Enhancement of ARINC 653 for Multi-core Hardware

Stephen Olsen
VxWorks Product Line Manager

WIND

This presentation contains no export restricted information.

VxWorks

Safe & Secure RTOS Platform

Agenda

- Industry Trends
- What is ARINC 653?
- Multicore issues
- Overview of the VxWorks 653 Single and Multi-core Edition
- Q&A

Main Aerospace & Defense Trends

Aerospace

- More Functionality – smarter avionics, SWaP, more payload
- Autonomous systems
- Global procurement/partnerships
- Safe and Secure
- Pressure on development costs, schedule
- Pressure on operational costs (personnel, training, spares)

Defense

- More Functionality – more lethality/survivability, integrated battlefield, more arms and armor
- Cyber warfare (more computer-based systems)
- Coalitions/interoperation
- Secure and Safe
- Pressure on development cost, schedule
- Pressure on operational costs (personnel, training, spares)

System Implications

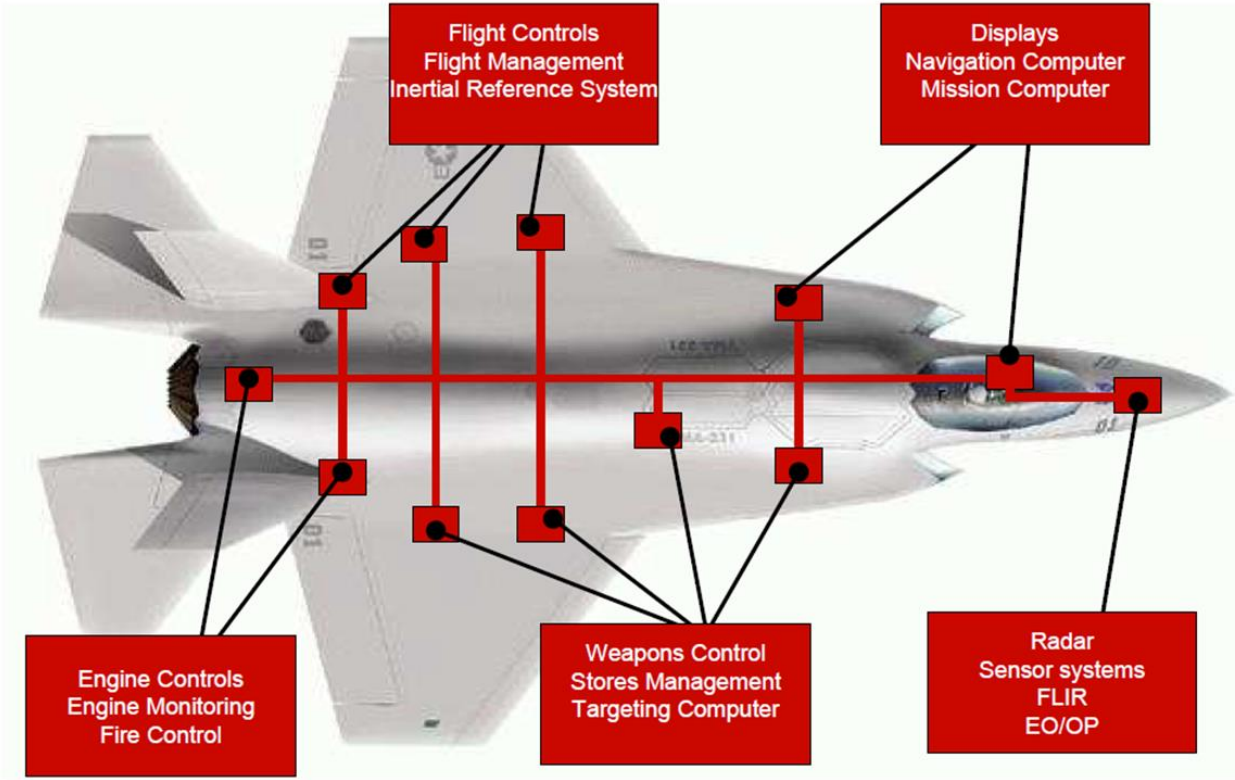
More functions, “systems of systems,” more connectivity in less space, weight, and power (SWaP), reduced cabling

Hardware consolidation
(multiple applications on fewer processors)

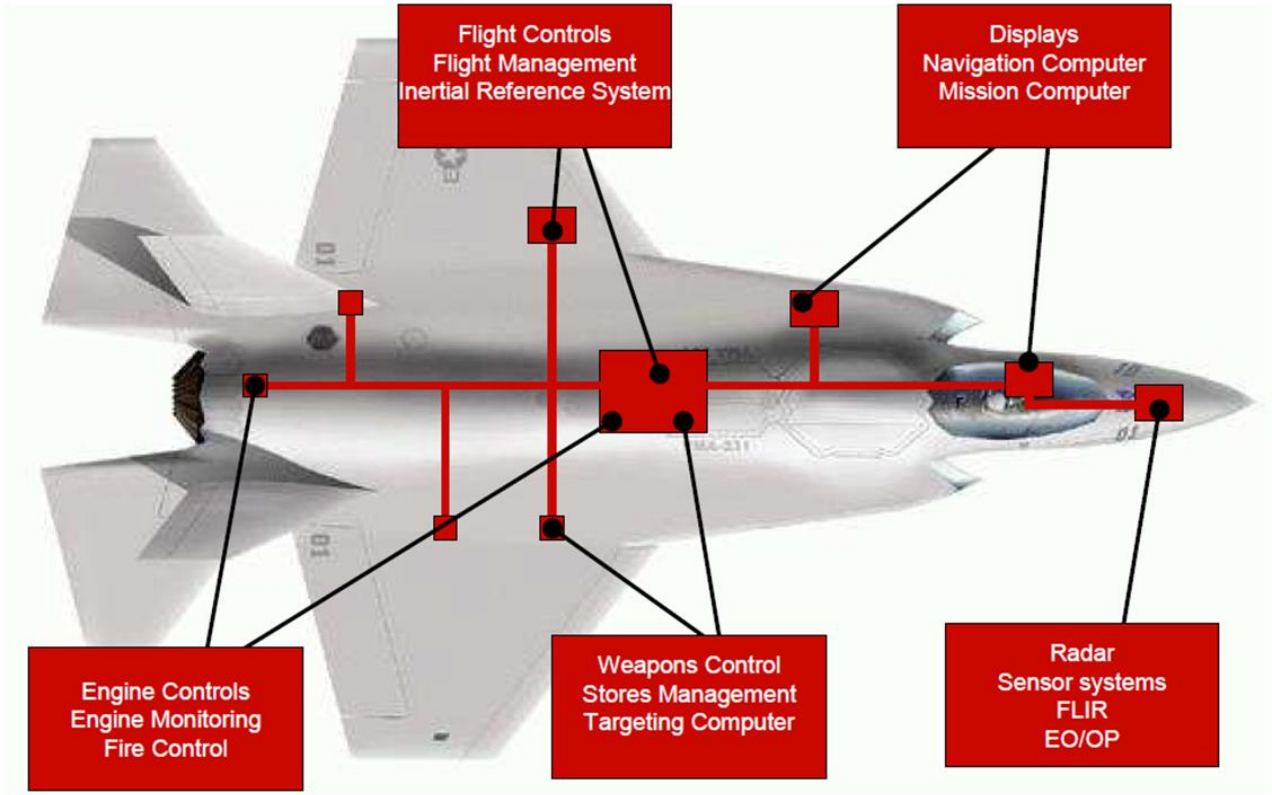
Software “pressure”: larger volume of
Software comingled on fewer processors

New challenges to Safe and Secure

Federated vs. IMA



Federated vs. IMA



Federated versus IMA

Federated

PROs

- Traditional methodology (Well Understood)
- Relative “ease” of Design and certification
- Supply chain geared for this

CONs

- SWaP – Each function is separate LRU
- Poor S/W Re-use
- Poor portability
- Poor modularity
- Tier 1 at mercy of Primes ($$ for Tier 1)

IMA

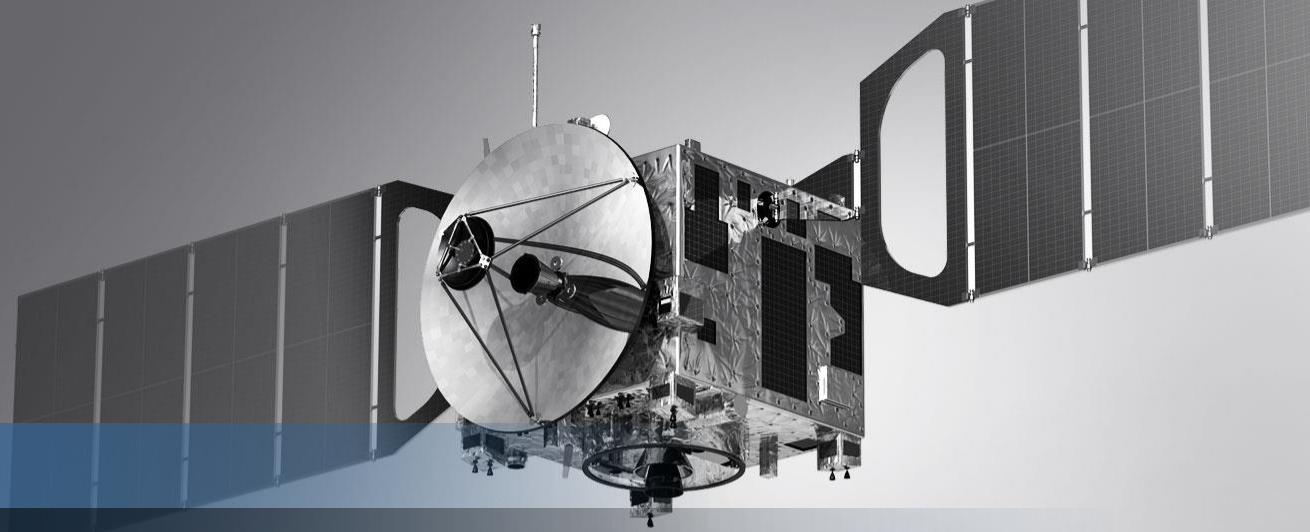
PROs

- SWaP (multiple functions on single LRU)
- Excellent S/W re-use
- Excellent portability
- Excellent modularity

CONs

- “Modern” methodology (777, A380, 787…)
- Poorly understood
- Complexity of design and certification
- Supply chain not setup for IMA projects

AEROSPACE



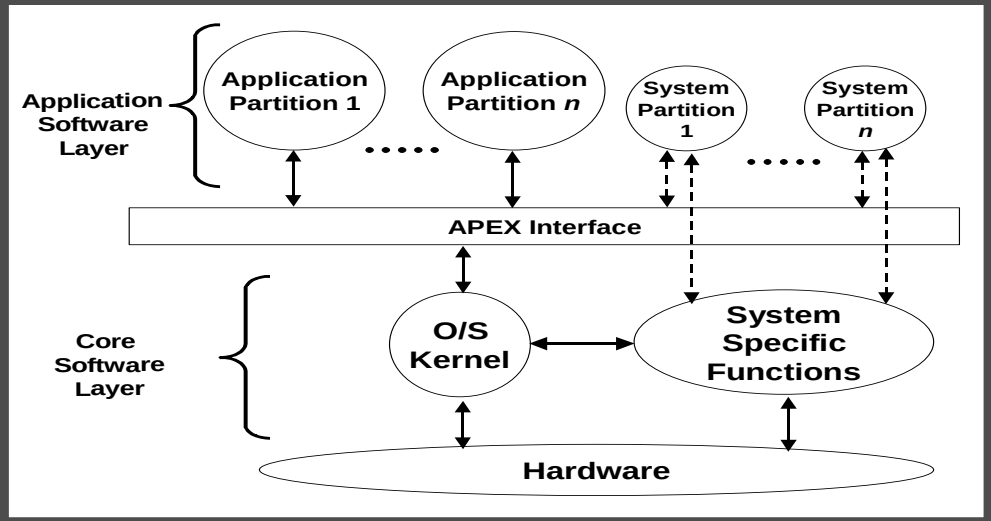
What is ARINC 653?

ARINC 653

- ARINC 653
  - Avionics Application Standard Software interface
    - APEX (Application Executive) APIs
  - Space and Time partitioning
  - Safety of Real Time Operating System (RTOS)
  - Multiple applications with different safety requirements
  - Integrated Modular Avionics (IMA)
- VxWorks 653 is specifically tuned to address the needs of ARINC 653

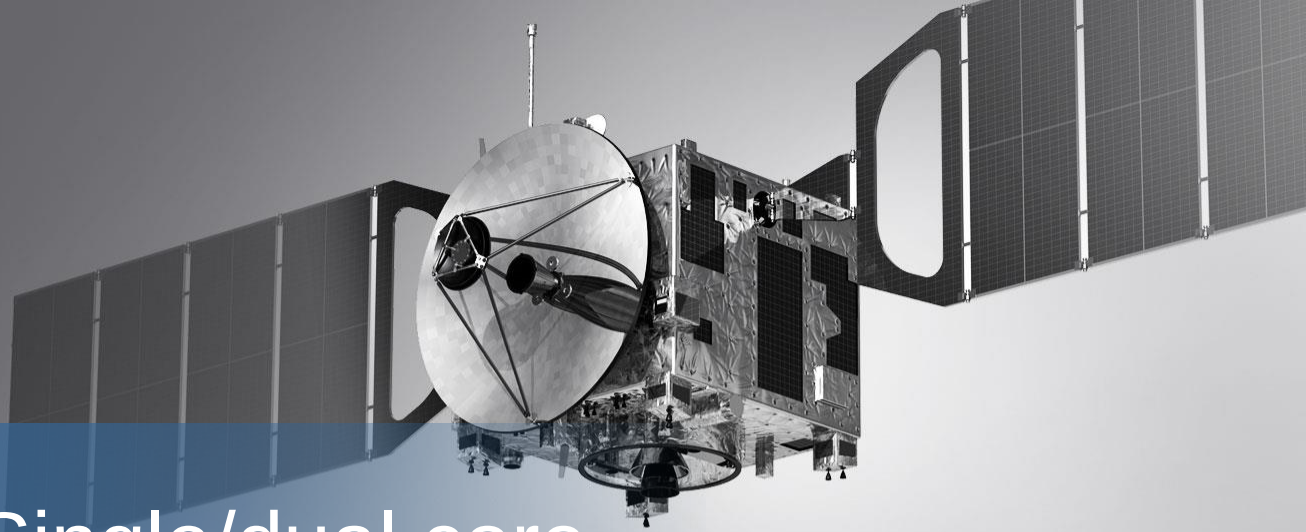
ARINC 653 APEX (APplication EXecutive)

- The ARINC 653 specification defines a general purpose APEX (Application/Executive) interface between the OS and the application software



- Partition management
- Process management
- Time management
- Inter-partition communication
- Intra-partition communication
- Error Handling

© 11



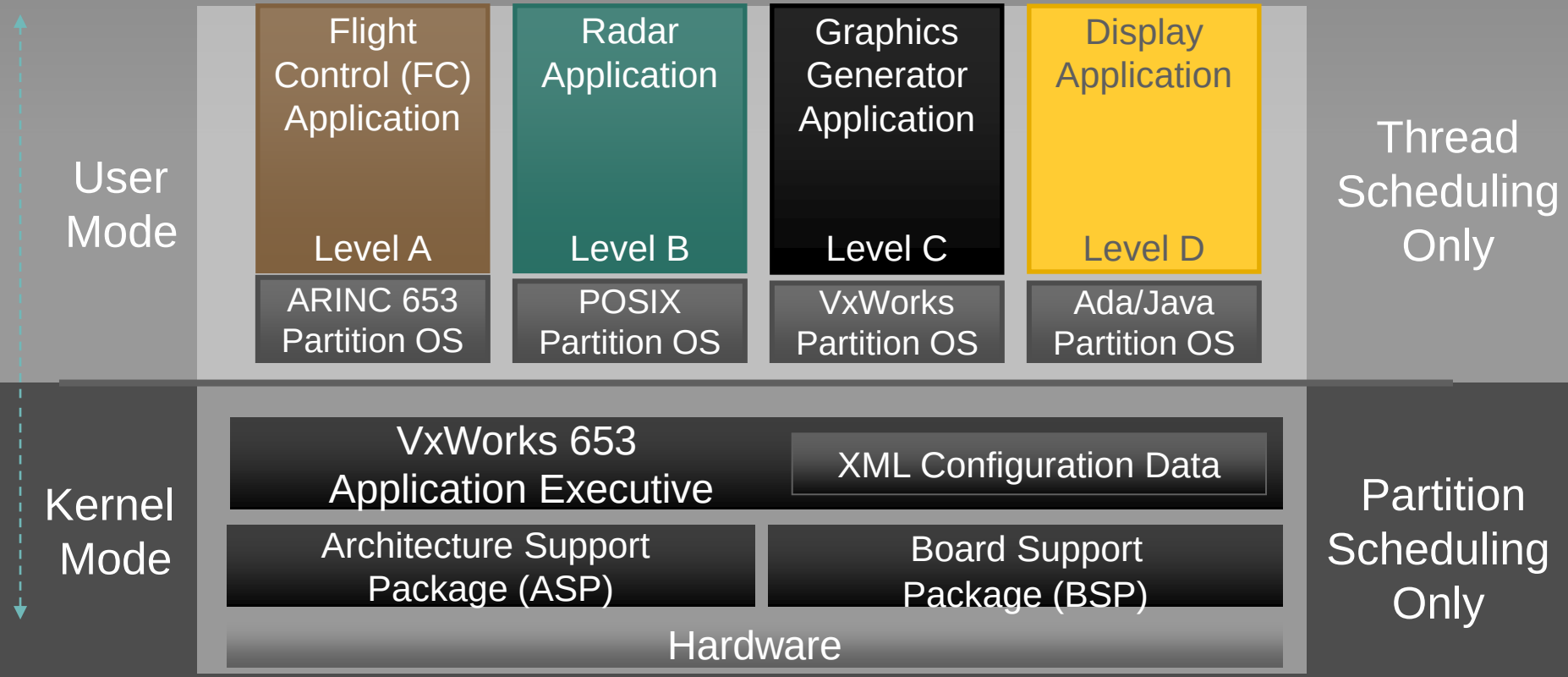
AEROSPACE

VxWorks 653 Single/dual core

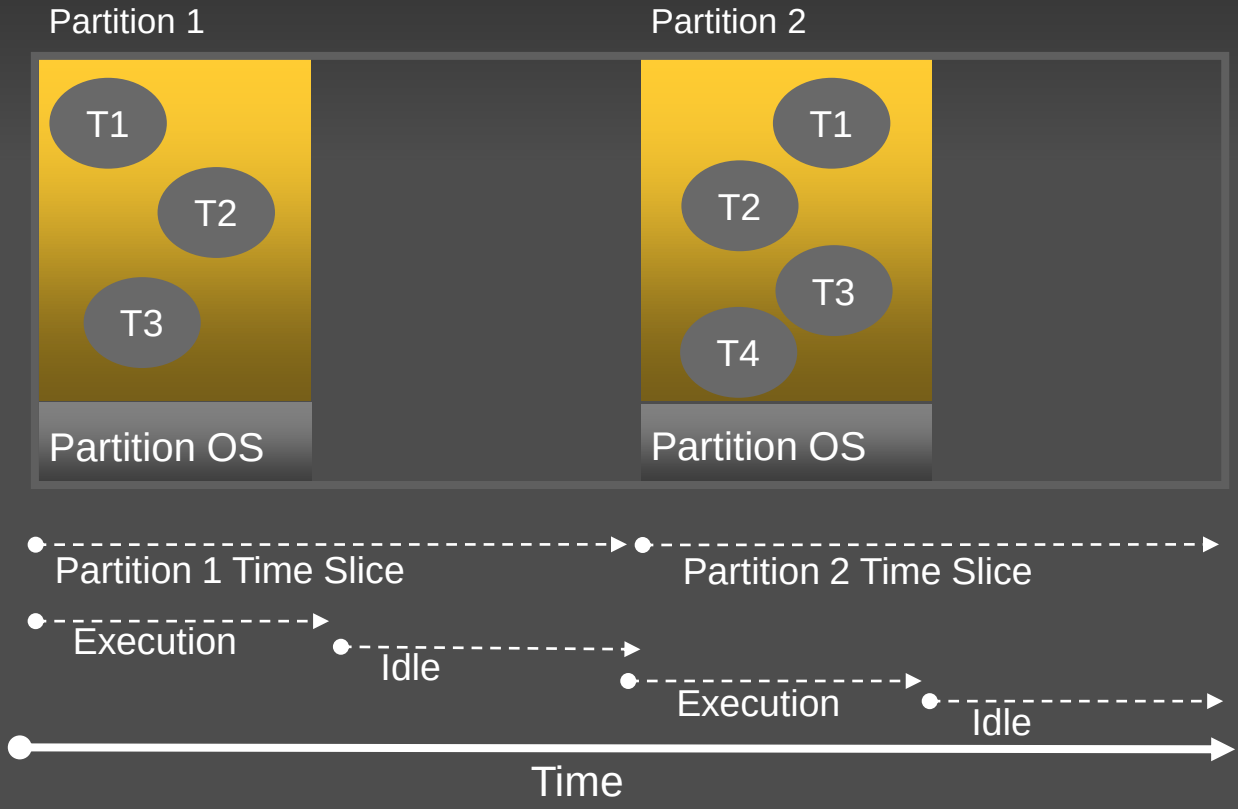
VxWorks 653 Single/Dual-core (up to 2.x)

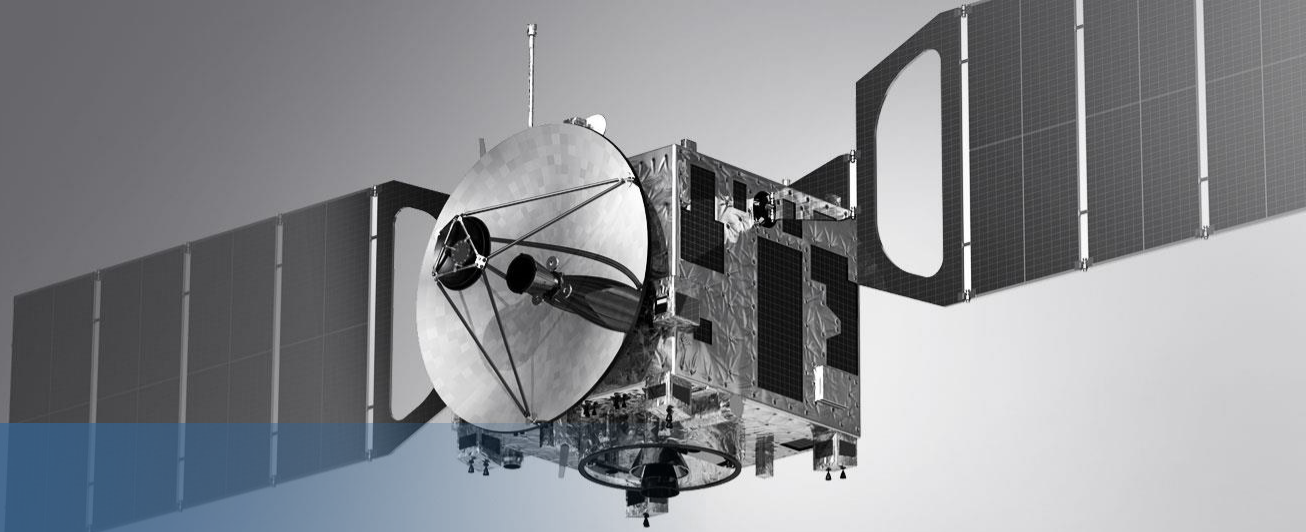
- Certifiable to RTCA DO-178C, Level A
- Support certification of multiple design assurance levels(DAL) on multiple cores running concurrently
- Fault isolation and containment: Health Monitors
  - The module operating system shall manage and enforce configuration of interconnect functions on the underlying architecture including IO, memory and caches
- Static configuration and enforcement in accordance with ARINC 653
- Role-based configuration per RTCA/DO-297

VxWorks 653 2.x IMA Architecture



High-Performance, Two-Level Scheduling





AEROSPACE

VxWorks 653 Multi-core Edition

Multi-core System Issues

- Contention makes it difficult to prove that timing constraints are met
- Most SoC's uses hardware that is shared between cores
- Designs and effects of sharing are often unavailable
- Sharing effects may change as SoC microcode is updated
- Addressing these issues can involve additional cert effort

Performance and certification costs depend on matching the choice of strategies of the multicore hardware and the software application

Certification Authorities Software Team CAST-32A (Multi-Core Processors)

- FAA-published guidance on usage of multi-core processors in aviation
- Available free on FAA website
- Topics Applicable to Multi-Core Processors (MCP) in Safety-Critical Applications
  - Sixteen objectives on MCP Determinism
  - Six objectives for MCP Software
  - Two objectives for MCP Error Handling
  - ~~CAST paper addresses only 2 cores at this time, but is largely applicable to more than 2 cores~~
  - Wind River Verification Activities will support many objectives, but integrators will need to conduct additional activities to ensure compliance

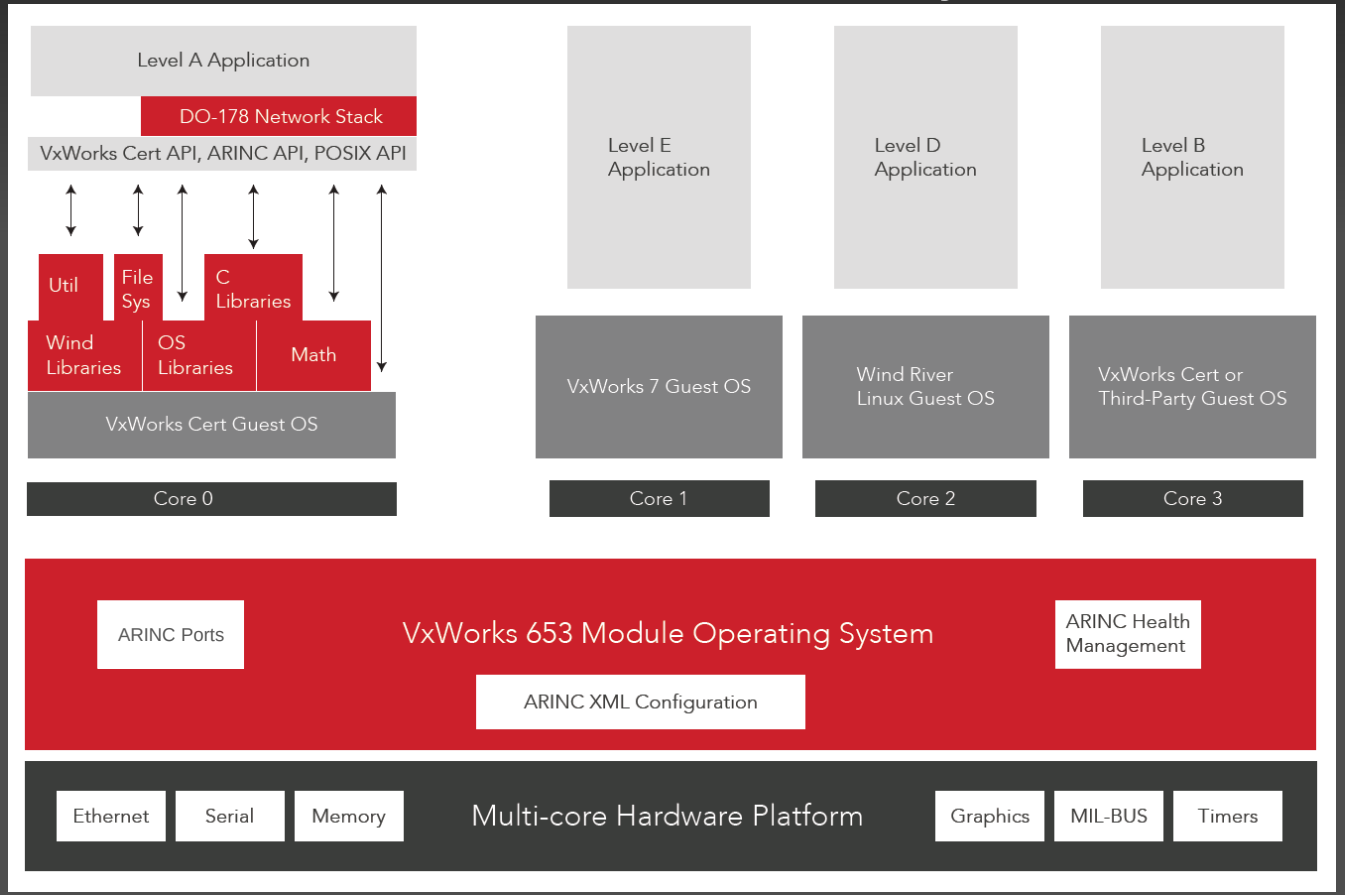
Released November 2016

CAST-32A Appendix has mapping from CAST 32 to 32A

VxWorks 653 3 Multi-core Edition Requirements

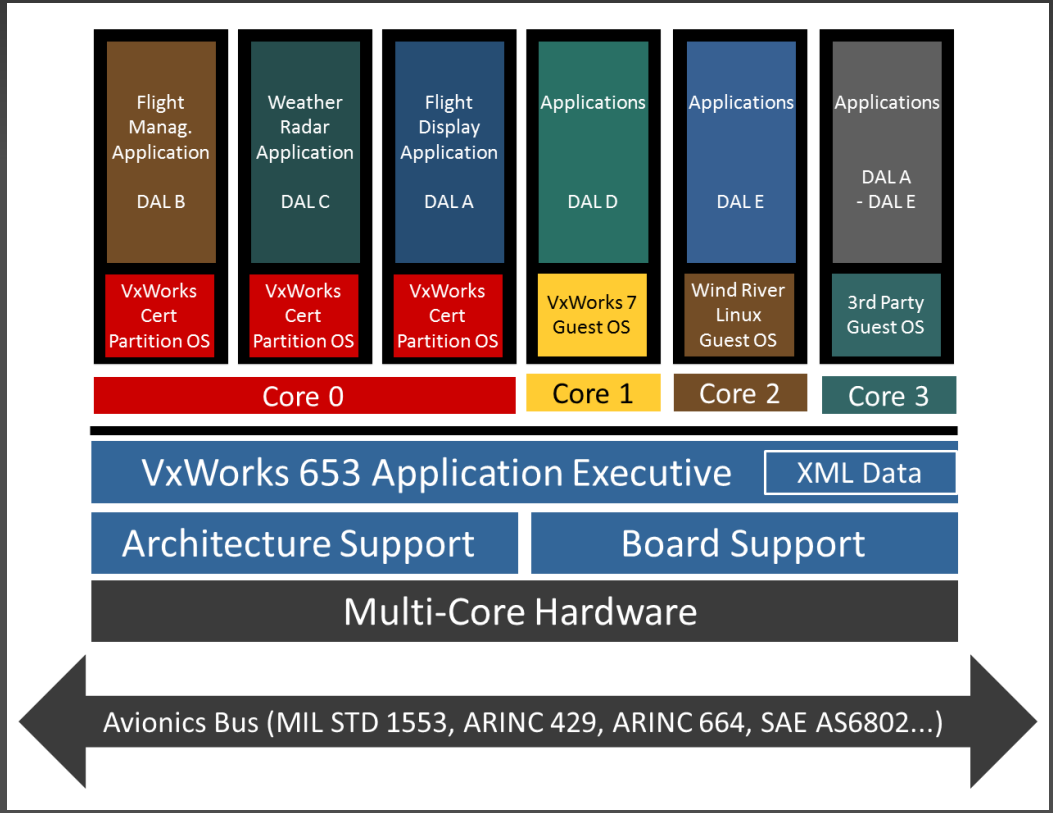
- Certifiable to RTCA DO-178C, Level A
- Support certification of multiple design assurance levels(DAL) on multiple cores running concurrently
- Fault isolation and containment: Health Monitors
  - The module operating system shall manage and enforce configuration of interconnect functions on the architecture
- Static configuration and enforcement in accordance with ARINC 653
- Role-based configuration per RTCA/DO-297

VxWorks 653 3.0 Multi-core Edition Safety Architecture



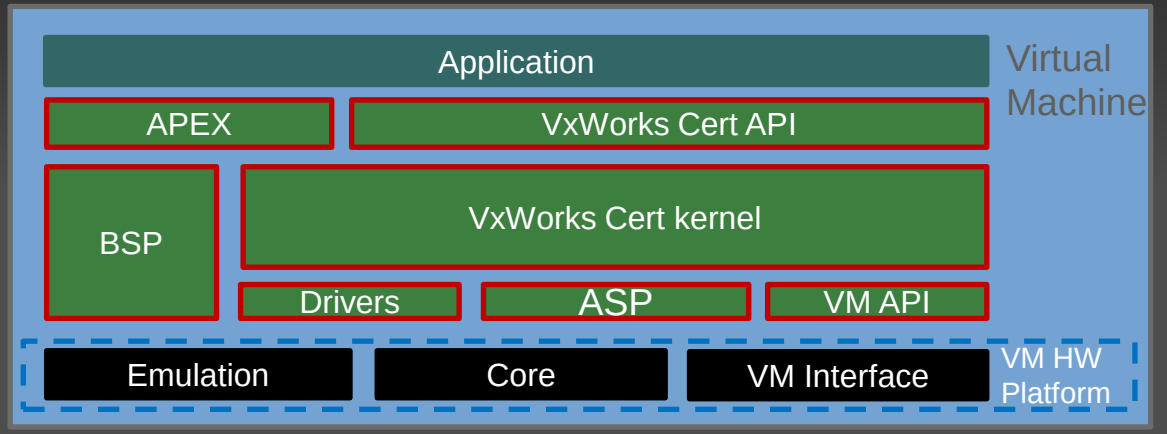
VxWorks 653 3.0 Multi-core Edition Time Scheduler

With the time partition scheduler, system integrators can schedule multiple guests in a specific time window to be scheduled on a core.



Roles of the MOS and POS in 3.0 Multi-core Edition

- Partition OS (POS)
  - VxWorks Cert 6.6.7
    - Native kernel
    - BSP has Virtualization component
  - *Device drivers are distributed to each Partition OS*
  - APEX library
  - Application IBLL



- Module OS (MOS)
  - Uses only devices required to enforce partitioning
  - Manages access to common architecture specific resources
  - Provides services for communication, health monitoring and emulation
  - System Fault Handling
  - Configuration management

Configuration Data

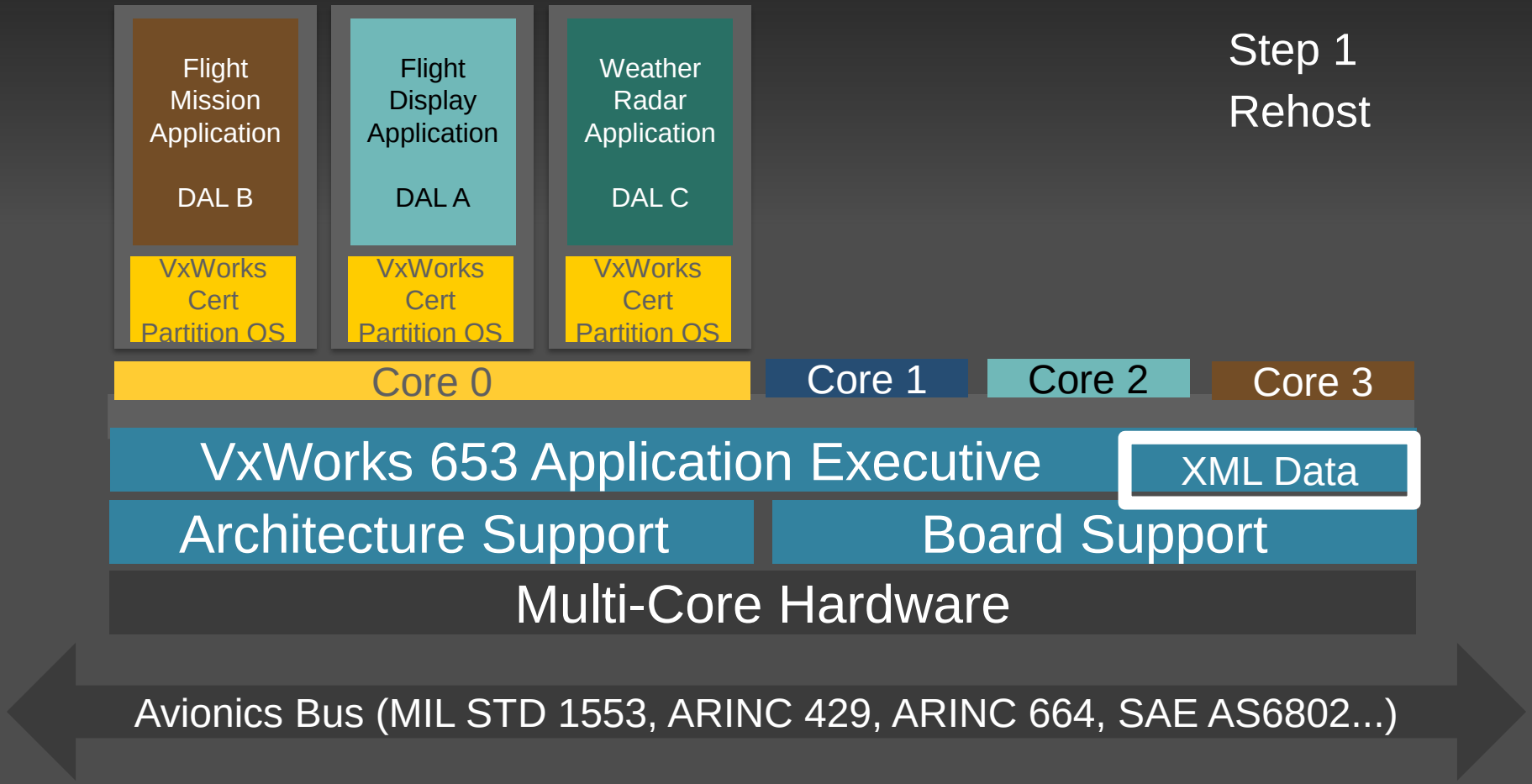
653 Platform Software

VM HW access interfaces

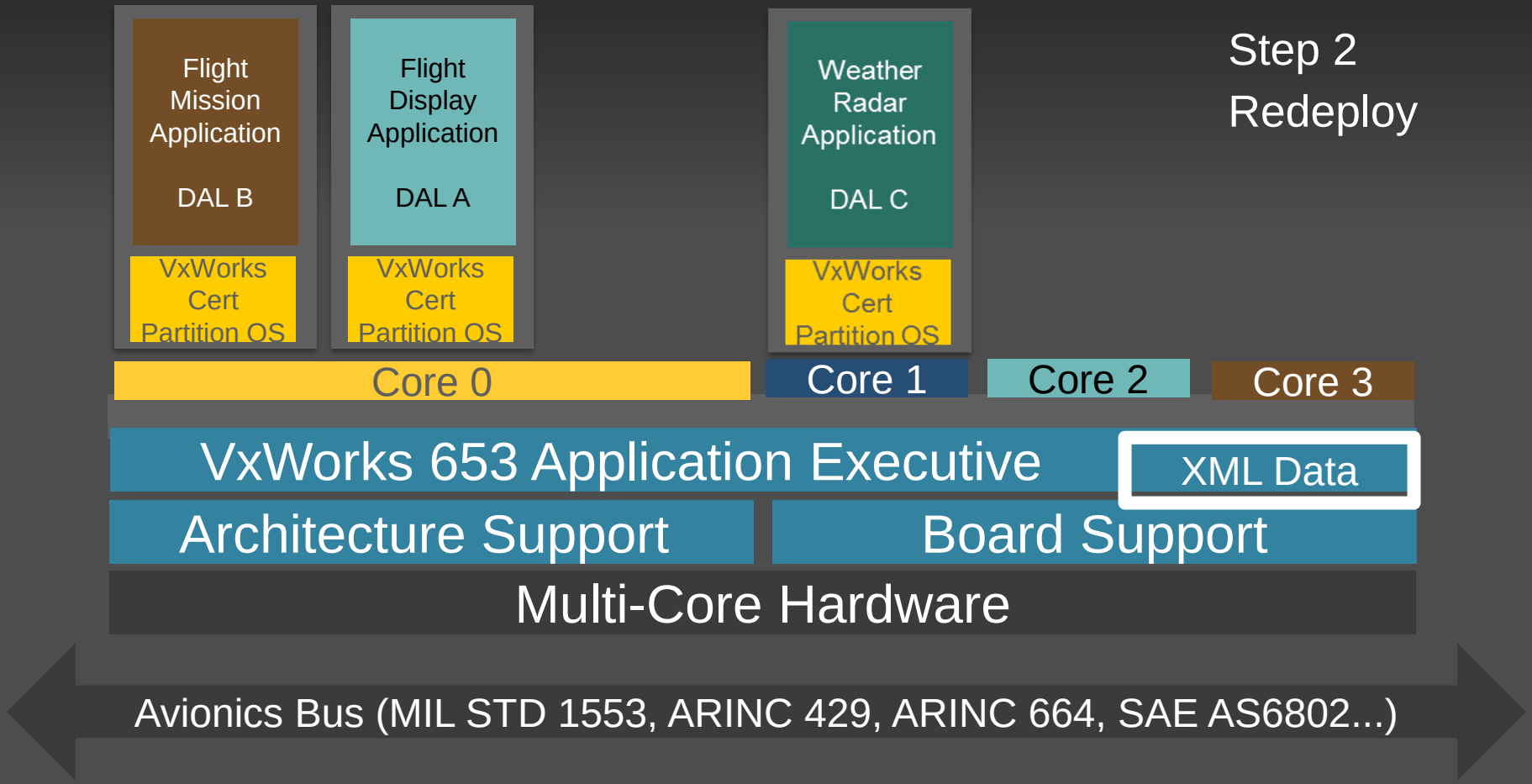
VxWorks 653 MCE Use Case - Migration

- Step 1
  - Re-host existing uni-core platform using a single core of a multicore
  - Minimizes risk but allows for characterization in the new environment to establish a baseline of performance and resolve any issues using existing techniques and understanding
  - Criteria for success easily established and bounded

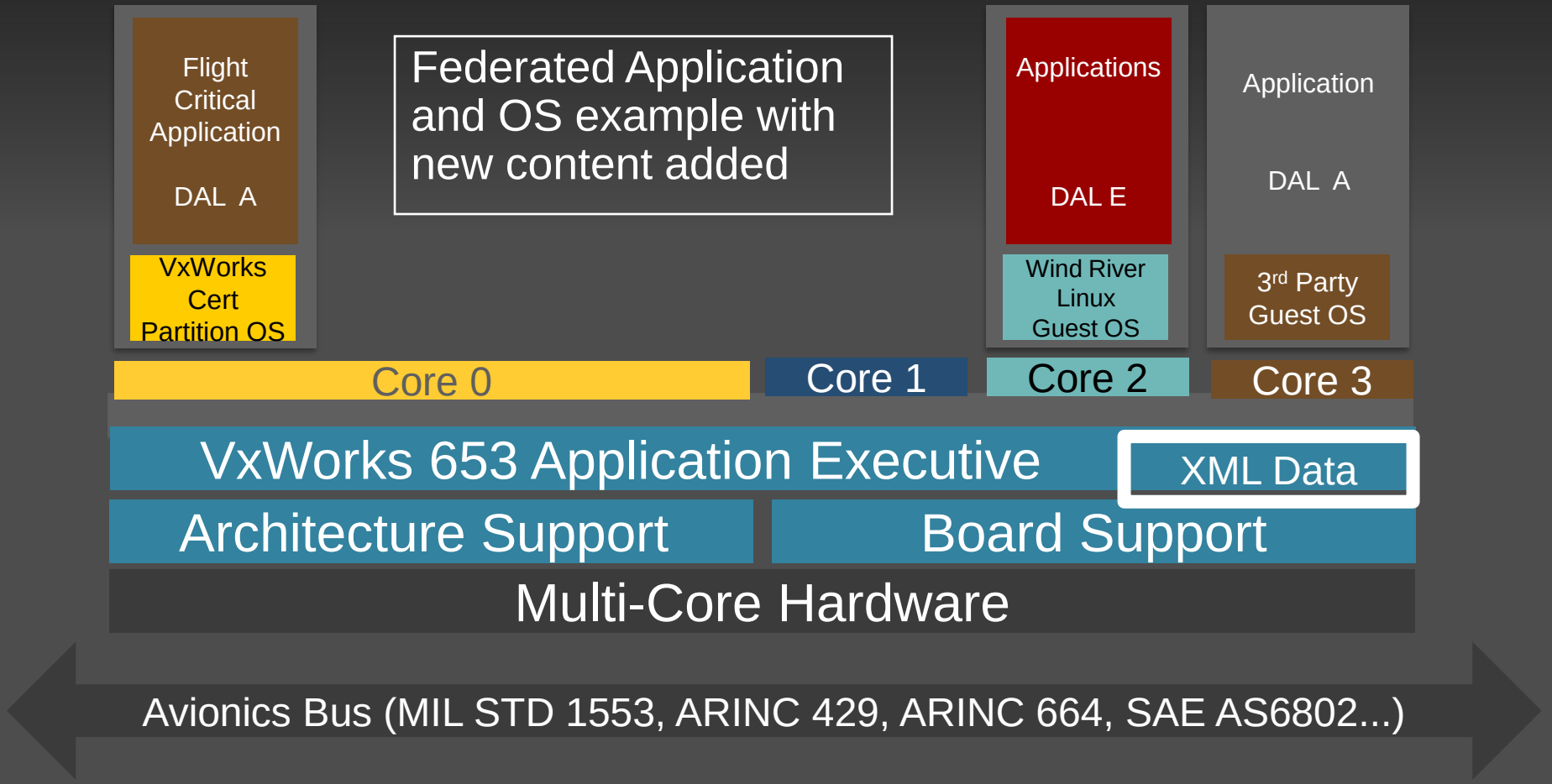
- Step 2
  - Redeploy platform by moving partition(s) to other core(s)
  - Re-distribute IO to allow for dedicated resources per partition
  - Perform characterization of new configuration against Step 1

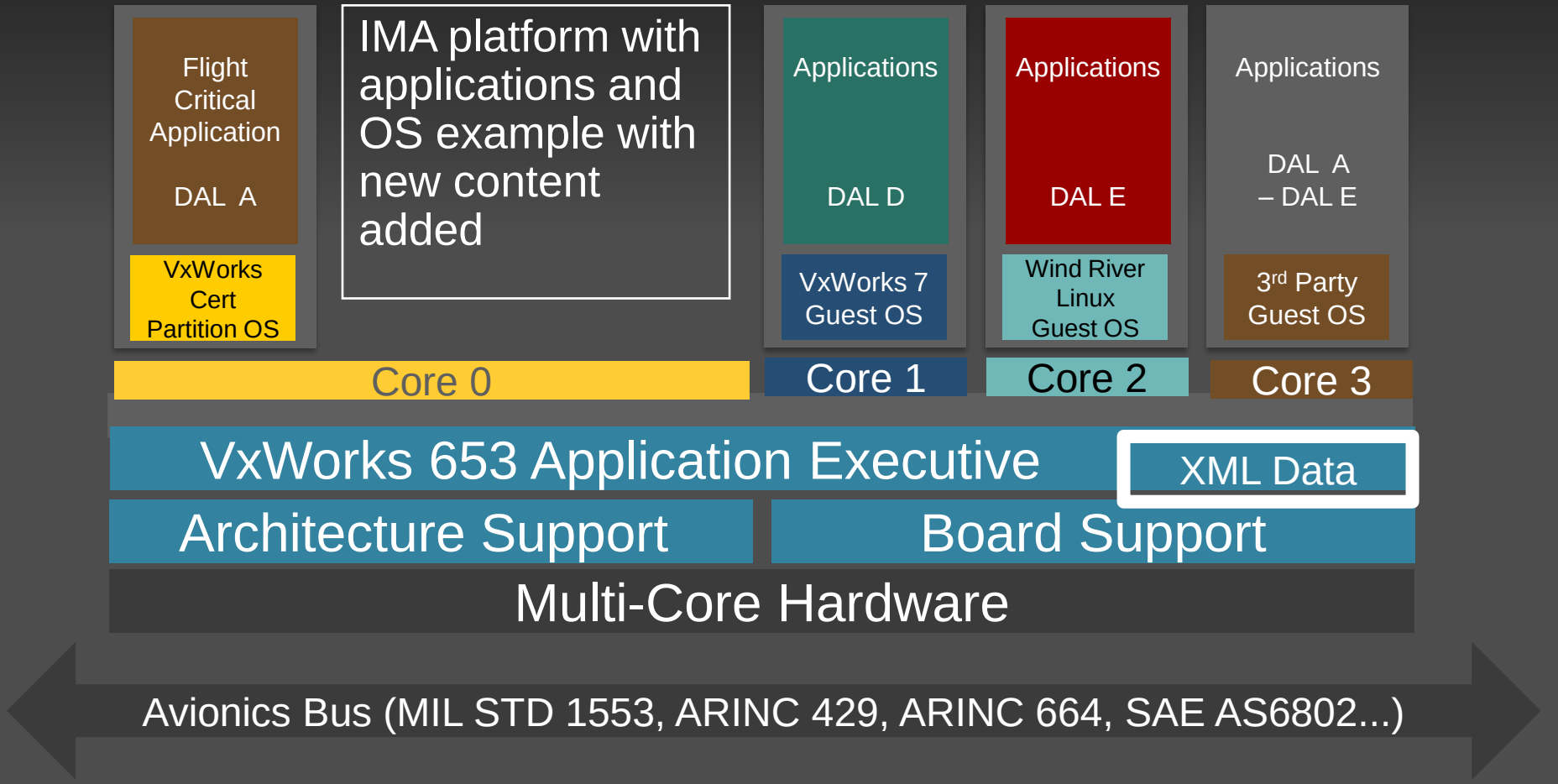


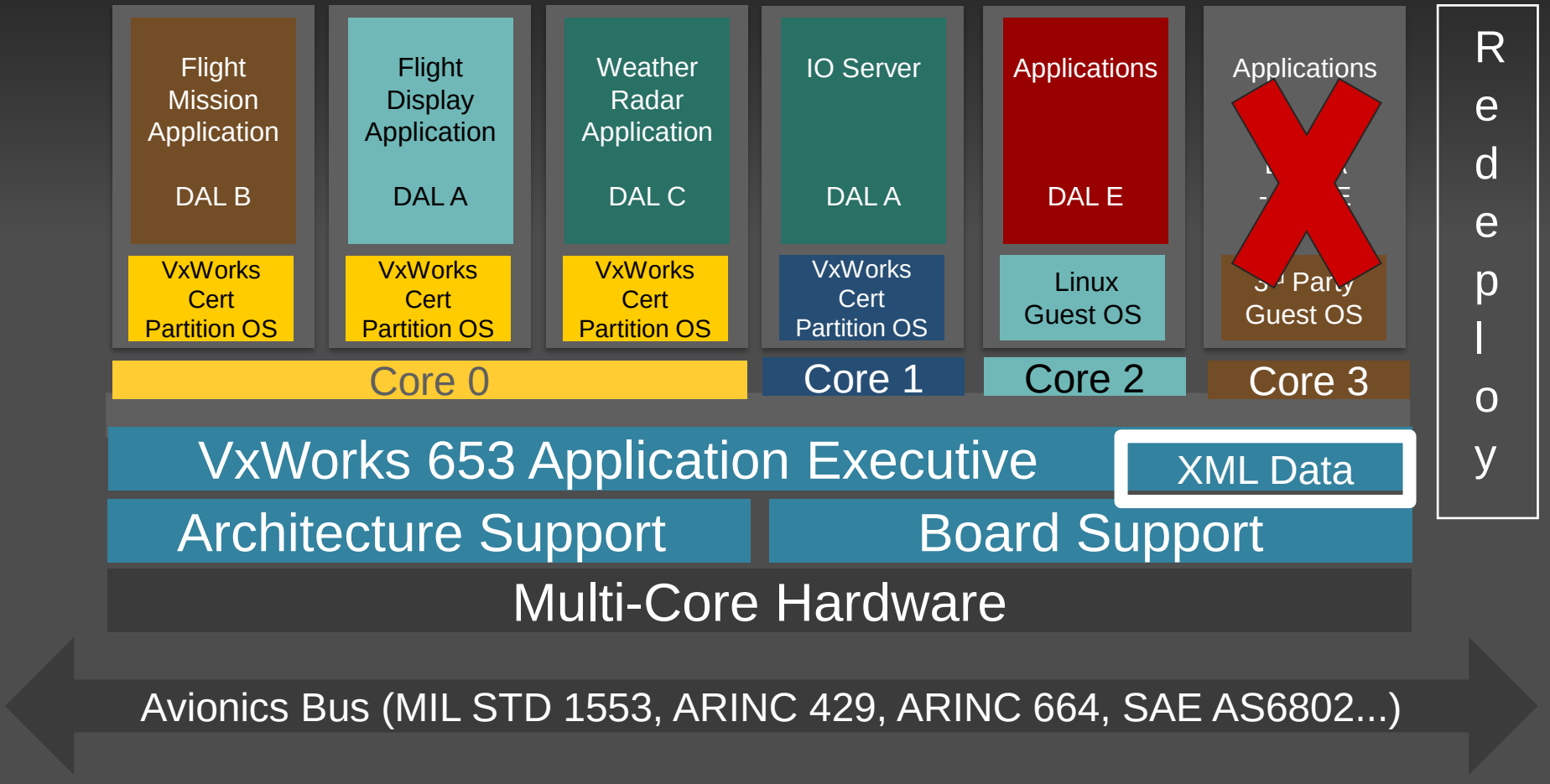
Step 1
Rehost



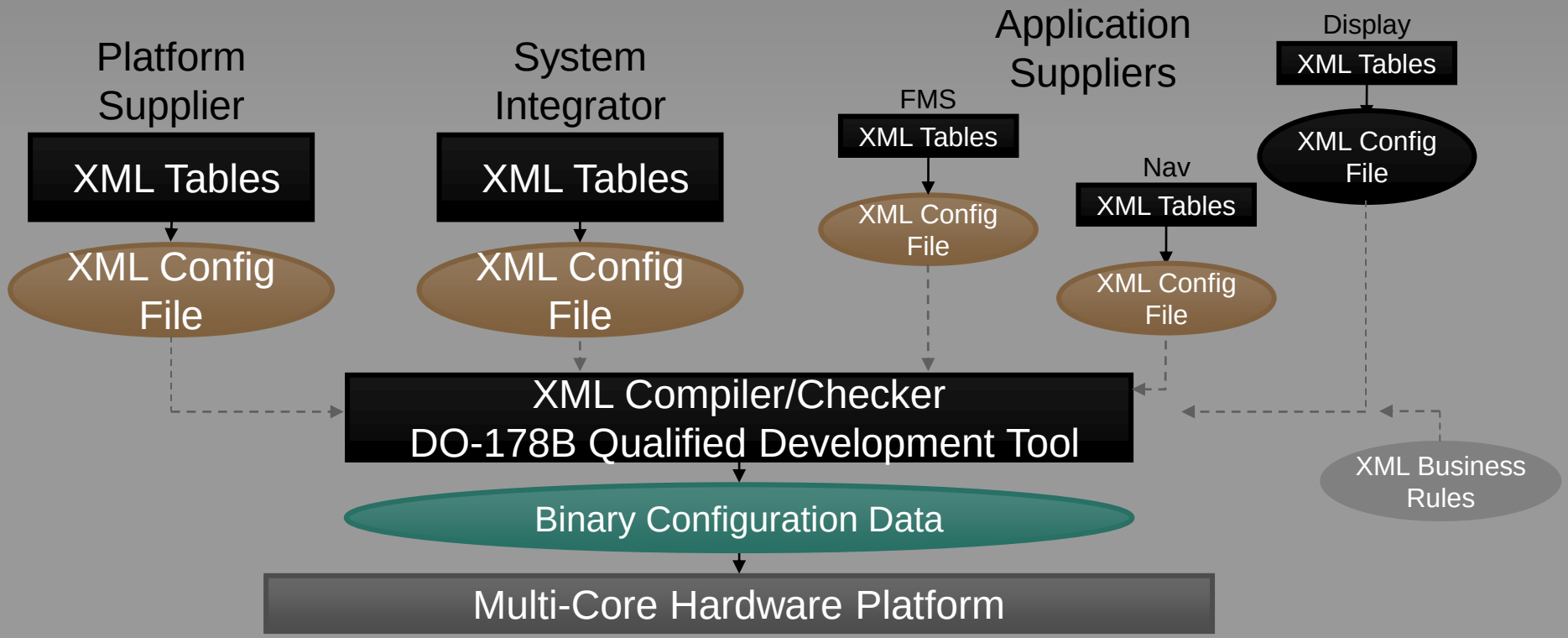
Step 2
Redeploy


Federated Application and OS example with new content added
Flight Critical Application
DAL A
VxWorks Cert Partition OS
Applications
DAL E
Wind River Linux Guest OS
Application
DAL A
3rd Party Guest OS
Core 0
Core 1
Core 2
Core 3
VxWorks 653 Application Executive
XML Data
Architecture Support
Board Support
Multi-Core Hardware
Avionics Bus (MIL STD 1553, ARINC 429, ARINC 664, SAE AS6802...)


Flight Critical Application
DAL A
VxWorks Cert Partition OS
IMA platform with applications and OS example with new content added
Applications
DAL D
VxWorks 7 Guest OS
Applications
DAL E
Wind River Linux Guest OS
Applications
DAL A – DAL E
3rd Party Guest OS
Core 0
Core 1
Core 2
Core 3
VxWorks 653 Application Executive
XML Data
Architecture Support
Board Support
Multi-Core Hardware
Avionics Bus (MIL STD 1553, ARINC 429, ARINC 664, SAE AS6802...)


Flight Mission Application
DAL B
VxWorks Cert Partition OS
Flight Display Application
DAL A
VxWorks Cert Partition OS
Weather Radar Application
DAL C
VxWorks Cert Partition OS
IO Server
DAL A
VxWorks Cert Partition OS
Applications
DAL E
Linux Guest OS
Applications
Guest OS
Core 0
Core 1
Core 2
Core 3
VxWorks 653 Application Executive
XML Data
Architecture Support
Board Support
Multi-Core Hardware
Avionics Bus (MIL STD 1553, ARINC 429, ARINC 664, SAE AS6802...)
Redeploy

DO-297 Role Separation



Conclusion

- Important industry trends are leading to integrated systems.
- ARINC 653 addresses these needs both for single and multi-core.
- VxWorks 653 addresses ARINC 653
- Remember: Safety and Security paramount