Use of compelling safety arguments for Integrated Modular Avionics systems

George Romanski, CSTA Aircraft Computer Software

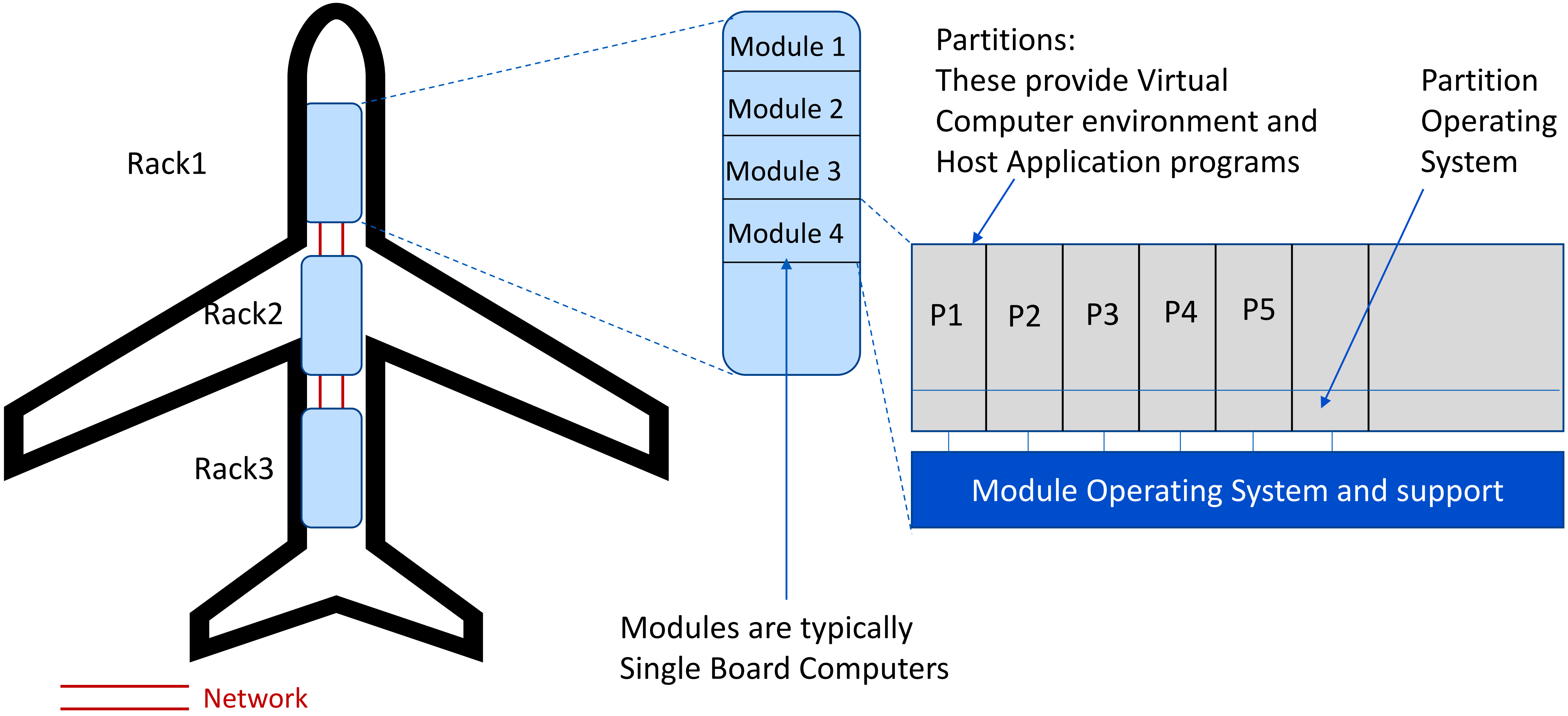
FAA

December 5, 2023

Federal Aviation Administration

STEP SENIOR TECHNICAL EXPERTS PROGRAM
ADVANCING SAFETY THROUGH SCIENCE

IMA System Organization



Partitions:
These provide Virtual Computer environment and Host Application programs

Partition Operating System

Modules are typically Single Board Computers

Robust Partitioning must be enforced and assured

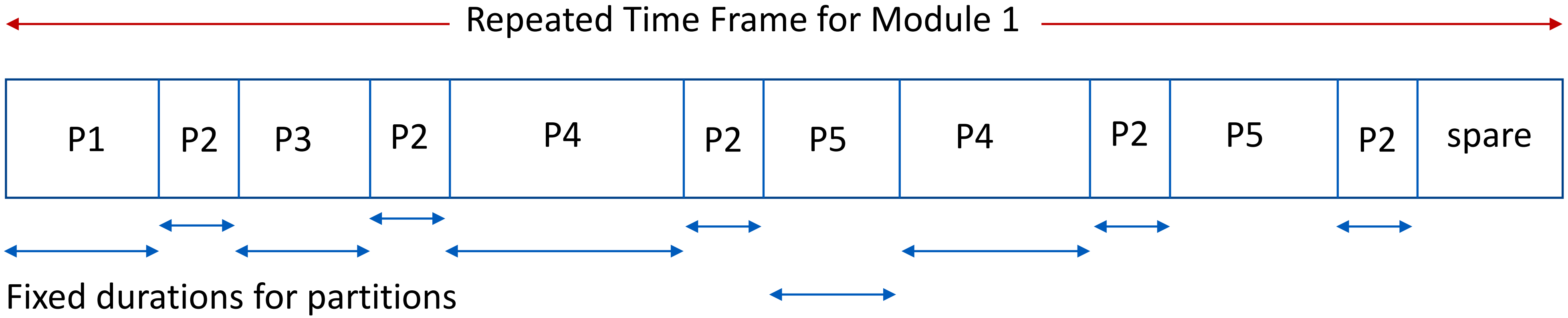
- IMA System can host many applications in Partitions
- ROBUST partitioning is Key
  - Space – one application CANNOT adversely affect any other partition or Module RTOS
  - Time – A partition cannot adversely affect the timing behavior of another partition
  - Resources – A partition cannot adversely affect shared resources
- With Robust partitioning, it is possible to host applications with mixed Design Assurance Levels
  - DAL A – may have catastrophic effects if it fails
  - DAL D – may have Minor effects if it fails
- A failure in one partition cannot affect the timing of another partition
  - Health management is partitioned – even the global health manager is pre-emptive
- The work to communicate between partitions must be performed in the partitions time
  - If P1 sends a message – the time to copy out is performed in P1's time
  - If P2 receives a message – the time to copy in is performed in p2's time

Time Scheduling

Schedule Configurations are prepared and reviewed. (as well as Space and other Resources)

Often Written as XML structured text

Translated to binary data (either using certified code, or qualified tools)



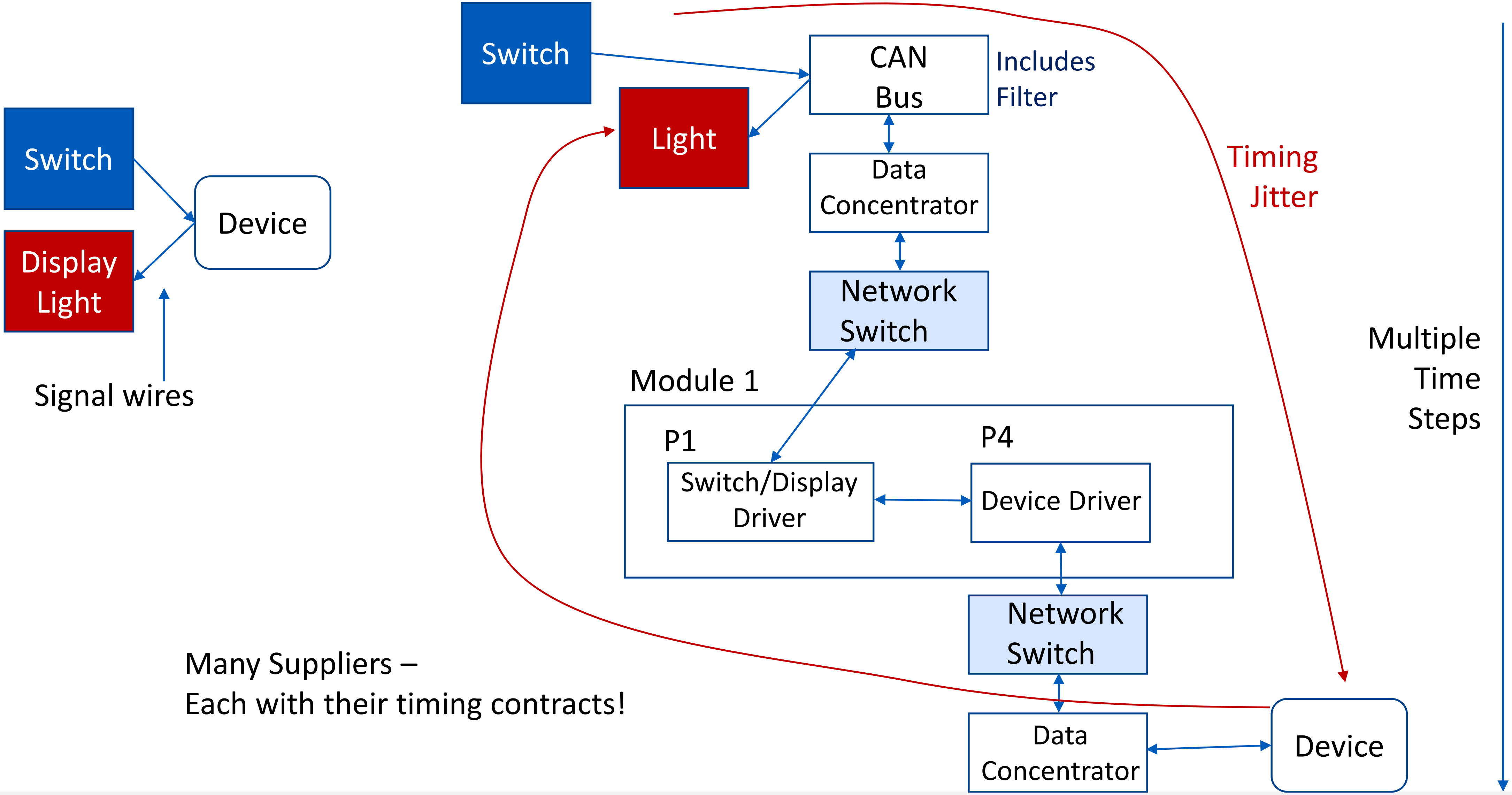
Repeated Time Frame for Module 1

P1	P2	P3	P2	P4	P2	P5	P4	P2	P5	P2	spare

Fixed durations for partitions
Some may be repeated within frame

- An application may complete within its partition schedule
- It may complete within a number of partition schedules
- Or it may run continuously

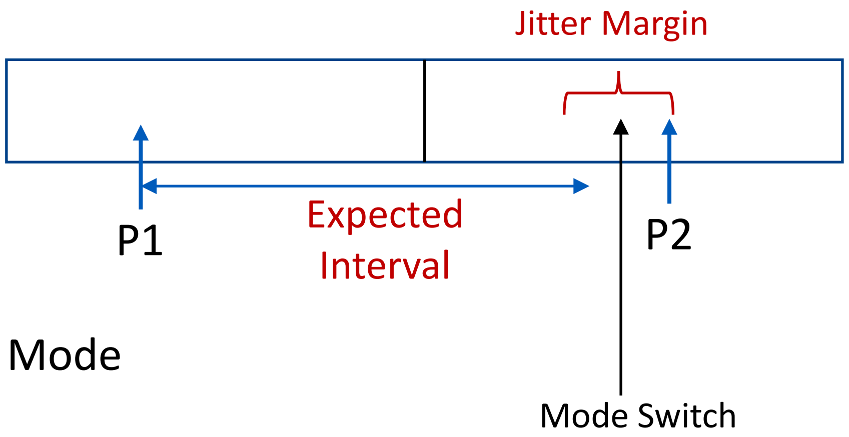
Timing Jitter due to Network



Many Suppliers –
Each with their timing contracts!

Errors due to Jitter

- Fixed Durations:
  - Position1 value when read
  - Position 2 value when read, in the next time frame
  - Time between P1 and P2 may be within the two time frames, with some jitter within frames
  - Rate of change is based on both values and the interval.
  - A mode switch within a frame may affect meaning of value

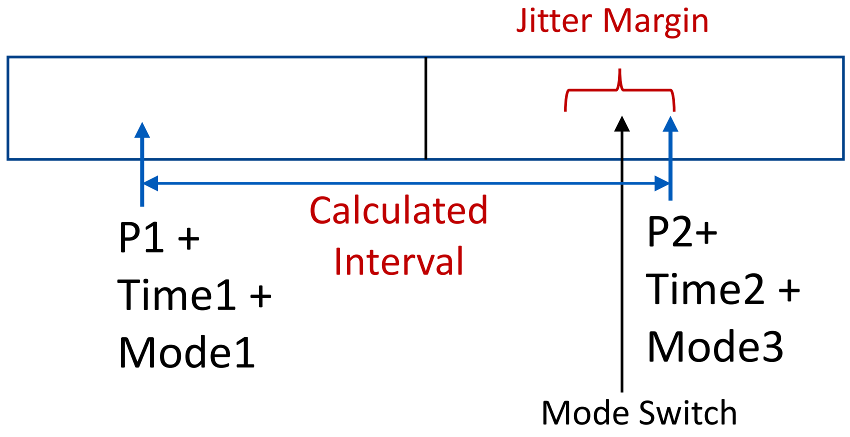


P2 may be compromised – calculated in different Mode

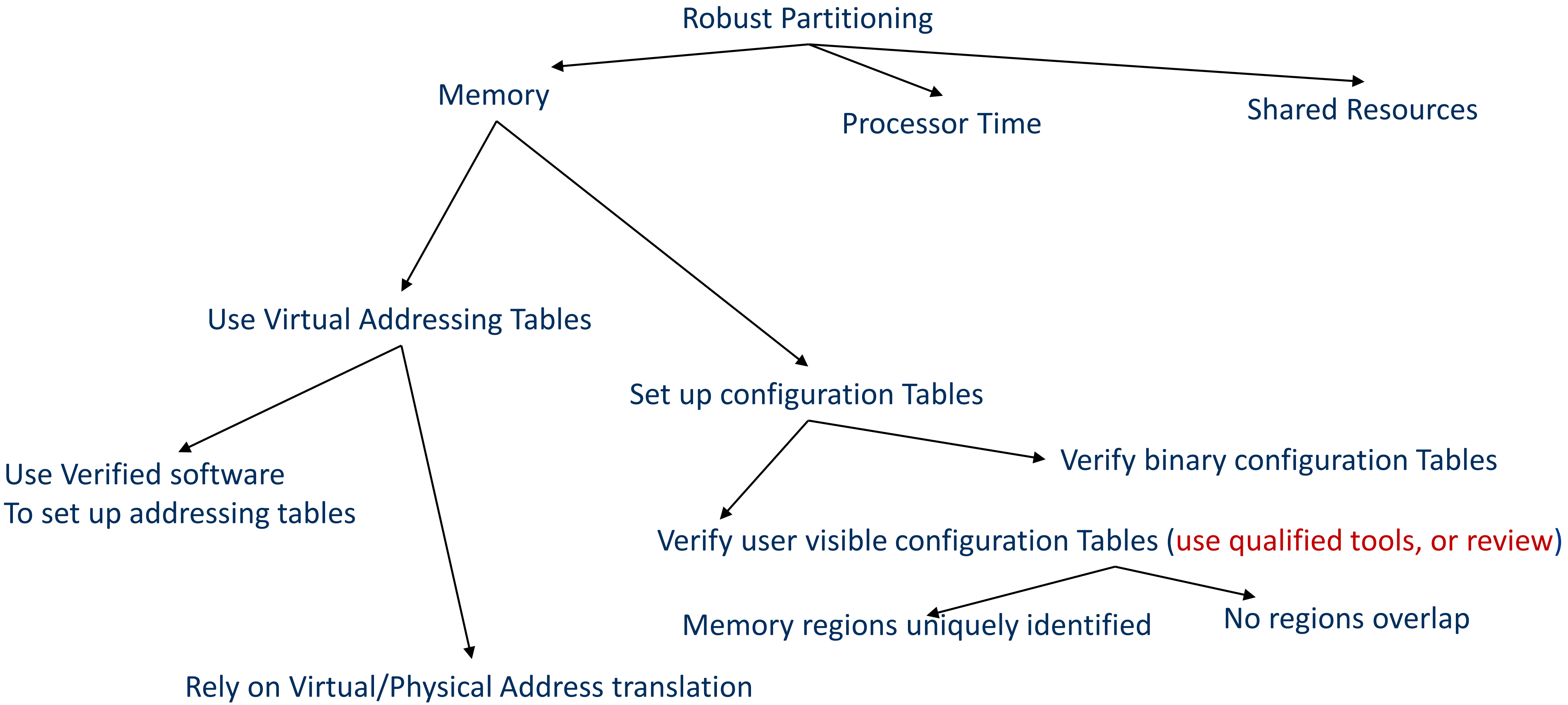
Time between P1 and P2 affect rate calculation

Jitter avoidance

- Time stamp each Position Value record
- Add Mode to Position Value record
- Discard P2 if mode switch values disagree
- Calculate rate change based on difference between time stamps



Use of Assurance Case - using Argument Structure



Robust Partitioning

Memory

Processor Time

Shared Resources

Use Virtual Addressing Tables

Set up configuration Tables

Use Verified software
To set up addressing tables

Verify binary configuration Tables

Verify user visible configuration Tables (use qualified tools, or review)

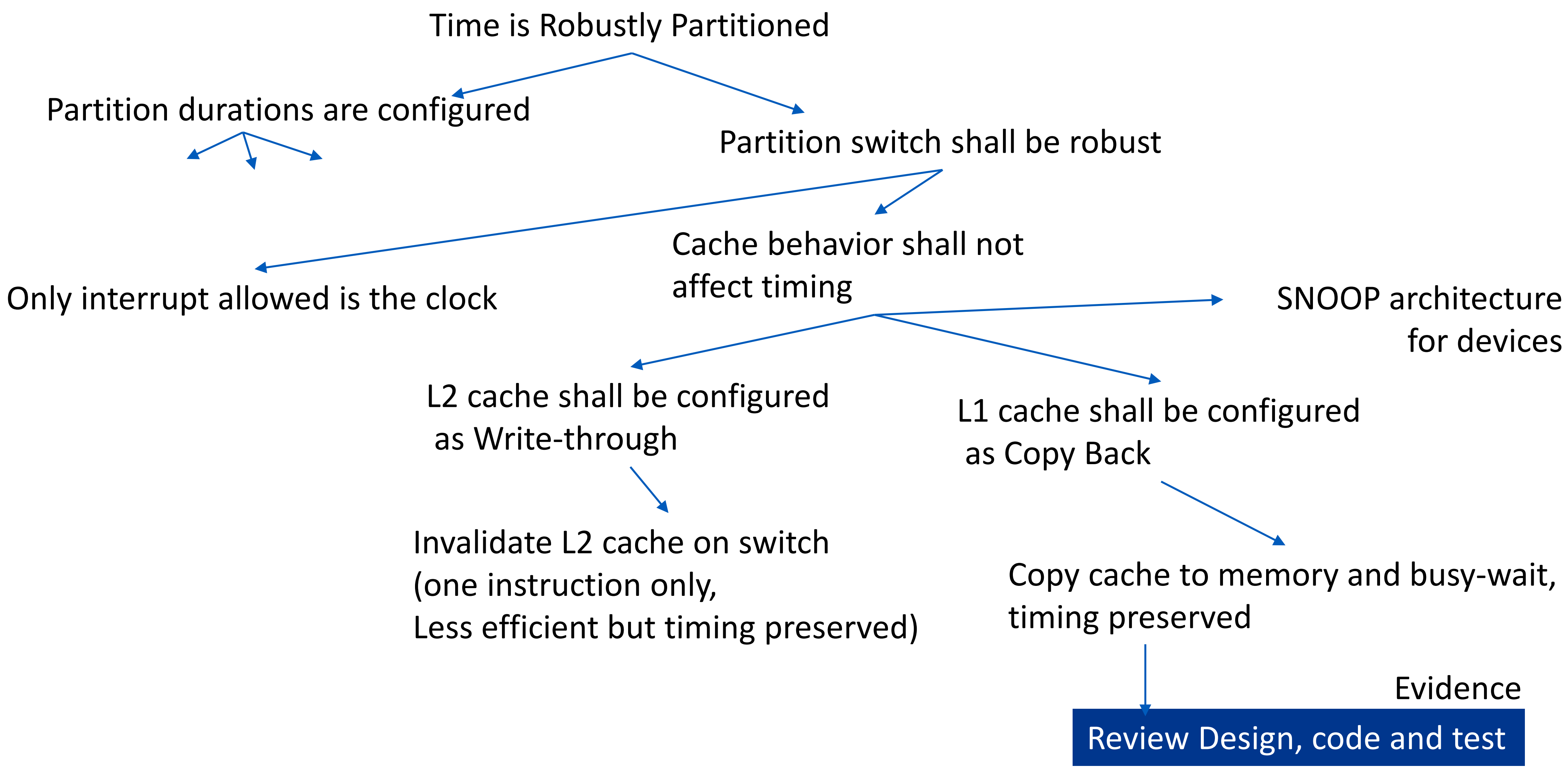
Memory regions uniquely identified

No regions overlap

Rely on Virtual/Physical Address translation

Evidence provided at the “leaf” nodes

Framework for Assurance Argument - Time



Time is Robustly Partitioned

Partition durations are configured

Partition switch shall be robust

Only interrupt allowed is the clock

Cache behavior shall not
affect timing

SNOOP architecture
for devices

L2 cache shall be configured
as Write-through

L1 cache shall be configured
as Copy Back

Invalidate L2 cache on switch
(one instruction only,
Less efficient but timing preserved)

Copy cache to memory and busy-wait,
timing preserved

Evidence

Review Design, code and test

Example: How to demonstrate Robust Partitioning?

- IMA Requirements based on Architecture of the solution
- Robust Partitioning argument
- “Negative” requirements hard to verify : for example
  - One partition **shall not** be able to access another partition’s memory
  - One partition **shall not** “steal” processor time from another partition
  - …

Prescriptive Regulations are HARD when Requirements are HARD

Use an argument instead of negative requirement!

Build an Assurance Case

Structured argument to show “Possession” of three properties

- Build Assurance Case
  - Communicates a line of reasoning which ties the ownership of the OPs to evidence
  - Should be a structured, **compelling** argument that is easy to consume
- Many notations exist
  - Goal Structuring Notation (GSN)
  - Toulmin
  - Friendly Argument Notation FAN
  - Etc.
- Structured Text proposed
  - Can be manipulated by tools
  - Can be translated to graphical forms

3 Overarching Properties

1. Intent – The *defined intended behavior* is correct and complete with respect to the desired behavior.
2. Correctness – The *implementation* is correct with respect to its *defined intended behavior*, under foreseeable operating conditions.
3. Innocuity – Any part of the *implementation* that is not required by the defined intended behavior has no *unacceptable safety impact*.

Assurance Case

An assurance case is an *argument* with its supporting artifacts. In the context of the *overarching properties*, the assurance case is intended to show how the properties are possessed by an *item* or combination of *items*.

The argument introduces, summarizes, and provides context and justification for *evidence* of possession of the properties.

Evidence is a reference to a means of assessing the truth of a given premise and the artifacts created or examined in that assessment.

- A means to convince others to believe a conclusion through reasoning and one or more premises
- An argument is supported by evidence.

Conclusions

- Lots of Material available https://bit.ly/cmhpapers
- Aviation based tutorial being developed
- Can be used as alternative means – Now (on FAA projects)
- Use cases still being developed and evaluated
- How this will fit into a regulatory framework – Still To Be Decided

Summary

- Existing Standards have served us well
- Innovation and Technology is driving change
- “Tweeking” changes don’t help enough

The Challenge -

More efficient, more effective Development and Certification

Requires – Authorities AND Industry participation

Assurance Cases are a promising option