Integrated Modular Avionics Approval Concerns

Presented to: FAA Software and Airborne Electronic Hardware Conference
By: Gregg Bartley ANM-111/AIR-20
Date: August 21, 2008
Introduction

• Complex IMA systems are becoming standard equipment on civil aircraft.
  – New technologies provide enhanced functionality, reduced costs (development and maintainability) and provides an architecture that easily accommodates hardware updates due to parts obsolescence.

• Each new aircraft program introduces increased capability and complexity of IMA architectures, while maintaining or shortening the time allowed for approval.
• The increased capability and complexity of IMA systems result in new concerns regarding approval of these systems.
Overview of Approval Concerns Regarding Complex IMA Systems

- Lack of integrated and cohesive FAA policy and guidance specific to IMA systems.
- Distributed IMA design responsibility.
- Unintended operation under non-normal and failure conditions.
- Erroneous assumptions regarding robust partitioning.
- Use of Technical Standard Orders for approval of complex IMA systems.
Lack of Integrated and Cohesive FAA Policy and Guidance Specific to IMA Systems

• There are published regulations, policy, advisory material and industry standards that apply to the approval of complex IMA systems.

• However, as many of these are not dedicated to IMA’s, there is some confusion about which ones actually apply, how they may be used with each other, what needs to occur if the specific system issues are not addressed by the existing material, etc.
Lack of Integrated and Cohesive FAA Policy and Guidance Specific to IMA Systems

• Existing FAA Regulations
  – Title 14 Code of Federal Regulations (14 CFR), §§ XX.1301 and XX.1309
  – Specific regulations, such as:
    • §23.1303, flight and navigation instruments for normal, utility, acrobatic and commuter category airplanes
    • §25.1329, flight guidance systems for transport category airplanes
    • §29.143, controllability and maneuverability for transport category rotorcraft
Lack of Integrated and Cohesive FAA Policy and Guidance Specific to IMA Systems

• FAA Policy
  – Order 8150.1B, Technical Standard Order Program
  – Notice N 8150.5, Non-TSO functions (expires Sept. 28, 2008)
  – Order 8110.49, Software Approval Guidelines
  – Order 8110.105, Simple and Complex Electronic Hardware Approval Guidance
  – TSO C-153, Integrated Modular Avionics Hardware Elements
Lack of Integrated and Cohesive FAA Policy and Guidance Specific to IMA Systems

• FAA Guidance
  – AC 23.1309-1, Equipment, Systems and Installation in Part 23 Aircraft
  – AC 25.1309-Arsenal Version, System Design and Analysis (Draft, not currently released)
  – AC 27-1, Certification of Normal Category Rotorcraft
  – AC 29-1, Certification of Transport Category Rotorcraft
  – AC 20-145, Guidance for Integrated Modular Avionics (IMA) that implement TSO C-153 Authorized Hardware Elements
  – AC 20-148, Reusable Software Components
Lack of Integrated and Cohesive FAA Policy and Guidance Specific to IMA Systems

• Industry Documents
  – SAE ARP 4754, Certification Concerns for Highly Integrated or Complex Aircraft Systems
  – SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
  – RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification
  – RTCA/D0-254, Design Assurance Guidance for Airborne Electronic Hardware
  – ARINC 653, Avionics Application Standard Software Interface
Lack of Integrated and Cohesive FAA Policy and Guidance Specific to IMA Systems

• The FAA is working toward resolving this issue. Possible future actions include:
  – New IMA policy.
  – New AC invoking RTCA/DO-297 as an acceptable means of compliance.
    • Many issues need to be understood and resolved, e.g., incremental acceptance.
  – Update AC 20-145.

• This process will take some time.
Distributed IMA Design Responsibility

• Many business models for IMA development and approval involve multiple companies (some international).
  – Aircraft certification applicant
  – IMA supplier/integrator
  – Individual IMA function/component suppliers
  – Sub-tier suppliers of hardware components, software verification, etc.

• This may necessitate the involvement of multiple Certification Authority offices.
Distributed IMA Design Responsibility

• Complex IMA systems, by their very nature, require close attention to detail:
  – Integrating IMA components into IMA shared resources
  – Integrating IMA partition to partition
  – Integrating IMA functions to functions
  – Integrating IMA system into aircraft
  – Human factors evaluations, crew alerting, safety analyses, etc.

• Yet, the very nature of the compartmentalized approach to IMA design makes it easy for necessary integration testing and analyses to be overlooked.
Distributed IMA Design Responsibility

• Applicant and IMA system integrator must:
  – Plan for all activity necessary to show compliance to all appropriate regulations, policy, guidance material, at the beginning of the program.
  – Schedule adequate time for such activities.
  – Ensure that the plans are being followed.
  – Ensure that there are few roadblocks to open communication between the various parties involved in the IMA project.
  – Coordinate early and often with FAA on new/novel designs, emerging issues and the proposed means of gaining approval.
  – Ensure that when schedule pressures start to mount, the required integration activities do not suffer as a result.
Unintended Operation under Non-Normal and Failure Conditions

- Cascading failures can occur in complex IMA systems as a result of data sharing between functions or partitions.
- The problem of cascading failures is not new to complex IMA systems. However, it is made much more complex and difficult to analyze due to:
  - The massive amount of data exchanged between modern avionics systems, functions and IMA partitions.
  - The complexity of the IMA system architecture.
  - The “piecemeal” approach to IMA design described earlier.
  - The data exchanged between functions or partitions may lead to interactions between functions and partitions that were not present in the first and second generation airborne digital avionics systems.
  - Schedule pressures.
Unintended Operation under Non-Normal and Failure Conditions

SIMPLIFIED EXAMPLE

- Shared resource in IMA-L fails, affecting Function A – Left.
- Function B comparison of Parameters XYZ – L and R now invalid.
- Parameter ABC output from Function B invalid.
- Sub-function of Function C cannot operate as designed without valid Parameter ABC.
- Crew Alert – Function C sub-function inoperative.
Unintended Operation under Non-Normal and Failure Conditions

• The example on the previous slide illustrates:
  – A primary failure that affects Function A – Left.
    • Function A – Right is still operative and therefore, Function A, overall, only suffers a loss of redundancy.
  – Secondary failures, also known as Cascading Failures, of both Functions B and C.
    • The overall effect of the secondary failure on Function B is negligible.
    • The secondary effect of Function C, however, results in a Crew Alert.
Unintended Operation under Non-Normal and Failure Conditions

• Great care and expertise must be utilized when analyzing fault conditions in complex IMA systems.
  – Failure analyses must be able to cross system and functional boundaries.
  – Dependencies may exist between systems and functions that did not historically exist.
  – These dependencies, for any particular failure mode, may not stop with the first shared data path but will, most likely, extend through multiple “links in a chain”.
Erroneous Assumptions Regarding Robust Partitioning

True or False?

“Robust partitioning, such as described in ARINC 653, when implemented in a complex IMA system architecture, will ensure that changes made to one partition will not adversely affect another partition.”
Erroneous Assumptions Regarding Robust Partitioning

FALSE!!

• Robust partitioning will ensure that changes to one partition will not expose other partitions to the potential hazards of data coupling, as defined in RTCA/DO-178B, paragraph 2.3.1 a., such as “shared or overlaying data, including stacks and processor registers”, i.e., having to do with IMA shared resources.

• Robust partitioning will not ensure that a functional partition is absolutely protected from changes to another functional partition, if those partitions exchange data.
Erroneous Assumptions Regarding Robust Partitioning

Follow Up Question:

“If the data exchanged between functional partitions is defined and captured in an Interface Control Drawing (ICD), doesn’t it then follow that, if the ICD does not need to change, then functional partitions using data produced by the revised partition cannot be adversely affected by that change?”
Erroneous Assumptions Regarding Robust Partitioning

Again, FALSE!!

• Several technical aspects of data computed by one partition/function for use by other partitions/functions can be affected without requiring a change to an ICD.
  – How the variable or parameter is computed.
  – Under what conditions it will become invalid.

• Changes of these types can be vitally important to the systems using the data! This type of change to the Source System may need to be flowed back to the Using System’s safety assessment process.
Erroneous Assumptions Regarding Robust Partitioning

- The applicant and IMA integrator should not become overly-dependent on robust partitioning. They must understand what protections robust partitioning does and does not provide.

- A rigorous Change Impact Analysis (CIA) process must be defined and used, when appropriate, to assess possible cross-functional impacts, even when the IMA system is robustly partitioned.

- The CIA must be able to:
  - Assess the possible cross-partition impacts in depth.
  - Must be able to assess the possible cascading effects if failure conditions are an issue.
Use of Technical Standard Orders for Approval of Complex IMA Systems

• Technical Standard Orders (TSO) are authorized by 14 CFR, Part 21, Subpart O.
  – TSO’s have existed since the 1950’s.
• Quick summary of important TSO points.
  1. A TSO is the minimum performance standard for an article designed for use on civil aircraft. It constitutes a “mini-TC”.
  2. A TSO deals with an article, independent of any aircraft.
  3. Only a selected list of articles has an associated TSO.
  4. Unless an applicant doesn’t submit what the FAA requires, the FAA has just 30 days to approve or deny the TSO Authorization application.
  5. Neither a TSO nor a TSO Authorization allows for installation of the article. A separate approval is needed to use the article on the aircraft.
  6. Just because an article meets a TSO, it doesn’t mean it’s safe to use in any environment. Installation requirements may be more rigorous than the TSO.
Use of Technical Standard Orders for Approval of Complex IMA Systems

• There are several issues that make approving IMA’s via TSO problematic.
  – There isn’t an IMA system TSO.
    • Therefore, no TSO system Minimum Performance Specification.
  – The boundary between IMA system approval and IMA installation approval can be vague.
    • Human factors evaluations
    • Safety assessment activity
    • Aircraft design considerations, such as electrical power sources and separation, reset of individual functions, configuration control of updated IMA components, etc.
Use of Technical Standard Orders for Approval of Complex IMA Systems

• There are several issues that make approving IMA’s via TSO problematic (continued).
  – IMA approval requires several “layers” of integration (module, function, IMA system) activity.
  – IMA systems are very complex and, taken as an entire integrated system, cannot be evaluated, in their entirety, separately from the aircraft in which they are to be installed.
  • Remember that TSO approvals apply to articles that are independent of any aircraft.
Use of Technical Standard Orders for Approval of Complex IMA Systems

• Aircraft Certification Program Issue Papers are NOT applied against an article seeking TSO authorization.
  – There will, most likely, be many issue papers that will be applicable to the complex IMA system (e.g., software model based development, use of a COTS operating system) as well as the functions hosted by the IMA (e.g., display of critical data in unusual operating conditions, autoland performance validation)
Use of Technical Standard Orders for Approval of Complex IMA Systems

• All of these factors make it very difficult to understand what IMA approval activity has been done via TSO and what remains to be done via the aircraft certification program.
  – Must be documented during the planning stages of the certification program. All parties involved in the IMA development, verification and approval must understand what is expected of them. This item cannot be postponed until TSO Approval.
Use of Technical Standard Orders for Approval of Complex IMA Systems

• How have TSO’s been utilized to approve complex IMA systems?
  – TSO C-153, for generic hardware computing modules, data concentrator units, power supplies and unpopulated racks.
  – The compiled list of all individual TSO’s that contain specifications for the functions that the final IMA system will perform.
    • e.g., TSO-C113, Airborne Multi-Purpose Electronic Displays; TSO-C2d, Airspeed Instruments; TSO-C31d, High Frequency (HF) Radio Communications Transmitting Equipment.
  – Non-TSO Functions, as defined in Notice N 8150.5.
  – Incomplete TSO, as defined in Order 8150.1.
  – “Functional” TSO, as defined in AC 20-145.
    • Software only, to be loaded into TSO C-153 approved IMA hardware at some later time.
Use of Technical Standard Orders for Approval of Complex IMA Systems

• This process is not strictly supported by current FAA policy.
  – It is confusing and has been applied unevenly.

• It is strongly suggested that IMA approval be done via the aircraft certification program activity (i.e., TC, STC, ATC, ASTC).

• After aircraft installation approval, the FAA ACO responsible for TSO approval, based on aircraft certification program, can issue TSO Authorization(s) concurrently or afterwards.
FAA plan for addressing approval of complex IMA systems

• Plan is currently in work and is, therefore, still TBD.
• The FAA needs a complete, coherent and consistent approach to approving complex IMA systems that uses elements already in place.
• To this end, the FAA is considering:
  – New FAA policy (i.e., an Order) on approval of IMA systems, including the use of TSO’s.
  – AC 20-IMA, which will invoke all or parts of RTCA/DO-297, and include additional information.
  – Update AC 20-145.
    • Remove all IMA system level considerations and put in AC 20-IMA.
    • Will give AMOC to gain TSO approval for TSO C-153 hardware components only.
  – Update Order 8150.1B, Technical Standard Order Program (currently in work).
Summary

• FAA regulations, policy and advisory material are struggling to keep up with the rapid pace of change in IMA technology.

• The advances in IMA technology are making it increasingly difficult to ensure compliance to all applicable regulations and advisory material.

• Applicants and IMA suppliers must:
  – Plan all required activities.
  – Follow the plans.
  – Work with the FAA early and often.
Caveat!!

- The information in this presentation represents the current thinking within the FAA. The information in this presentation is not intended to commit the FAA to any particular course of action on the issues discussed. It is intended solely as a method of keeping both industry and other regulatory authorities up to date.
Questions?