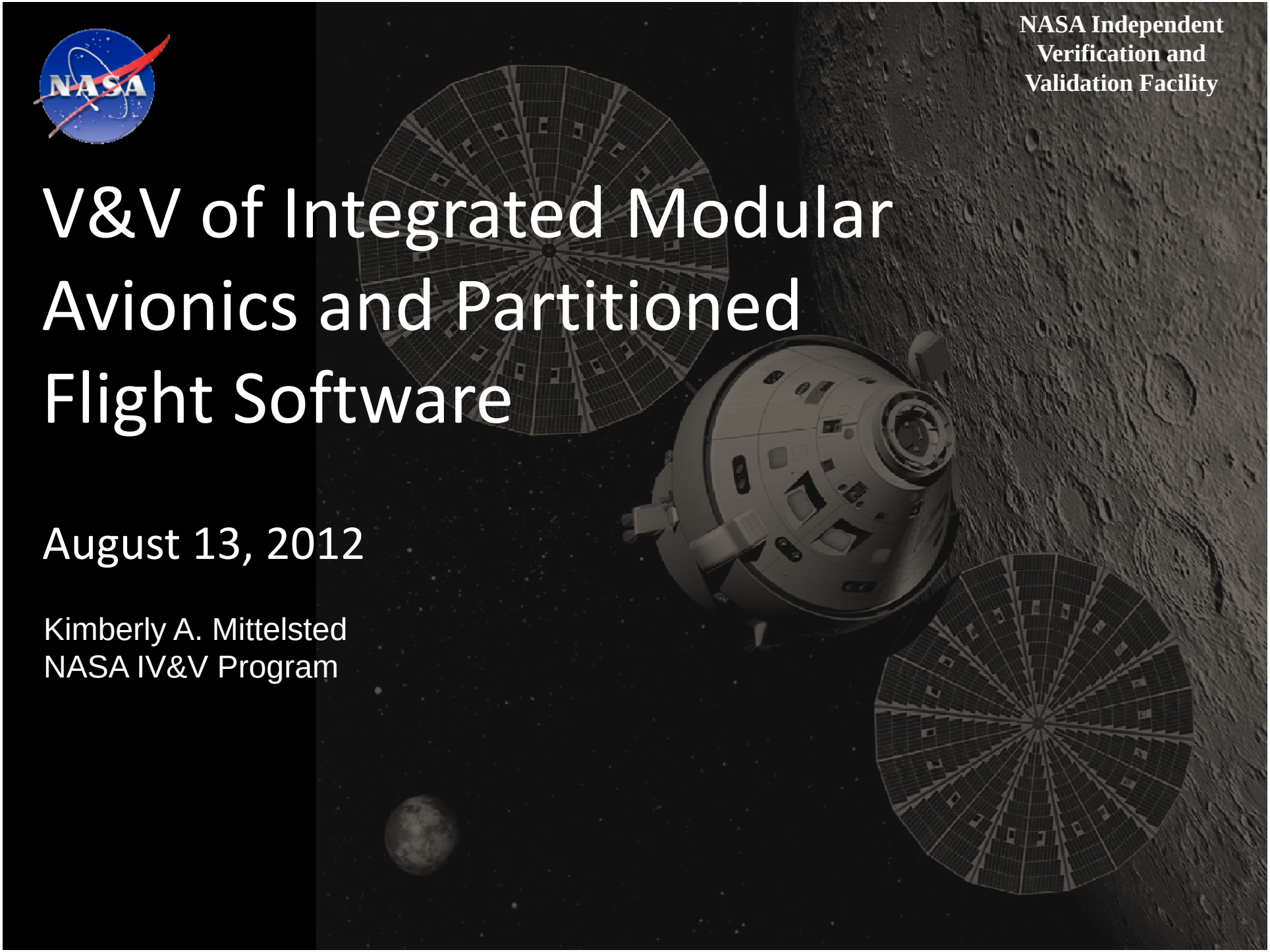


NASA Independent Verification and Validation Facility

V&V of Integrated Modular Avionics and Partitioned Flight Software

August 13, 2012

Kimberly A. Mittelsted
NASA IV&V Program

Purpose

- Present the identified impacts to NASA IV&V practices from the application of Integrated Modular Avionics (IMA) and ARINC 653 time and space partitioned software to human rated NASA mission.
  - Discuss recent NASA IV&V project experience.

Why Does this Matter?

- There is a greater potential for IMA and ARINC 653 systems in NASA's future.
- Cost advantages, RTOS availability, and processor power will continue to make DO-297 IMA and ARINC 653 partitioned software more useful to future projects.
- There are roles for both FAA (launch and landing) and NASA (RPOD) in programs similar to COTS or CCP.
  - DO-297 IMA and ARINC 653 FSW are areas where common approaches appear to benefit both.

Introduction

- The material in this presentation is the result of three recent IV&V projects
  - CxP Orion IV&V: support to the Constellation Program's Orion project
  - MPCV IV&V: support to the Multi Purpose Crew Vehicle Program
  - IAGTAS: IV&V Capabilities Development task "Analysis Guideline and Template for ARINC-653 Systems"
- The V&V of ARINC 653 time and space partitioned FSW was the subject of two prior Monday workshops; an attempt is made avoid duplication.
- Multiple tangential topics are trivially introduced and not addressed fully. These topics are worthy of future capabilities development efforts, technical discussions, or were the subjects of prior Monday workshop sessions, including:
  - Hard, Firm or Soft RTOS V&V
  - COTS OS V&V
  - DO178 artifacts and value of DO178 to NASA readiness for flight
  - Data flow analysis within partitioned systems

IMA and Quality of Service

- A working definition of IMA:
  - *"Modular Avionics is defined as a shared set of flexible reusable, and interoperable hardware and software resources that create a platform that provides **services**, designed and verified to a defined set of safety and performance requirements, host applications performing aircraft related functions"*
- IMA is an abstracted approach to HW/SW, SW/SW, and HW/HW interfaces.
  - This abstraction places a greater demand on the negotiation and conformance to the quality of service.
  - Application performance is dependent on services and independent of the platform.
    - Need to conform to interface agreements is exceptionally great.

Integrated Modular Avionics (IMA)

- IMA is a move away from federations of dedicated or specialty processors.
  - Smaller number of general purpose processors.
- Distinctions of federated systems vs. IMA systems are subjective and delivered systems may incorporate elements of both.
- Distinguishing characteristics of IMA systems:
  - Shared resources
  - Platform independent application development
  - Portable applications
  - Expandable/Reconfigurable with limited impacts
  - Increased configuration management complexity
    - Most CM issues must be managed at the integrated level

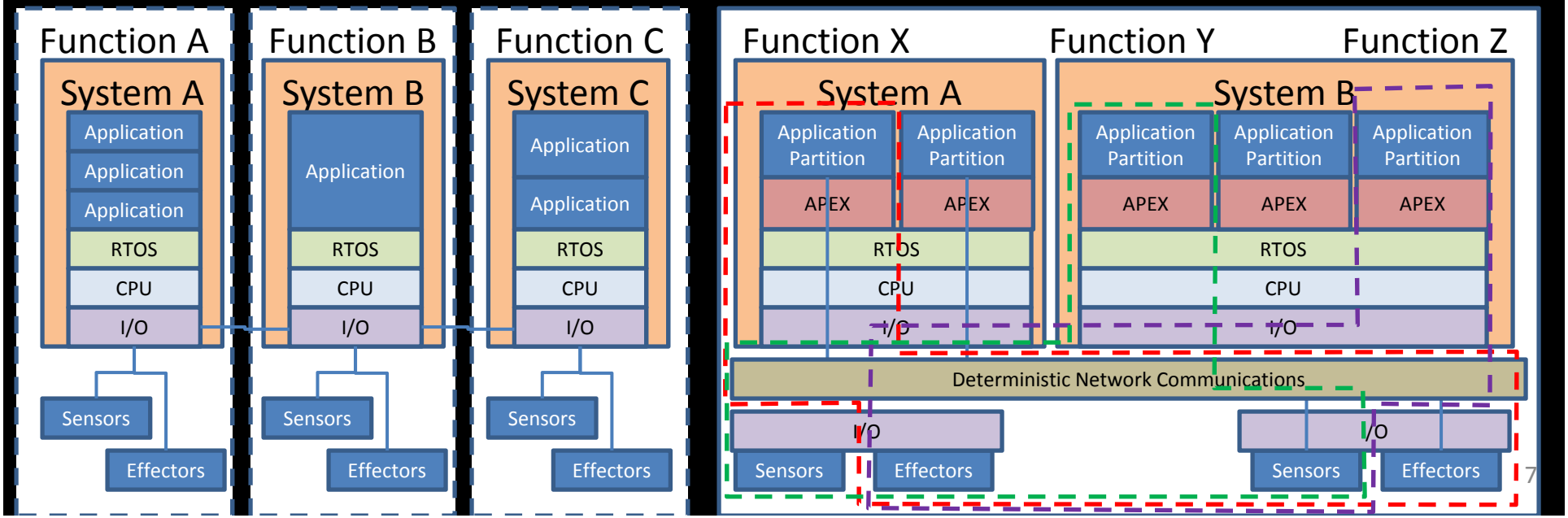
Idealized Architecture Comparison

Federated

- Dedicated processors.
- Dedicated resources
- Lower CM complexity
- Platform dependent applications.
- Redundancy managed at box level.

IMA

- Smaller # of processors
- Shared resources
- Platform independent application
- Portable applications
- Expandable/Reconfigurable
- Redundancy managed at IMA.

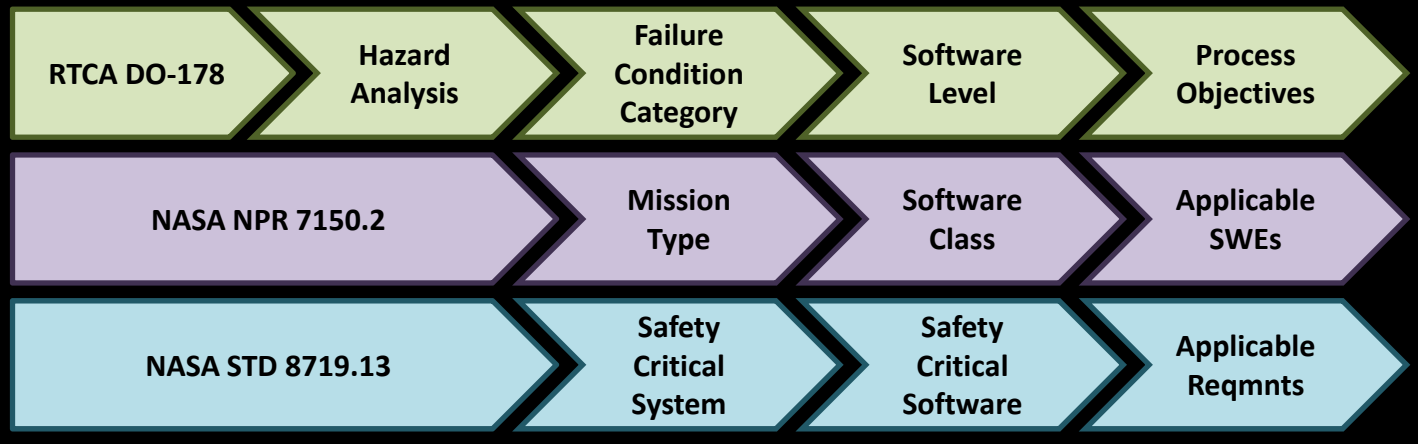


Naming and standards

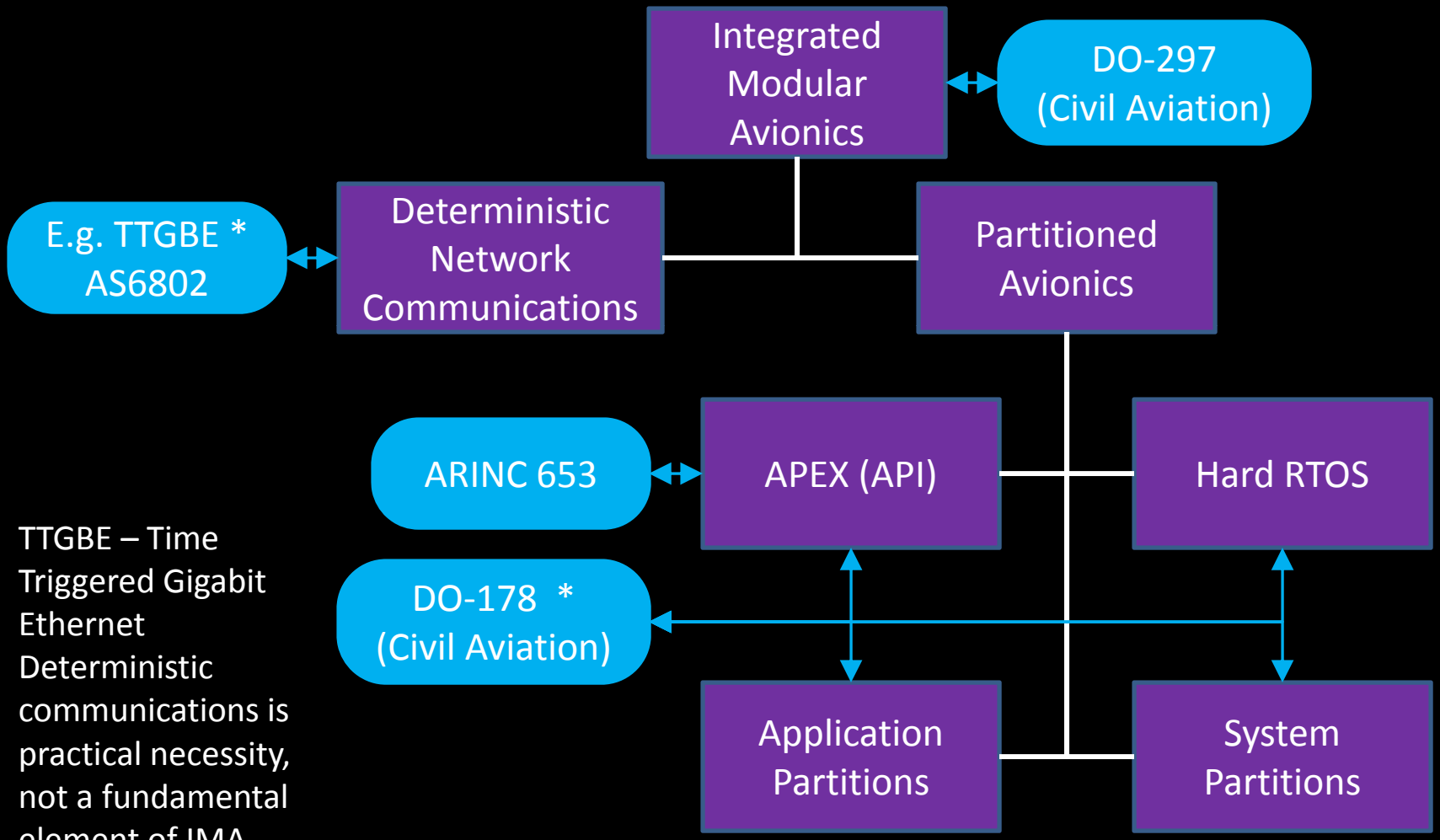
- IMA and ARINC 653 are frequently conflated.
  - ARINC 653 *"Avionics Application Standard Software Interface"*. This is a standard at the FSW level
  - IMA is more correctly tied to DO-297 *"IMA Development Guidance and Certification Issues Document"*
    - A product of RTCA Incorporated.
    - A guidance document for conforming to FAA airworthiness standards

Associated Concept DO-178

- IMA and ARINC 653 will further be tied to DO-178, "*Software Considerations in Airborne Systems and Equipment Certification*"
  - This is a process standard for FSW development consistent with FAA air worthiness standards.
  - Not literally a standard; it's a guidance document, no "Shalls", many "shoulds".
  - Similar to NASA NPR 7150.2 or NPR 8719.13



Concept Structure & Relationships



- TTGBE – Time Triggered Gigabit Ethernet
- Deterministic communications is practical necessity, not a fundamental element of IMA.

- DO-178 defines a software development process and it is not specifically related to IMA or partitioned FSW. RTOS IMA products and civil aviation applications are frequently developed under DO-178 practices.

MPCV, IMA, and DO-297 History

- DO-297 was released November 8, 2005.
- MPCV/Orion contractors were named in August 2006.
- MPCV application of IMA and ARINC 653 was not "bleeding edge".
  - Each was new to NASA.
  - Application of each in civil or military aviation is still expanding.

Partitioned Avionics Software

- An enabling technology for Integrated Modular Avionics
  - Not literally part of IMA
- Particularly valuable for systems incorporating mixed criticality.
  - Mixed criticality is not the only basis for selecting partitioned SW.
  - Criticality is frequently defined in terms of safety impact.
  - Criticality is ultimately whatever the consumer wants to define criticality to be e.g., security criticality.
    - "GHS Integrity 178" and "LynxOS-SE" advertized for mixed security apps.
  - Criticality drives compliance cost. Isolation saves compliance cost.
- Encourages unique application layer development, with commonality below.
  - Applications of mixed criticality or function
  - Common from physical layer to sub-app layer, and built to the highest application's criticality.
- Potential to increase system fault tolerance.

Partitioned Avionics Software

- Partitioning – *"Separation, physically and/or logically, of safety-critical functions from other functionality."* (NASA STD 8719.13)
  - Safety Critical - *Any condition, event, operation, process, equipment, or system that possesses the potential of directly or indirectly causing harm to humans, destruction of the system, damage to property external to the system, or damage to the environment.* (NASA NPR 8719.13)
- Supports structured and isolated FSW
- Supports mixed FSW criticality
  - Supports mixed safety criticality under NASA standards
  - Supports mixed criticality under DO-178

Safety Critical Software (from NASA STD 8719.13)

At least one of the following criteria is true:

- *Resides in a safety-critical system (as determined by a hazard analysis) AND at least one of the following:*
  - *a. Causes or contributes to a hazard.*
  - *b. Provides control or mitigation for hazards.*
  - *c. Controls safety-critical functions.*
  - *d. Processes safety-critical commands or data.*
  - *e. Detects and reports, or takes corrective action, if the system reaches a specific hazardous state.*
  - *f. Mitigates damage if a hazard occurs.*
  - ***g. Resides on the same system (processor) as safety-critical software.***

…

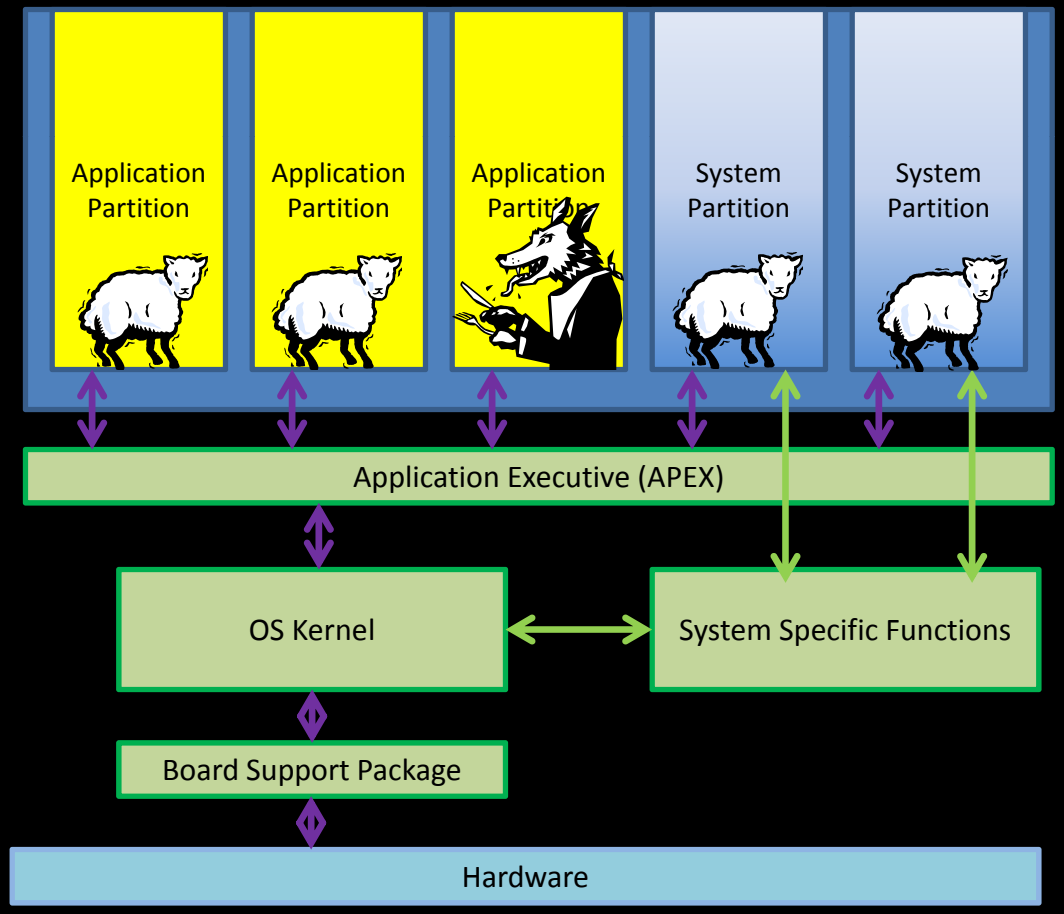
- *Non-safety-critical software residing with safety-critical software is a concern because it may fail in such a way as to disable or impair the functioning of the safety-critical software.* ***Methods to separate the code, such as partitioning, can be used to limit the software defined as safety-critical.*** *If such methods are used, then the isolation method is safety-critical, but the isolated non-critical code is not.*

…

Why partition?

Partitioned SW reflects a solution to an architectural need.

1. **Contain Faults:** The direct impact of faults are usually limited to the partition where the fault occurs. Common errors such as overwriting memory locations or hung processes will not directly impact other partitions.



2. **Limit costs driven by SW criticality.** Partition criticality determined by most critical SW application.
3. **Limit regression tests/ increase portability.** Regression tests largely limited to area inside the partition walls plus ports.
4. **Aid Development/Ease upgrades.** Partition structure reflects a useful boundary for defining CSCIs or development team responsibility.
5. **Improve system architecture.** Consolidate code with similar execution rates. Encapsulates code of similar functionality

"Adequate" SW Partitioning

- A "Gold standard" for partition structure - A partitioned system should provide fault containment equal to an idealized system in which each partition is allocated an independent processor and associated peripherals and all inter-partition communications are carried on dedicated lines.
  - *Spatial partitioning must ensure that software in one partition cannot change the software or private data of another partition (either in memory or in transit) nor command the private devices or actuators of other partitions.*
  - *Temporal partitioning must ensure that the service received from shared resources by the software in one partition cannot be affected by the software in another partition. This includes the performance of the resource concerned, as well as the rate, latency, jitter, and duration of scheduled access to it.*

Experience – Mission Restructure

- Modular and upgradable IMA structure used to reorient vehicle after the cancellation of the Constellation Program.
  - Modular and upgradable nature of IMA used to cut first mission costs.
  - Avionics were restructured for a new mission. Example:
    - First mission change from LEO RPOD to MEO ballistic free flight.
    - Minimal avionics processors. Examples:
      - Elimination of one Vehicle Management Computer
      - Elimination of 6 Power and Data Units (PDUs).
      - Restructured 4 remaining PDU's.
      - Elimination of the backup flight computer
    - Replacement of the display module with a second flight module
    - Sensor and effector changes
      - SM main propulsion eliminated
      - EPS and ECLSS simplification
      - RCS simplification
      - Attitude sensors eliminated (Sun Sensors, Star Trackers, Vision Nav. System)
      - Relative Navigation deleted
  - Prior IV&V architectural analyses were not invalidated by the restructuring

Example Areas of Concern Identified by IV&V

- Lack of insight into code and development processes for COTS software, specifically the operating system, could result in inconsistent verification processes with other flight code
  - Vendor supplied operating system verification artifacts are not available due to high cost
  - With IV&V support, MPCV has decided to verify all software requirements related to features of the operating system being used.
  - Additionally, the operating system is indirectly tested as part of the thousands of other flight software verification tests.
- Use of modern software development tools generates artifacts that are not always familiar to the stakeholder community
  - NASA has no single defined requirement for architecture content, but does establish requirements for a documented architecture.
    - This can lead to disagreements about what is necessary
    - There is a risk that external (e.g. IV&V) reviewers' architectural comments maybe subjective or perceived as subjective.
    - External standards may help define necessary architectural elements.

More Information

- DO-297 *"Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations"* from RTCA
- DO-178 *"Software Considerations in Airborne Systems and Equipment Certification"* from RTCA
- ARINC 653 *"Avionics Application Software Standard Interface"*
- SAE AS6802 *"Time Triggered Ethernet"* SAE International
- NASA/CR-1999-209347 - DOT/FAA/AR-99/58 *"Partitioning in Avionics Architectures: Requirements, Mechanisms and Assurance"*
- AC 20-170 FAA Advisory Circular *"IMA Development, Verification, Integration and Approval Using RTCA/DO-297 and Technical Standard Order C153"*
- *DOT/FAA/AR-07/48"Handbook for Real-Time Operating Systems Integration and Component Integration Considerations in Integrated Modular Avionics Systems"*
- *"Using Model Checking for verification of Partitioning Properties in Integrated Modular Avionics"* Cofer, Engstrom and Weininger
- *"Certification Concerns with Integrated Modular Avionics (IMA) Projects"* Lewis and Rierson