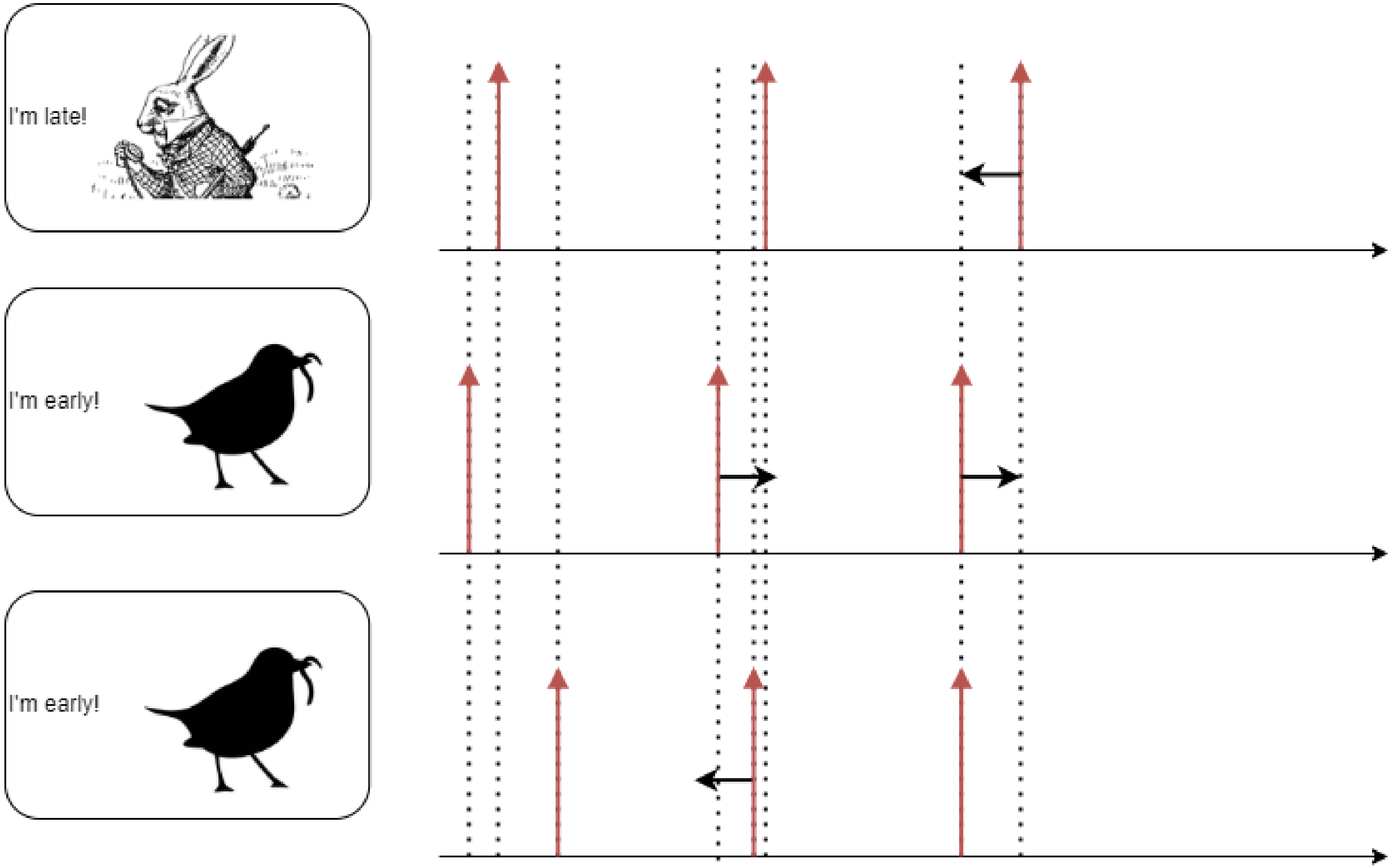
Time consensus: closed loop

- Was it enough?
- Iterate



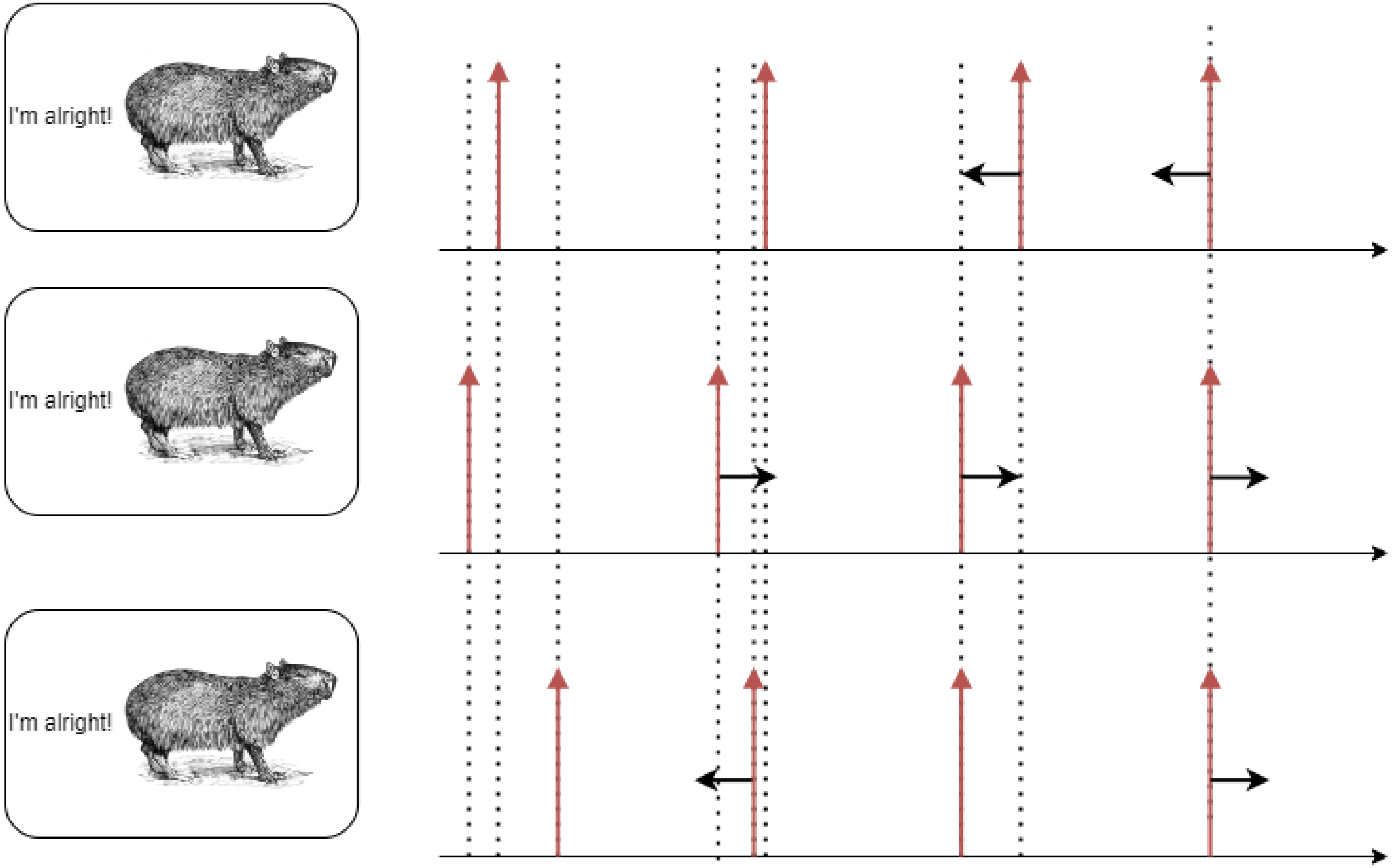
Time consensus: closed loop

- Getting to it…



Time consensus: closed loop

- Phase-locked
- Frequency compensation (in average)



Presentation Outline

- How to build a Failure-Operational equipment for Space?

I. Project & Environmental constraints

II. Techniques to ensure system consistency

   I. Agree on a shared timebase

   II. Agree on expected behaviour

III. Verification & Validation

IV. Conclusion/Lessons learnt

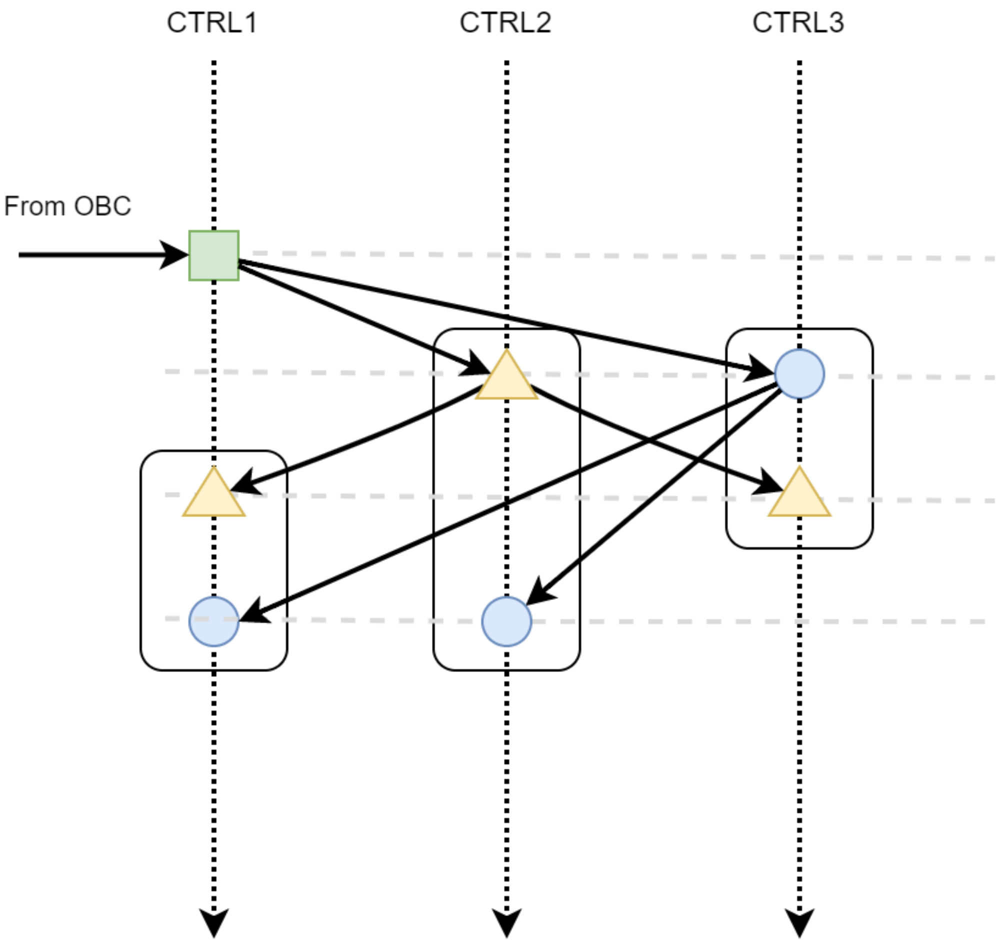
Drive: TM/TCs

- CTRL1 receives a new TC:
  - Sends it to both neighbours
  - First neighbour sends it back
  - Second does it as well

- In the end, everyone has received the info

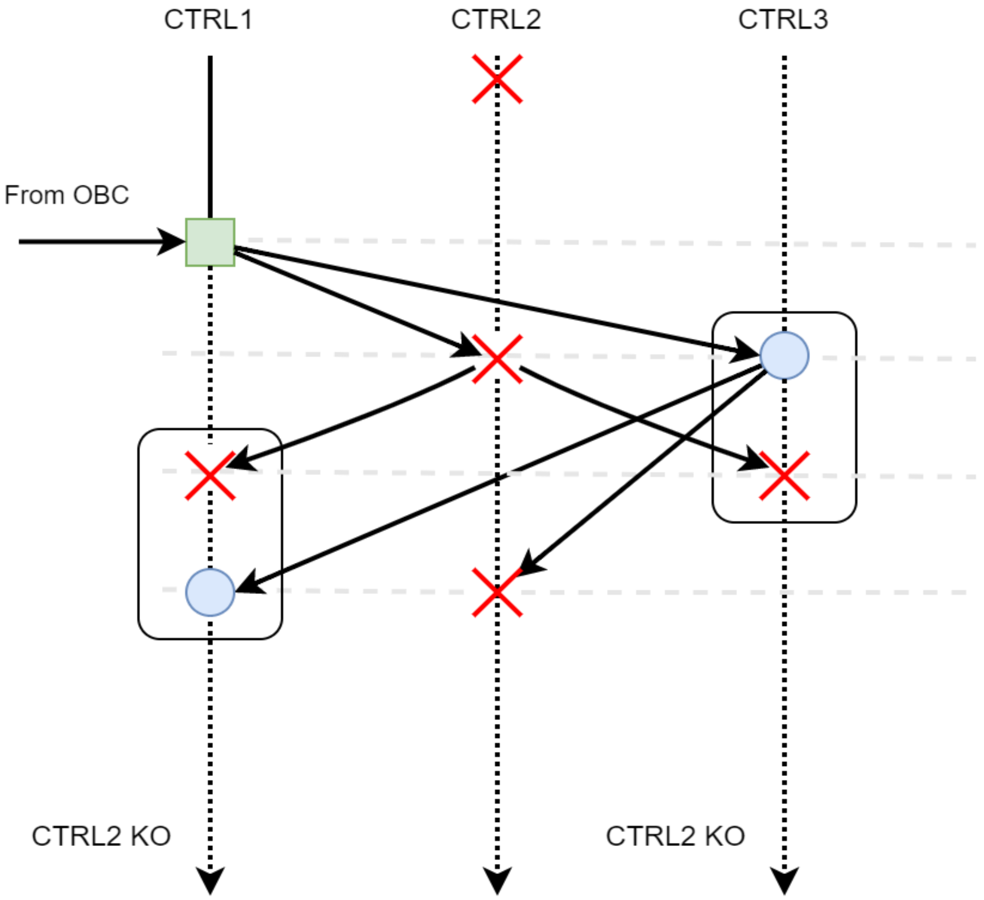
- AND everyone knows the others have received as well

- Is it robust to faults?



Powell, David & Arlat, Jean *et al.*. (1999). GUARDS: A Generic Upgradable Architecture for Real-Time Dependable Systems.. Parallel and Distributed Systems, IEEE Transactions on. 10. 580 - 599. 10.1109/71.774908.

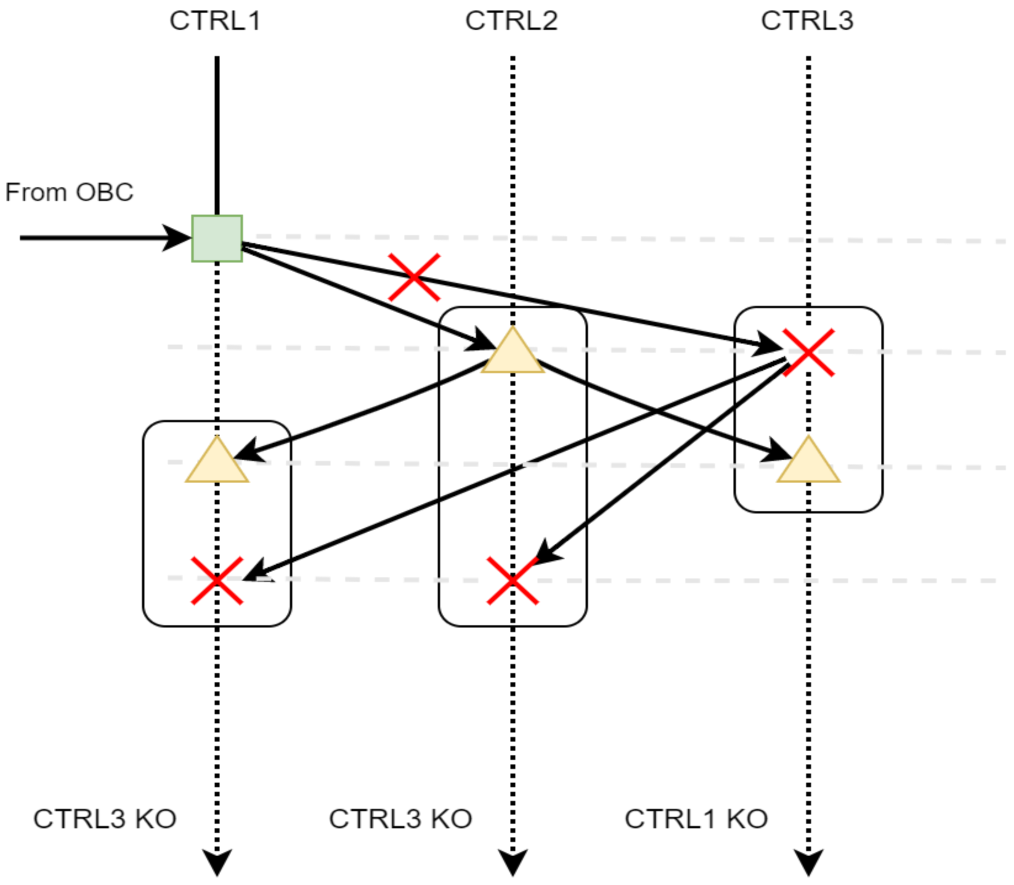
Fault 1: permanent



- What happens in the case of a permanent failure?
- Every working CTRL has a valid picture of the event
- Failure is detectable

Fault 2: spurious

- In the case of a spurious fault?
- Every CTRL has a valid picture of the event
- Failure is also detected



Presentation Outline

How to build a Failure-Operational equipment for Space?

I. Project & Environmental constraints

II. Techniques to ensure system consistency

  I. Agree on a shared timebase
  II. Agree on expected behaviour
  III. Agree on real-time closed loop operation

III. Verification & Validation

IV. Conclusion/Lessons learnt

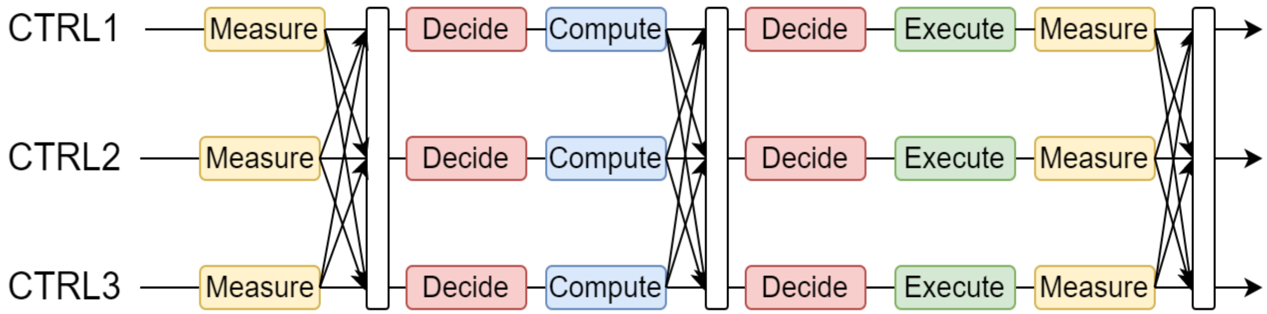
Distributed motor control cycle

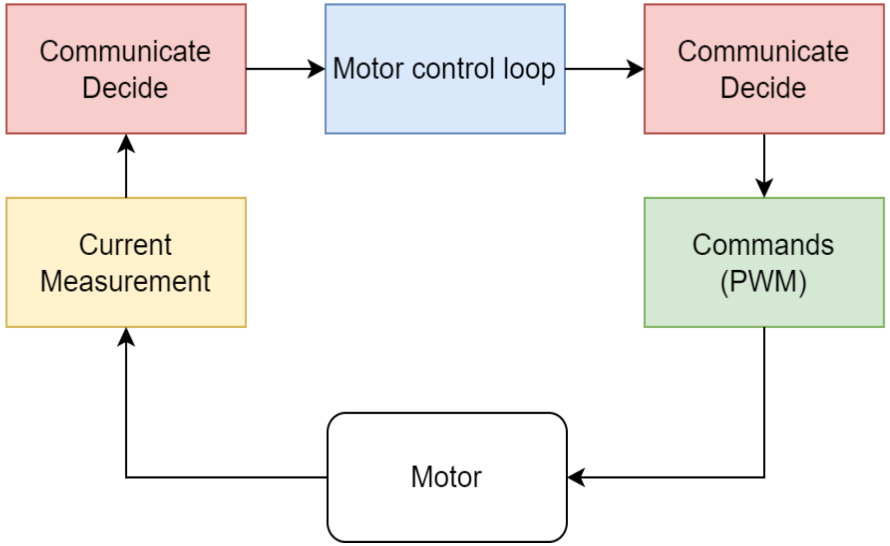
- Motor control: current loop

- Adding 2 steps: build a consensus
  - On the physical system's state
  - On the control system's state

- Communication & decision

- Algorithm is robust to the environment
  - OK with spurious faults
  - OK with permanent subsystem failures





Presentation Outline

- How to build a Failure-Operational equipment for Space?

I. Project & Environmental constraints

II. Techniques to ensure system consistency

III. Verification & Validation

IV. Conclusion/Lessons learnt

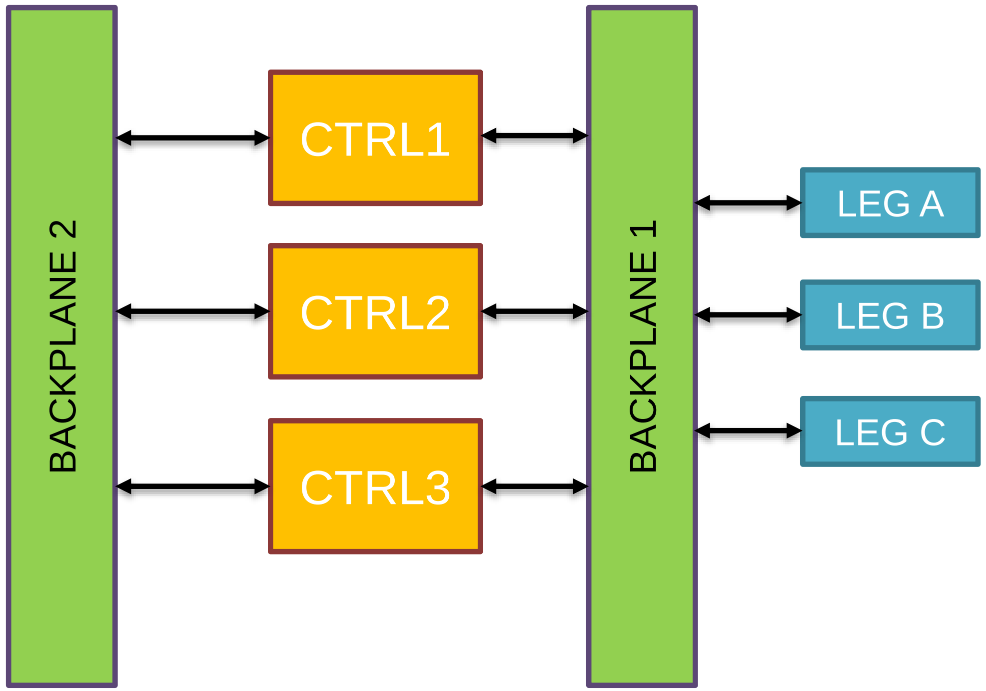
In-system Validation : CITRON

- How do you verify a fail-functional system?
  - Classical FPGA V&V : RTL simulation
  - Difficult for several FPGAs working together
  - Model-based verif. Is only as good as the model

- In-system fault injection & verification

- 3 Control Boards + several power boards
- 2 Backplane interconnect Boards

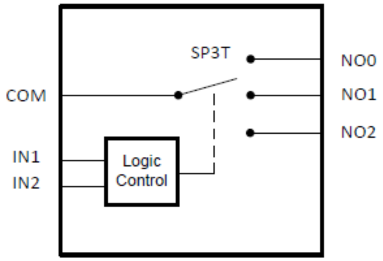
CITRON: Controller **I**n**T**e**R**b**O**ard a**N**alyzer

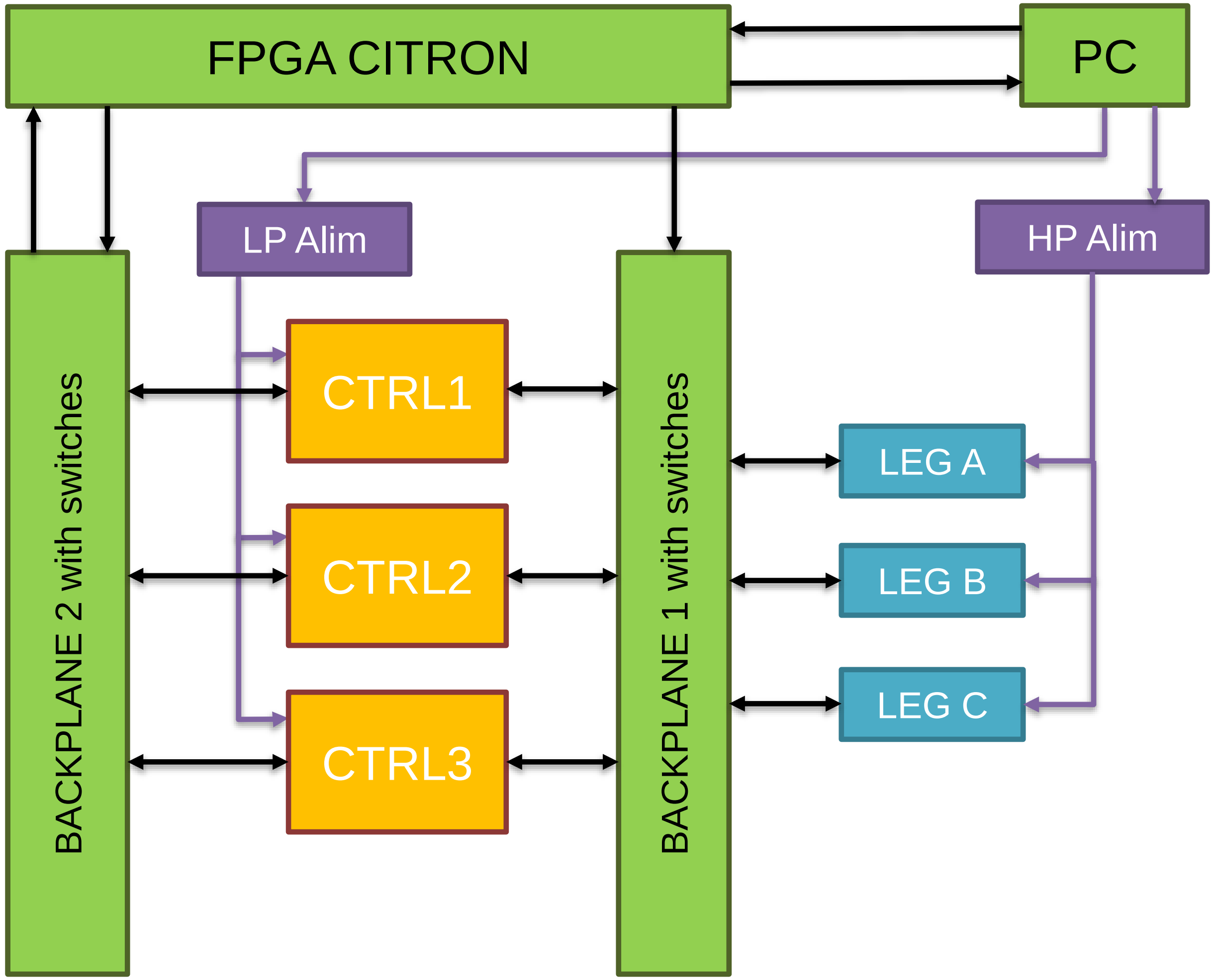


In-system Validation : CITRON

- “Intelligent backplane” including an FPGA
- Analog switches placed on data lanes
- Allows introducing disruptions:
  - force to VCC,
  - Force to GND
  - open lane
- FPGA & Power supplies controlled by PC

Simplified Schematic





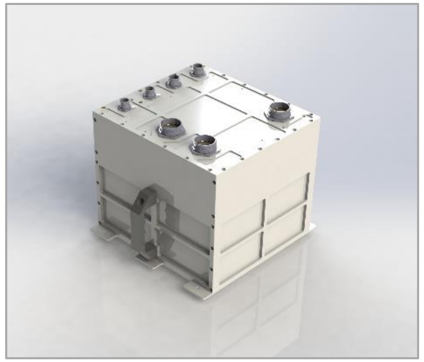
Conclusion

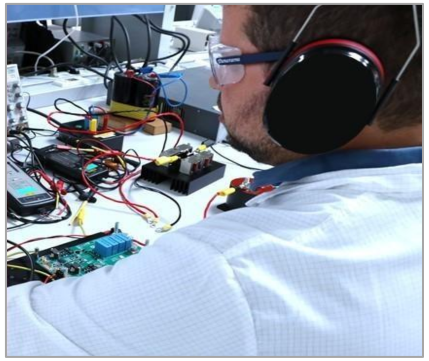
- Fault tolerance by architecture => Complex but **powerful** system
- Identify what data are part of the **system state**
- **Agree often** to avoid divergence
- Graceful degradation: faults are mostly silent
  - important to verify thoroughly
  - error injection is invaluable

Innovation Makers

Technology Bricks

Motor Controllers, Power Supplies,
Fail-Operational Controllers



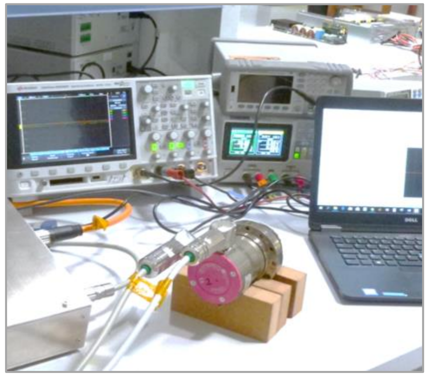


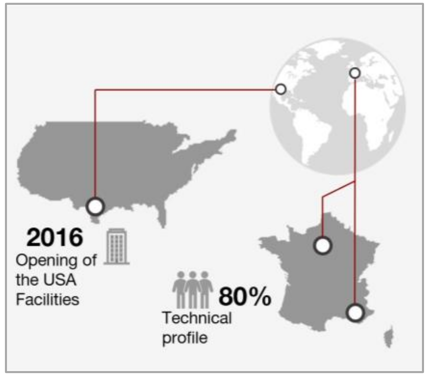
Expertise

60 Employees,
80% of Engineers & Ph.D.

Quality Management System

EN9100 to ECSS Standards
& Procedures



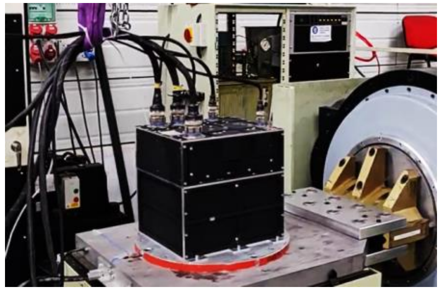


Global Footprint

Paris: R&D
Aix-en-Provence: Manufacturing
Houston: Commercial
+ Stavanger, Norway : Commercial
Privately owned and self financed

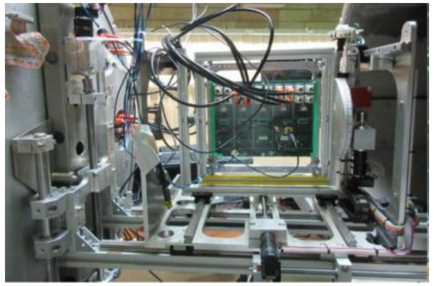
Product Lines: Aerospace, E-Mobility, Energy

Aerospace Technologies



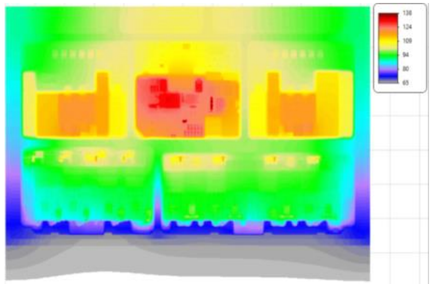
Electronics Racks for Shock & Vibration

Ruggedization to resist extreme shock and vibration levels without failure



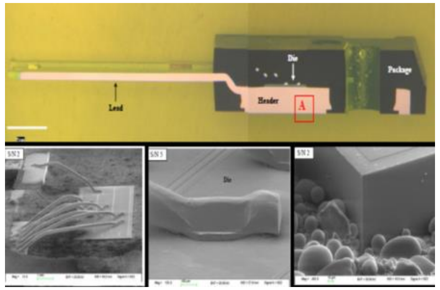
Radiation Tolerant Components & Modules

Low recurring cost with off-the-shelf components, tolerant to radiation and designed accordingly



System Thermal Management

Key aspect of converter design, thermal model and loss profiles are accurately estimate



Wide Bandgap Switches

Experience in Silicon Carbide MOSFETs integration and EMC filter design know-how

Thank You!
Any Questions?

alois.wolff [at] wattandwell.com
https://aerospace.wattandwell.com