Differences and Similarities in DO-178B Compliance in an IMA System vs a Federated Product

FAA National Software Conference

July 2005

Marty Gasiorowski

IMA Architecture has advantages

- Lower weight
- Lower wire count
- Possible generic PNs resulting in reduced spares
- Use of common components (OS, Middlewear) provides development benefits
- BUT...
- *Overall development effort should not be under-estimated*

Differences and Similarities in DO-178B Compliance in an IMA System vs a Federated Product

- "Processes for certifying complex integrated avionics systems is the Number 1 thing that must be addressed"

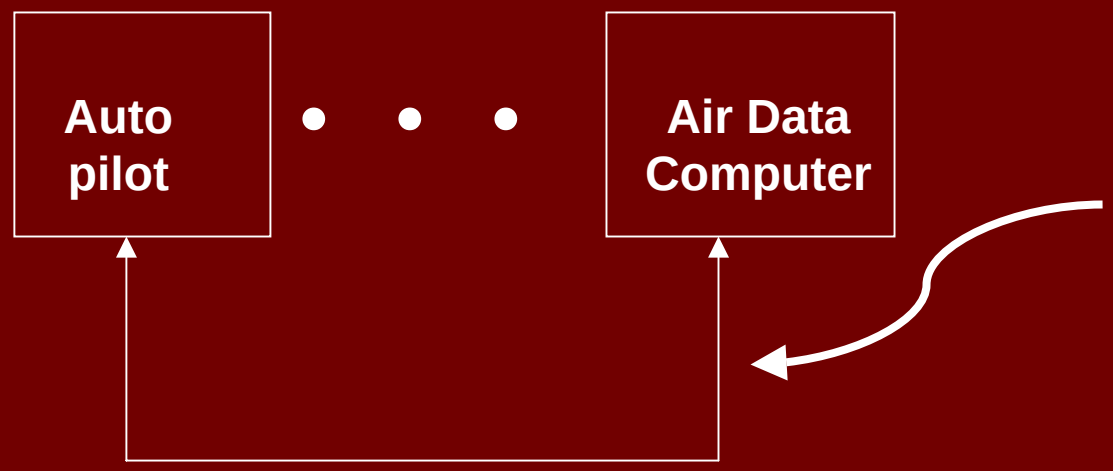
  - Nick Sabatini, FAA Associate Administrator for Aviation Safety, at International Aviation Safety Conference, June 9, 2005

Differences and Similarities in DO-178B Compliance in an IMA System vs a Federated Product

- "Current Processes (e.g. DO-178B) were developed with much simpler architectures in mind"
- "Numerous DO-178B work-arounds needed"

  - Ali Bahrami, Manager of FAA Transport Aircraft Directorate, in presentation on "Complex Integrated Avionics Systems and System Safety" at International Aviation Safety Conference, June 9, 2005 (see EASA web page for full presentation)

Previous Federated Architecture

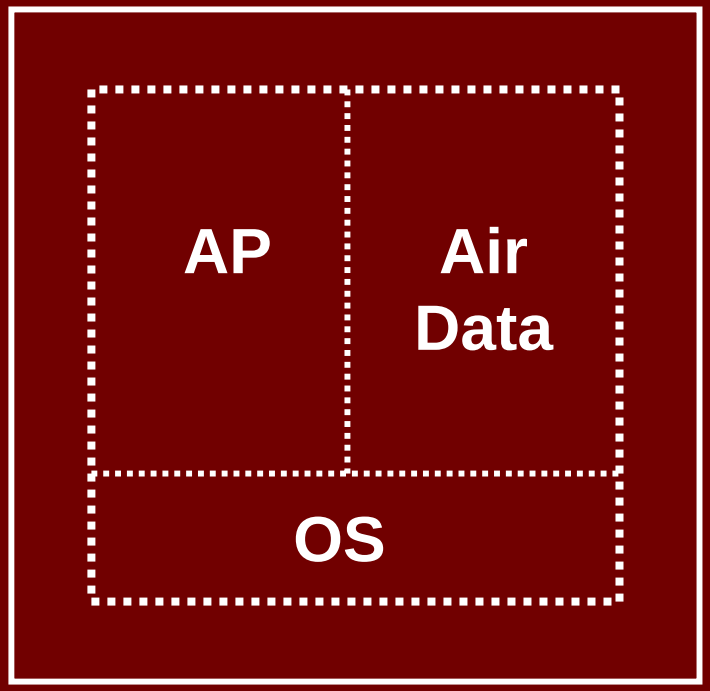


Interface is limited to single type (ie ARINC 429)

DO178B can be fully met by each component independently

One function can still provide “bad” data to the other, resulting in interface issues

Integrated Partitioned Architecture



Module

Integration introduces new interference possibilities:

- overwriting memory
- using too much CPU time

Integration also may provide multiple interfaces

- System bus
- Shared memory buffers

OS provides partitioning (“walls”) to eliminate these interference possibilities

Urban Myths

~~Urban~~ Myths

Suburban Myths

- The OS can take care of all partitioning
- ICDs are system documents
- Data tables are outside the scope of DO-178B
- Software Levels can be determined top-down from the FHA
- A Federated LRU doesn’t have the same partitioning, data/control coupling or interface issues as an IMA System
- An IMA System is more complex than a Federated System

Determining DALs

- Typically, the SW or HW Level of a component is determined “top down” from the FHA
  - A component involved in displaying Primary Attitude would need to be Level A, to comply with the FHA condition of Misleading Primary Attitude classified as Catastrophic
  - A component involved in controlling a Comm Radio would need to be Level C, to comply with the FHA condition of Loss of Comm classified as Major

This is typically adequate for Federated Systems

Determining DALs

- In an IMA System, the process starts the same, but there is an extra step if common components (OS, common hardware components, etc) are used in multiple functions
- A bottoms-up System FMEA is needed to determine if there are combinational failures that are collectively more severe than the individual failure conditions

There is a higher likelihood of potential Common Modes in an IMA System

Determining DALs

- Example:
  - An IMA Module hosts two unrelated functions
    - Flight Management System
    - IO between a controller and the Radios
  - Loss of either of these functions individually would probably be classified as Major
  - Loss of them collectively would at least be Hazardous
    - Common components, like an OS or the hardware platform, would need to meet a higher DAL than would be required for the individual functions

In IMA, two “Majors” may require a Level B

Spreading Objectives

- A component on an IMA Module normally cannot meet all DO-178B objectives by itself
- Objectives may need to be “delegated” from the OS to the Applications
- An individual objective (ie partitioning) may require contributions from multiple components to be met
- Objectives may need to be met at the software/software, hardware/software, and IMA system level

Establishing compliance in an IMA system may be more complex than in a Federated System

Spreading Objectives

- Assuming one PSAC per component, each PSAC needs to state which objectives will not be fully met at the component level
  - Assign to other components
  - Assign to integration activities

Establishing compliance in an IMA system may be more complex than in a Federated System

Data/Control Coupling & Partitioning

- Data & Control Coupling are not well covered in DO-178B
- Difference between D/C Coupling and Partitioning is not clear in DO-178B

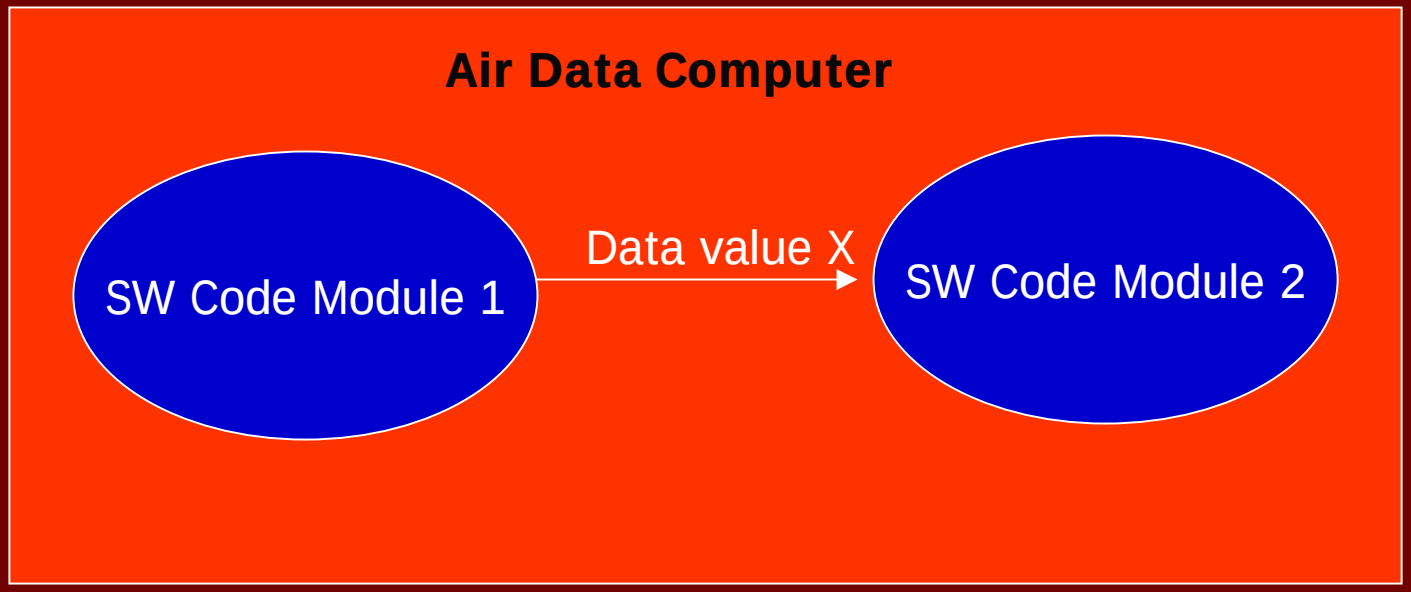
Whether Federated or IMA, D/C Coupling needs to be understood

D/C Coupling

- Data/Control Coupling included in DO-178B to ensure integrated software (as opposed to just code modules) is tested
- Intent was to verify interface between one code module and another, within a software function (ie within an Air Data Computer)
- Note that the D/C Objective calls out "test" rather than "verify"

This aspect of D/C Coupling applies equally to IMA or Federated Systems

DO-178B D/C Coupling



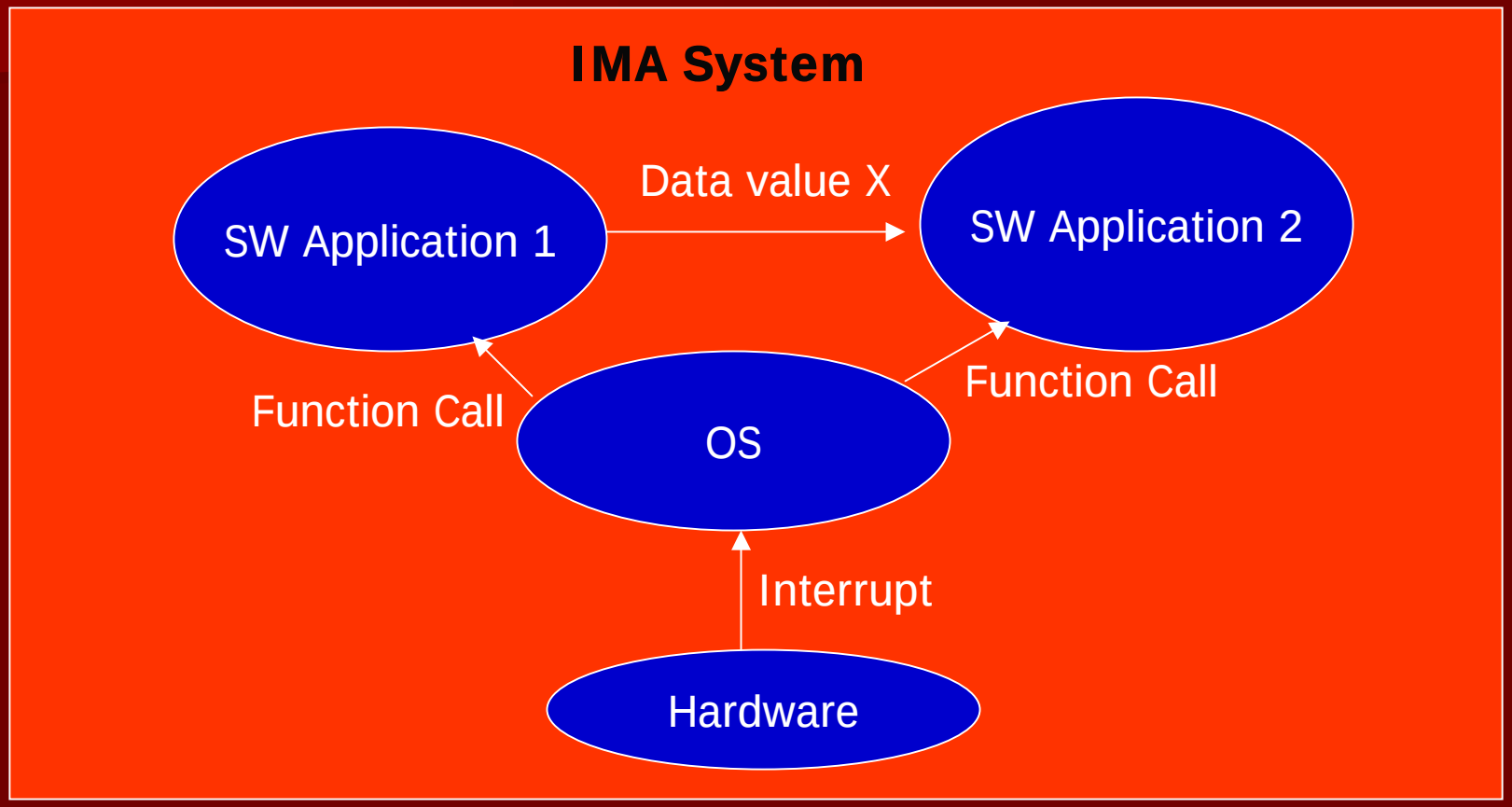
Per DO-178B Table A-7, Objective 8, Modules 1 and 2 must be tested together to verify data coupling

D/C Coupling

- In reality, whether a Federated or IMA System, D/C Coupling errors could be made between components at various levels
  - Between code modules within a sw function (ie application) – this is covered by DO-178B
  - Between one application and another
  - Between an application and the OS
  - Between software and hardware
  - Between components at the same DAL, or at different DALs

D/C Coupling have been looked at more closely in IMA, but they also apply to Federated Systems

D/C Coupling



In an IMA System, the quantity of D/C interfaces tends to be higher

D/C Coupling vs Partitioning

- If a component, by design, uses an input from a lower DAL component, and an error in the lower level component causes a higher criticality error by the higher level component, that is a data or control coupling error
  - Example – if a Level A Autopilot uses an input from a Level C Flight Management System, and the FMS has an error that causes the AP to operate incorrectly, then that is a Data Coupling problem, not a partitioning problem

Whether IMA or Federated, these intended interfaces must be addressed

D/C Coupling vs Partitioning

- If two unrelated components are on the same IMA module, and the lower DAL component interferes with the higher DAL component, that is a partitioning problem
  - Example – An IMA module hosts Level A Air Data and Level B GPS. The Air Data is not designed to use any data from the GPS. The GPS, however, has an error, that overwrites some of the Air Data's data. If the overwrite is not prevented, it is a partitioning violation

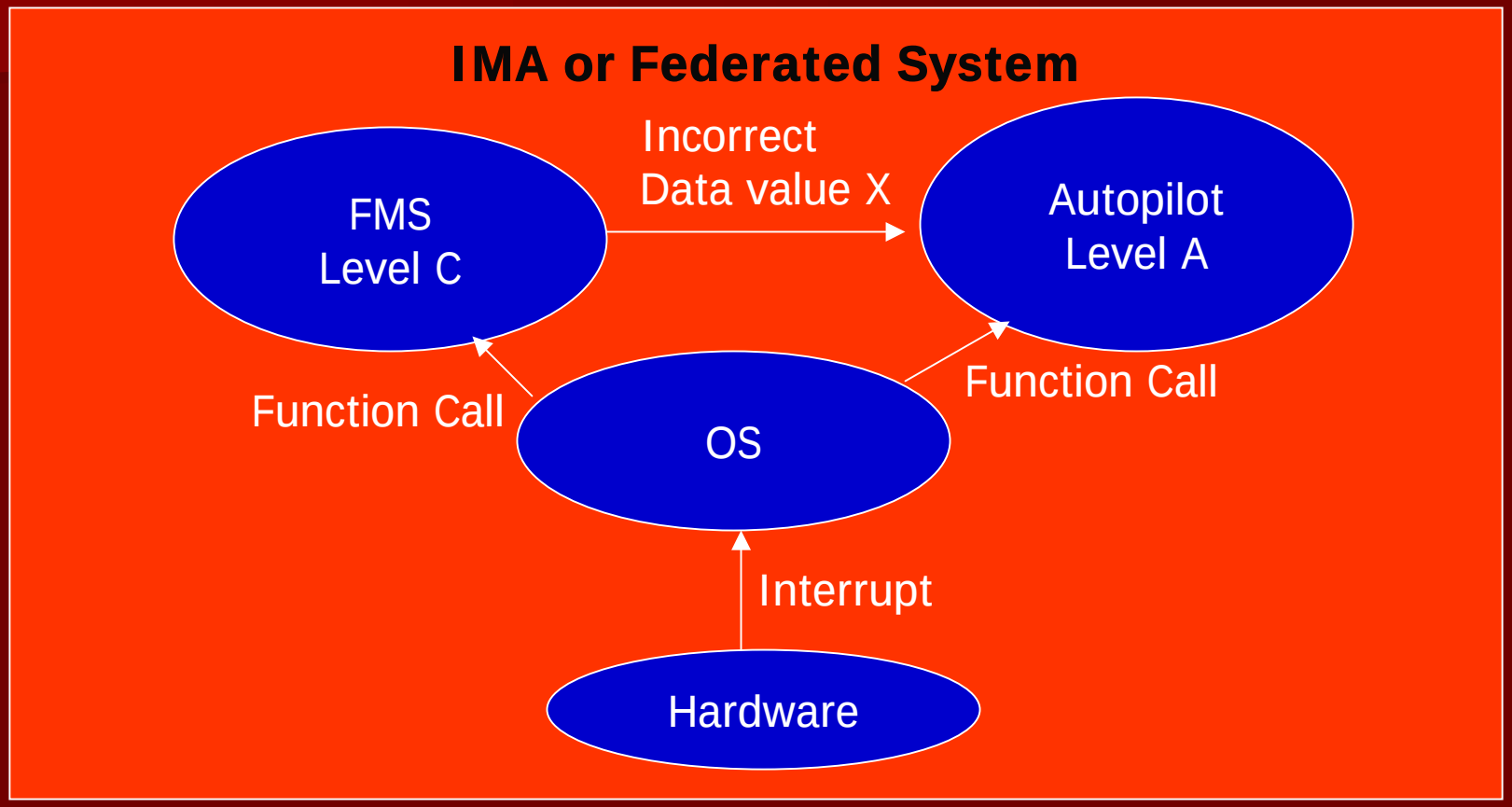
Partitioning is related to unintended interactions between components

D/C Coupling vs Partitioning

- The difference in the two cases is that in the D/C Coupling example, there was an intended interaction between the components
- In this case, there are several issues to address:
  - Is the interface defined and implemented correctly? – this is necessary whether the levels are the same or different
  - Are potential design errors in a lower DAL component accounted for in the higher DAL design? – this is only necessary if there is a difference in DALs
    - Note – hardware random failures would still need to be considered in this case

Unintended vs intended interaction is the key

D/C Coupling



Level C FMS sending incorrect data that causes incorrect AP operation – D/C Coupling

Data/Control Coupling

- DO-178B does not call out an ICD as a data item
- In an IMA System, there are several potential ways that two components could interact
- An ICD is one means that could be used to ensure that the interaction between the components are correctly defined and implemented
- Design and Code reviews should ensure that the use of data or control from other components is correctly implemented

Extra effort on interface definition in IMA

Data Tables/Registries

- IMA Systems often use data tables, registries or config files to customize the use of common components
  - Not DO-200A Databases
- Data Tables are not specifically covered by DO-178B, so they could be overlooked
- Not all DO-178B objectives necessarily apply to data tables
- The PSAC needs to identify the use of data tables, and define how they will be appropriately verified

Registries are not “software” but still must be verified

Customizing DO-178B Data Items for IMA

- Due to the spreading of objectives, the use of data tables, and the use of common components across modules in a system, it may not be “clean” to generate a PSAC, SAS and SCI per component that fully covers everything
  - This may also be true of other items, like SDP, SVP, Verification Report

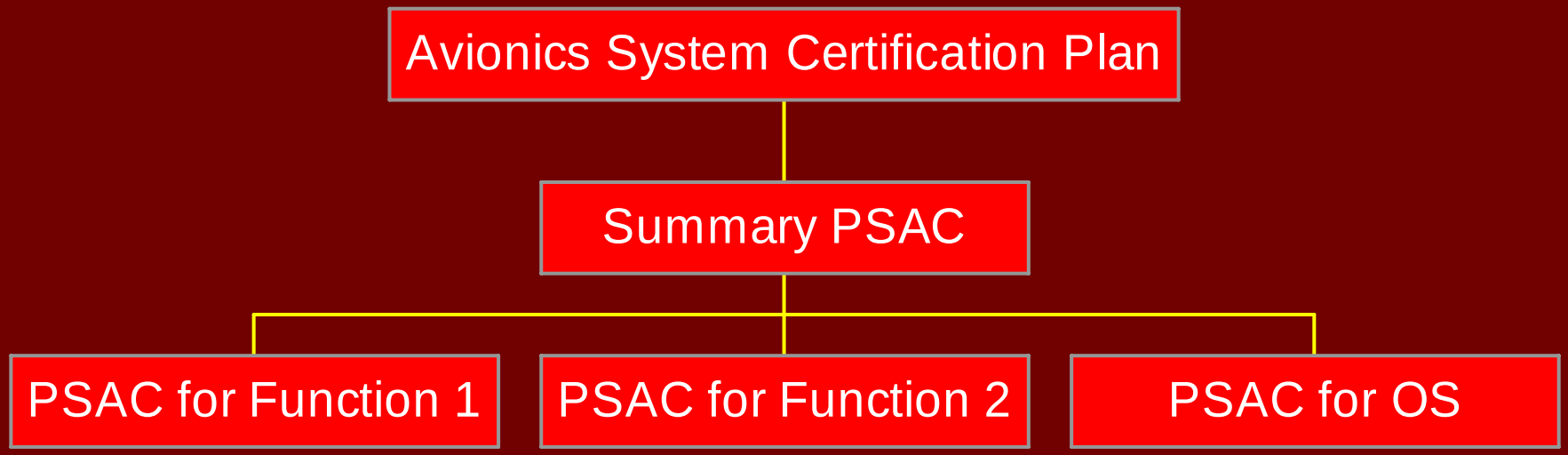
Innovative document structure may be needed

Customizing DO-178B Data Items for IMA

- Over-arching summary documents could be used to fill the gaps
  - Summary PSAC – covers the integration of all components, including data tables
  - Summary SAS
  - System Level SCI

One approach, but other approaches could work

Possible Document Structure for IMA



Conclusion

- IMA provides significant benefits to the aircraft, but it can present certification challenges
- Thought needs to go into the application of DO-178B to IMA Systems, to customize the development and verification processes in a way to ensure the IMA System meets the intent of DO-178B Objectives
- SC-205 needs to address IMA in generating DO-178C