CERTIFICATION CONCERNS OF INTEGRATED MODULAR AVIONICS (IMA) SYSTEMS

Gregg Bartley and Barbara Lingberg, Federal Aviation Administration (FAA), Washington, D.C.

Abstract

The pace of technological advances in the area of Integrated Modular Avionics (IMA) is progressing at a breakneck speed. The FAA is concerned that the complexity of these IMA systems and the interaction between their functions is not well understood, especially under failure conditions. Additionally, given the developing business models used by industry, it is likely that large-scale IMA systems will be developed and integrated by multiple companies. Given the system complexity and aggressive approval schedules, it is extremely difficult to ensure that all aspects of the IMA system have been fully covered during the approval for use on an aircraft.

From the FAA perspective, IMA systems are not fundamentally different in nature from more traditional, usually simpler, federated systems. The existing regulations, policy and guidance material that apply to federated systems also apply to IMA systems. What has changed, however, is the complexity of these systems, the possibility of unintended interaction between the individual functions of these systems, and the number of companies that develop components of the IMA system. This requires a high level of care and attention to detail to ensure that the final IMA system is safe and is compliant with, not only the specific existing regulations and guidance material, but also the intent behind the regulations and guidance in the event that they do not adequately cover the proposed IMA design.

This paper explores some of the issues and concerns surrounding the approval of large scale integrated modular avionics systems.

Existing Material Available for Integrated Modular Avionics (IMA) Development and Approval

A number of current regulations, policy, guidance, and industry standards may apply to the development and approval of complex IMA systems. These include the following:

FAA Regulations

Additionally, many regulations that apply to specific systems or functions are also applicable to the IMA system that hosts those systems or functions. Examples include §23.1303, flight and navigation instruments for normal, utility, acrobatic and commuter category airplanes; §25.1329, flight guidance systems for transport category airplanes; and §29.143, controllability and maneuverability for transport category rotorcraft.

**FAA Policy**
- Order 8150.1B, Technical Standard Order Program
- Notice N 8150.5, Non-TSO functions
- Order 8110.49, Software Approval Guidelines
- Order 8110.105, Simple and Complex Electronic Hardware Approval Guidance
- TSO C-153, Integrated Modular Avionics Hardware Elements

**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

**Industry Documents**
- SAE APR 4754, Certification Concerns for Highly Integrated or Complex Aircraft Systems
- SAE APR 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/DO-254, Design Assurance Guidance for Airborne Electronic Hardware
- ARINC 653, Avionics Application Standard Software Interface

### Overview of Certification Concerns Regarding Complex IMA Systems

The FAA has concerns regarding several aspects of how IMA systems are developed and approved.

- 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.

---

1. XX refers to the specific Parts within 14 CFR that are applicable to the different aircraft types, i.e., Part 23 for Normal, Utility, Acrobatic and Commuter category Airplanes, 25 for Transport Category Aircraft, 27 for Normal Category Rotorcraft and 29 for Transport Category Rotorcraft.
2. Not officially released, but referred to and applied to many Part 25 projects by issue paper.
3. Currently undergoing update in committee
4. Currently undergoing update in committee
5. Currently undergoing update in committee
6. Not currently recognized by FAA as an acceptable means of compliance. AC is currently in work.
• Erroneous assumptions regarding robust partitioning.
• Use of Technical Standard Orders for approval of complex IMA systems.

Each of these subjects is explored further in the following sections.

**Lack of Integrated and Cohesive FAA Policy and Guidance Specific to IMA Systems**

As noted at the beginning of this paper, a large body of material exists in the form of FAA regulations, policy and guidance as well as several industry documents, that is relevant and applicable to the development and approval of complex IMA systems. However, much of this material is not specific to IMA systems. Consequently, some of this material may be confusing as to how it might be applied to IMA systems. Also, the material is dispersed across many different sources and documents, such as RTCA/DO-297, that are not yet officially recognized by the FAA as an acceptable means of compliance to the regulations. Finally, the material may not always be harmonized (e.g., RTCA/DO-297 vs. AC 20-145), so it is unclear as to what is expected from the IMA developer.

These issues make the development and approval of complex IMA systems problematic for both the IMA developer and the FAA. The IMA developers may not have a good understanding of how the various material listed above might be applied, or even if it does apply to their specific development program. The FAA faces a similar dilemma. They may have a difficult time determining how to apply this material to any specific program and to apply this material consistently across different programs.

The FAA is in the process of addressing these issues. However, as with all new policy or guidance material, this process takes time.

**Distributed IMA Design Responsibility**

Documents such as AC 20-145 and RTCA/DO-297 address the design and verification activities that must occur during the integration phase of an IMA development program. However, due to the fragmented nature of IMA designs and the scale of an IMA project, there is a danger that many necessary design considerations and required integration activities may actually be inadvertently omitted. Additionally, for the same reasons, these omissions may not be detected by the IMA integrator, applicant or FAA personnel assigned to the project during final approval of the IMA system.

Each IMA system is unique, in that a system as complex as an IMA must be designed to fulfill the exact needs of each aircraft in which it will be installed. This is a true statement even though an IMA design might be built around generic “core” hardware and software components that can be adapted or modified to fit into unique IMA system installations. The final IMA system must, in all likelihood, be specifically designed or modified to fit a unique aircraft installation.

An IMA system may contain very limited functionality (e.g., radios and displays), or it may host a large majority of the avionics functions required by the aircraft. At both ends of the complexity spectrum, specific engineering and design expertise is required to produce the complete IMA system. For example, a design group whose expertise lies in developing Flight Management systems would not normally be assigned responsibility to develop a software operating system capable of hosting multiple functions while providing robust partitioning. Engineering and design groups are specialized and are normally assigned work only in their area of expertise.

Due to the scope and diversity of the IMA project, many different design groups with their own areas of expertise will be involved. These various design groups may all be part of the same company. However, due to economic incentives and the availability of very specialized avionics suppliers available across the globe, it is just as likely that many different companies, possibly in several different countries, will be involved in the development, verification and integration activities of an IMA system.

Distributing the design responsibilities for complex IMA systems has obvious advantages, both technically and economically. However,
distributed responsibilities also have a significant downside; no single entity “owns” or understands completely all the various functions contained in an IMA system. This makes it increasingly difficult to analyze and test the IMA system for unexpected interactions between functions, especially under failure conditions.

Unless this type of activity is planned for and forced to occur by the IMA system integrator and/or applicant of an aircraft certification program (i.e., Type Certification (TC), Supplemental TC (STC), Amended TC (ATC), Amended Supplemental TC (ASTC)), there is a danger of that many tasks required to approve an IMA system may “fall through the cracks.” The various design groups and companies will tend to concentrate on getting the functions they are directly responsible for operating correctly per the schedule. Integration issues and activities can become, very easily, a secondary concern. An additional complication is that communications between the developers of the various IMA functions may be made more difficult when the developers are normally aggressive competitors in other areas. The formal lines of communication are normally through the IMA system integrator, not between individual functional designers or even companies responsible for supplying the IMA functions.

All of these issues can be seen as impediments to quickly identifying and resolving problems that may occur across functional boundaries. These issues demonstrate the need for the IMA system integrator to plan all required integration activity at the beginning of the project and to ensure that it does indeed occur. The required integration activity for complex IMA systems can be very involved and will require time and attention to technical details that cross many functional boundaries. This integration activity must be planned for and given the appropriate level of resources (e.g., manpower, schedule time). When time and costs start becoming critical during the final stages of a certification program, required integration activities may be the first thing to suffer neglect. This is not due to deliberate malfeasance or lack of interest on the part of any individual or company. The most likely reason is that, in the final rush to finish the design and complete all milestones as required by the aircraft certification program, some items may be overlooked or given only a cursory “once-over.”

Unfortunately, when all the required integration testing and analysis does not occur, it may not be obvious that it has been missed. When all functions are working correctly, there are no downstream secondary failure effects (which are discussed later in this paper) to be seen. In fact, it may take several failures of a very particular nature before any of these secondary effects manifest themselves. If all functions hosted by an IMA system appear to be working correctly and the aircraft program has achieved certification, there is little incentive for anyone to go back and examine if any integration activity of the IMA system has been missed.

Unintended Operation under Non-Normal and Failure Conditions

As noted previously, the complexity of IMA systems, compared to previous generations of airborne avionics equipment, has increased dramatically. Functions that have historically been hosted in relatively self-contained, federated systems now reside in highly integrated systems that share many resources, such as computing, I/O, power, etc. IMA systems provide many benefits, such as decreased weight, more open systems that can be updated more easily and lower overall power consumption. However, they also contain potential pitfalls of which the functional developers and IMA system integrator must be aware and take extreme care to avoid.

Primary and Secondary Failure Effects

One obvious difference between IMA systems and the previous generation of simpler federated systems is that failures of the IMA infrastructure will affect all systems that make use that shared resource. Failure of a shared resource will result in the failure, partial failure or loss of redundancy of all functions that make direct use that shared resource. These affected functions are the primary effects caused by the failed resource. Primary effects of a failed resource should be relatively simple to determine by analysis and/or testing. Of equal importance but, in many cases, more difficult to determine are the secondary effects caused by the failed resource.
Secondary effects (also referred to as “cascading failures”) of failed shared resources are usually caused by a data dependency between a function that does not make direct use of the component that suffered the failure and a function that suffers the direct effect of the failure. To make matters even more complex, this data dependency may have multiple links in the chain such that multiple functions are involved. A simplified example of this is as described below.

Figure 1 shows that Function A is hosted in two independent IMA cabinets, left and right. Function A suffers a loss of redundancy when the computing module in one of the IMA cabinets that hosts Function A fails. As a result, parameter xyz-left from that function is no longer calculated by the left version of Function A. Function B uses both parameters xyz-left and xyz-right, which are calculated by multiple version of Function A that are hosted in different computing modules.

In order to maintain the integrity required for the function it performs, Function B must compare the two independent versions, left and right, of the same parameter xyz. Function B, for the purpose of signal integrity, cannot use parameter xyz if it does not have two valid signals to compare to against each other. If this occurs, parameter abc from Function B becomes invalid. Function C, which uses parameter abc as input for several of its calculations, can no longer fulfill all the tasks it normally performs. As a result, Function C, as designed, puts up a Flight Deck Effect to annunciate that it is no longer able to perform any of its intended functions.

It is acknowledged that this very simplified scenario is rather unrealistic. Actual aircraft systems would have additional redundancy and robustness built in that would achieve the necessary integrity and availability for all systems involved. However, the example can be used to demonstrate the concept of primary and secondary failure effects. One conclusion that can be made is that secondary effects caused by failure of shared resources may not be immediately obvious without some level of detailed, cross functional analysis.

The loss of redundancy of Function A is the primary effect of the failure. It can be seen that both Function B and Function C suffer secondary effects. Function B only suffers an impact on one of its output parameters. However, Function C actually suffers a loss of function failure due to the cascading faults initially caused by the failure of a shared resource for Function A.

This type of cascading failure condition is certainly not unique to IMA systems. Simpler, federated architectures suffered from this same problem. However, what is different is that these systems are much more complex and provide many additional functions and features than did the first generation of digital avionics systems. Therefore, the potential interaction between these functions and systems may be many times greater than with the simpler, federated systems. The result of this increase in complexity is that many cascading failure effects may no longer be obvious.

Several of the documents referenced in the beginning of this paper address how to do the safety assessment process for complex systems. SAE documents APR 4754, Section 6 and ARP 4761,
Section 3 are both dedicated to the Safety Assessment Process. Section 4 of ARP 4761, along with several of its appendices, discuss safety assessment analysis methods in great detail. RTCA DO-297, Section 5.1.5 is also dedicated to Safety Assessment Activities. Therefore, the FAA believes that adequate information is available to assist an IMA developer in making a comprehensive safety assessment, including a failure analysis, of a very complex IMA system. However, even with extreme care and diligence on the part of the suppliers of complex digital avionics systems, several complex avionics systems currently in service (not necessarily IMA architectures) have experienced some very unusual and unexpected problems during failure conditions.

The reasons behind these problems are varied and complex, and it is difficult to make any generalized conclusions as to why these failure conditions were not discovered during initial development and verification of these systems. The similarity between the events is that they were all unexpected and resulted in serious events while the aircraft was in flight that required the flight crew to take action to mitigate the effects of the failure condition. These events illustrate why the failure modes of these complex systems, including IMA systems, be well understood before they are put into service.

**Large Number of Possible Interacting Failure Effects for Multiple Failure Conditions.**

As stated in the preceding discussion, the large number of very complex aircraft functions hosted by an IMA system and on other systems with which the IMA interfaces makes unexpected interactions between these functions sometimes difficult to predict by analysis. The complexity of the functionality provided by these latest generation of systems is much greater than the first generation digital systems. This increase in the complexity of functions requires, by necessity, more and more data to be exchanged between various functions. This increase in data interfaces between what otherwise might be unrelated functions may create new dependencies among them that may not have been present in first generation digital avionics systems.

Analyzing the IMA system and the systems which with it interfaces for primary and secondary effects is a challenging and possibly daunting task. Analyzing the system for primary failure effects even under multiple failure conditions still should remain relatively straightforward. Single secondary effects resulting from the primary failure may also be relatively benign by themselves. However, when coupled with other primary and the increased number of secondary effects resulting from the same failure, the interactions between these various failure effects may end up being critical from a safety assessment perspective, but also may be very difficult to analyze.

The importance of understanding the interaction of failure conditions cannot be overstated. Aircraft systems are designed and built such that serious single failure conditions are mitigated in some manner. A study of the accidents and serious incident in the history of aviation reveals that a large percentage of them involved multiple failure conditions (sometimes exacerbated by incorrect flight crew action). This same conclusion can be reached by careful study of non-aviation related accidents, such as the Three Mile Island nuclear plant Unit #2 in 1978 and the release of deadly gas in 1984 at the Union Carbide chemical plant in Bhopal, India.[1]

These events, both within the aviation industry and outside of it, demonstrate the importance of understanding how multiple faults within very complex systems may interact to produce unexpected results.

**Erroneous Assumptions Regarding Robust Partitioning**

One of the FAA’s concerns regarding the design and approval of complex IMA systems is that there may be several incorrect assumptions regarding robust partitioning. While robust partitioning does provide many important benefits, overconfidence in this design approach could result in a compromised IMA architecture.

**Benefits of Robust Partitioning**

Robust partitioning between functions that share computing resources within an IMA is discussed in many of the referenced documents at
the beginning of this paper, including AC 20-145, RTCA/DO-297, RTCA/DO-178B and SAE ARP 4754. Robust partitioning is considered an essential feature of a complex IMA system. In a robustly partitioned system, a failure or incorrect operation in one partition will not adversely impact a different partition by affecting the IMA resources shared by the two partitions. Additionally, dividing functions between different partitions allows the designer to develop the IMA hardware and software components to different assurance levels. Partitions of lesser criticality may be developed to a lesser design assurance level than the partitions of higher criticality but still reside within the same system and use the same shared resources.

It is not the intent of this paper to discuss in depth the philosophy or implementation of a robustly partitioned system. The reader is referred to the documents referenced above for the details regarding partitioning.

**Data and Control Coupling**

A misconception regarding robust partitioning is that coupling between functions of a partitioned IMA system is either minimized or completely absent. That is, to a certain degree, a true statement. However, there are instances where this is not true. To analyze this further, we must first define coupling in the context of IMA partitions.

RTCA/DO-178B defines two different types of coupling possible between software components; data coupling and control coupling [2]

**Data Coupling** – The dependence of a software component on data not exclusively under the control of that software component.

**Control Coupling** – The manner or degree by which one software component influences the execution of another software component.

Robust partitioning schemes, such as defined by ARINC 653, successfully deal with coupling issues that involve use of resources that are shared by the various partitions within a partitioned system, such as “shared or overlaying data, including stacks and processor registers”. [2] By using robust partitioning, the potentially harmful aspects of data coupling associated with the use of shared IMA resources are minimized or eliminated entirely.

However, there exists a different type of data coupling beyond that which involves resources shared between partitions. This coupling occurs when a function hosted in one partition uses data computed by a function in a different partition. Sharing large amounts of data between functions is a vital and required aspect of complex avionics systems. The more data that is shared between functions/partitions, the more opportunities exist for the creation of data dependencies between the functions of different partitions. The cascading fault scenario shown in Figure 1 of this paper demonstrates the mechanism of data coupling between partitions.

**Change Impact Analysis**

The fact that an IMA system is robustly partitioned does not alleviate the need to understand the dependencies and possible cascading failure effects discussed in this paper. For this reason, robustly partitioned systems still must be subjected to the rigorous Change Impact Analysis discussed in Order 8110.49, Chapter 11.

Although the FAA does not have a firm understanding of how widespread this practice is, one approach apparently used by industry to assess whether a cross-functional Change Impact Analysis is needed is by determining if an Interface Control Document (ICD) revision is needed to support that change. Another way of stating this is the following. If an ICD revision is not necessary for any particular change to a function/partition, then a cross-function/partition Change Impact Analysis is also not necessary. The premise behind this approach is that the different functions are isolated from each other by robust partitioning and can only communicate via a very defined and specific mechanism that minimizes data and control coupling between partitions. Therefore, it is felt, if a change to a certain function does not require a change to the ICD, which defines the output parameters from that function, then, by definition, the functions using those parameters cannot be impacted by the change.

This is a false assumption, as the discussion below will attempt to demonstrate.
“Flaps Extended” Example

Figure 2 shows the interface between the Flaps System Controller and a defined user of data transmitted by that controller. Two bits of the Flap System Discrete Word shown are defined as the FLAPS EXTENDED variable. What the ICD entry does not tell the user is the exact technical definition of “Flaps Extended”. Without further definition, a True state of the FLAPS EXTENDED discrete could possibly mean any of the following:

Both left and right trailing edge flap surfaces detected in the “1” or greater flap detent.
Both left and right trailing edge flap surfaces detected not in the “Up” flap detent.
Flap Lever Handle detected in the “1” or greater flap handle detent.
Flap Lever Handle detected not in the “Up” flap handle detent.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid</td>
<td>00</td>
</tr>
<tr>
<td>Flaps Ext</td>
<td>01</td>
</tr>
<tr>
<td>Flaps Not Ext</td>
<td>10</td>
</tr>
<tr>
<td>Not Used</td>
<td>11</td>
</tr>
</tbody>
</table>

Figure 2. Flaps Extended Discrete Data Transmission

All four of these possibilities have differing characteristics from each other that might be vitally important to functions that use that discrete. For example, once the trailing edge flaps begin to move, the logic that determines “flaps not in the Up position” will be satisfied almost immediately. In contrast, the flaps may take five to ten seconds to fully reach the “flaps detected in the ‘1’ detent” position. Additionally, the FLAPS EXTENDED discrete may also exhibit significantly different characteristics during failure conditions. If the flap surfaces will not respond to a valid command due to a hydraulic system failure, the flap lever position will no longer reflect the true position of the flap surfaces once the lever is moved out of the ‘Up’ detent.

Obviously, how a signal is computed needs to be understood by the designers of any function that uses that particular signal. Differences such as those described above may be of critical importance to the using system. However, once the design is finalized for both the source function and functions using this data, then the assumption is that the basic design of the source data will not change, and if it does change, the users of that data will be notified so they may assess the impact this change may have on their function. This is normally a valid assumption. However, that assumption cannot be relied upon with complete confidence unless it has the backing of a thorough Change Impact Analysis process. A continuation of the previous example illustrates why this is a very real concern.

Due to a problem discovered during the flight test program, a change is now required to the internal logic that calculates a flight deck alert for their system. One of the parameters used in the alert logic of the flap system is the FLAPS EXTENDED variable, which is also the same variable discussed above that is transmitted on the data bus for use by other functions on the airplane.

The flap system designers discover that one method of addressing this problem with the flap alert logic is to compute the FLAPS EXTENDED variable using the flap lever position instead of the actual flap surface position, which was the original design. Note that this change in how the FLAPS EXTENDED variable is calculated will not require a revision to the ICD, as the variable name has not changed and all the information regarding how the variable is transmitted on the data bus remains the same. However, the actual meaning of the variable in question is now technically different than it was before the change.
The impact of this change on the using systems cannot be ascertained without being analyzed by designers and analysts familiar with that system. However, they may not be alerted to this change if the one and only ‘red flag’ announcing the change is a revision to the ICD. Unless the system designers and analysts are aware a change has been made, no analysis will occur.

The point illustrated is that it cannot not be left to the designers and system experts of the function being updated (in this example, the flap system) to determine the effect of that change on downstream users. The experts that are required to assess the impact of the change are the designers and analysts of the using system, not the source system. A Change Impact Analysis that crosses functional boundaries is clearly required for this example, even though the ICD for the source function did not change. Additionally, this example illustrates why robust partitioning does not totally insulate functions residing in one partition from changes to a function in a different partition.

Use of Technical Standard Orders for Approval of Complex IMA Systems

Technical Standard Order Summary

Technical Standard Orders (TSO) are authorized by 14 CFR, Part 21, Subpart O and have existed since the 1950s. Although it is not the purpose of this paper to document the history and use of TSOs, a few specific points regarding TSOs from Part 21, Subpart O are summarized below.

1. A TSO is the minimum performance standard for an article designed for use on civil aircraft.
   A TSO deals with an article, independent of any aircraft.
   Only a selected list of articles has an associated TSO.
   Unless an applicant doesn’t submit what the FAA requires, the FAA has just 30 days to approve or deny the TSO Authorization application.
   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.
   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.

Complexity of IMA Systems

TSOs have been used successfully by industry and the FAA for many years. They provide a specific method for companies to provide the industry with approved components that have an established pedigree. However, TSOs were also conceived initially when articles were much simpler in nature.

If TSO Authorization is sought for a complete IMA system, there is the need to identify what certification activity will be done in support of the Type Certification and what will be done to show compliance to the TSO Minimum Performance Standard (MPS). This requires a great deal of coordination between the IMA developer seeking the TSO(s), the applicant wishing to install the TSO into an aircraft, the FAA ACO granting TSO authorization for the IMA system and the FAA ACO (or non-U.S. certification authority) that will be approving the IMA installation.

Current Process for Approving Complex IMA Systems Using TSOs

One very large complication that an applicant encounters when attempting to gain TSO authorization for a complex IMA system is the fact that there is currently no such thing as an IMA system TSO. As stated above in the CFR 14, Part O summary, only a few articles have TSOs. A complete IMA system is not one of those articles. Nowhere is an MPS for a complete IMA system documented. TSO C-153, although specific to IMA systems, only gives the MPS for generic IMA hardware components that do not, by themselves, perform airplane functions.

To gain TSO Authorization for an IMA system, the FAA and industry have been using a combination of the following:

- TSO C-153, for generic hardware computing modules, data concentrator
Compiled list of all individual TSOs 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 (software only, to be loaded into TSO C-153 approved IMA hardware at some later time), as defined in AC 20-145.

This approach is very piecemeal in nature. It is not at all clear to the parties involved as to how the entire IMA system has been approved and what needs to occur during installation approval of the IMA system.

There may be functions and sub-functions contained in an IMA system that will not be described in any of the individual article TSO minimum performance specifications. If they were to be included as being part of a complete “TSO’ed IMA system,” then those functions and sub-functions would need to be included as “non-TSO functions.”

Additionally, there is the question of all the other activity required to approve an IMA system, such as the integration activity (testing, analysis, etc.), human factors evaluation, safety assessment activity (fault tree analysis, functional hazard analysis) that the IMA developer also may desire to put under the banner of being “TSO approved.” However, these types of activities, by definition, are not “functions.” Defining all activity required for approval of a complex IMA system as “non-TSO functions” does not seem in the spirit of what was intended with Notice 8150.5. However, if this approach is used (i.e., defining all required IMA approval activities as “non-TSO functions”), then those aspects of the IMA approval will need to be documented, just as would true aircraft functions.

Compliance to Certification Program Issue Papers

FAA issue papers are imposed upon an aircraft or engine certification program (e.g., TC, STC). As stated in the TSO summarization at the beginning of this section, a TSO deals with an article, independent of any aircraft. That is, an article that is to receive a TSO authorization does not need to be evaluated for compliance to certification program issue papers, even if that article has been designed for installation into a specific aircraft.

However, with a system as complex as an IMA, there will undoubtedly be some aspects of the IMA system that will come under the purview of the issue papers levied against the aircraft program. An issue paper may require certain features of the IMA system to be designed in a specific manner, or it could place restrictions on how certain automated tools may be used during the software development and verification process. Issue papers are also used to document agreements on how “new and novel” technology or design approaches will be treated during the certification program. These types of issues cannot be dealt with solely at the aircraft level. They must be accounted for during the initial planning and development of the IMA system. This will require the developer of an IMA system to coordinate and work with at least two FAA (or non-U.S.) certification offices simultaneously. Also required will be a coordinated effort between the multiple FAA offices.

Most articles that receive TSO authorizations are not complex enough (e.g., seats, radio antennas) that extensive coordination is required between all the parties involved. However, for complex IMA systems, there is a danger that some required elements of the IMA system design or how it is approved may be missed if this coordination is not accomplished.

Human Factors TSO Compliance Evaluation

AC 20-145 is titled, “Guidance for Integrated Modular Avionics (IMA) that Implement TSO C-153 Authorized Hardware Elements.” The title of this AC may seem to indicate that it contains only guidance about how to comply with TSO C-153. However, that is an incorrect assumption. For example, section 16 of this AC is dedicated to
guidance for human factors and flight crew interface issues, as they apply to IMA systems. The guidance contained in this AC is relevant to all IMA systems, regardless of whether or not the IMA system supplier is seeking TSO authorization for the generic hardware components.

Many of the human factors and flight crew interface issues will be impossible to evaluate separately from the specific aircraft installation. Even for issues and evaluations that might be done in isolation, this is not the desired approach. Unless there are compelling reasons to do otherwise, human factors and flight crew interface issues and evaluations should be addressed as part of an aircraft certification program, not as part of the TSO authorization.

**Thirty Days Allowed for TSO Approval**

Unless the FAA finds that the applicant for a TSO has not submitted the correct information, the FAA only has thirty days to either approve or deny the application. For a complex IMA system, that is hardly enough time for the FAA to fully evaluate a TSO application. Even though a TSO constitutes a “self-certification,” the developer of the IMA should coordinate early and often with the FAA ACO that will approve the TSO, as well as with the FAA ACO or non-U.S. certification authority that will approve the installation. The issuance of the TSO authorization for an IMA system should be the culmination of a long and detailed process.

**Major/Minor Changes to Non-TSO Functions**

14 CFR, § 21.611 contains the regulations that govern the change process for articles that have been granted TSO authorizations. This process includes the concept of a “major change” and “minor change” to the article. § 21.611(b) contains information regarding how major changes to authorized TSO articles with must be processed as applications for a new TSO authorization. However, per § 21.611(a), the manufacturer of an article with prior TSO authorization may make minor changes to that article without involvement by the FAA.

Once again, this process works very well with articles that are relatively simple and have very well defined and bounded TSO minimum performance specifications. However, with complex IMA systems that may contain a significant amount of non-TSO functionality, what constitutes a “minor change” may become difficult to determine. Technically, the FAA ACO did not “approve” the non-TSO functions; it only “accepted” that those non-TSO functions exist within the article on a basis of non-interference with the primary function provided by the article. Therefore, it becomes very difficult to determine if a change should be categorized, per § 21.611, as a major or minor change for something that the FAA ACO did not initially approve but only “accepted” on the basis of non-interference.

**Summary**

History has repeatedly shown that the pace at which the technology used in aviation products evolves and is installed on aircraft progresses very rapidly, where the regulations, policy and advisory material related to these new technologies struggle to keep up. IMA systems are no exception.

The advanced technology of IMA systems has allowed designers of aircraft functions the ability to greatly expand the capabilities of those functions. Although the advanced capability aircraft functions need to be evaluated and approved, the main concern with IMA systems is not the advanced aircraft functionality it is able to provide. Rather, the concerns presented in this paper are about the IMA architecture itself. The sheer scale of IMA architectures introduces new issues into many aspects of the design, testing and approval of aircraft systems that did not previously exist, or alternatively, did exist but at a much simpler and easily understandable level.

Concurrent with these advances in technology, new business models are being introduced by industry that require collaborative partnerships between the developers of the IMA functions and IMA shared resources, the IMA system integrator, the aircraft certification applicant and all the various certification authority offices (both FAA and non-U.S.). Finally, program schedules are becoming more and more aggressive with each new aircraft certification program.

All of these issues make it increasingly likely that, unless great care is taken, some aspect of the
IMA system development, integration, testing and approval may be overlooked. In many cases, what is overlooked will have no safety effect and may never be noticed. In other cases, however, overlooked systems aspects may have safety impact. But, without the correct oversight and analysis, there is no way of knowing just how these oversights might manifest themselves at some future time. A number of incidents involving certified aircraft would seem to indicate that these complex systems, at times, behave quite differently than their designers’ intent. Some of these incidents have had significant safety implications.

The FAA is currently in the process of “taking stock” of all the issues surrounding complex IMA systems. It appears that action on a number of different fronts may be necessary. Developing and publishing (e.g., new regulations, guidance material, or policy) a comprehensive and integrated approach for approving complex IMA systems is needed. Currently, as can be seen in the beginning sections of this paper, many sources of information exist but they do not provide adequate or consistent guidance about how they are to be applied. Confusion, on the part of both industry and the FAA, is almost a certainty.

In addition to the actions that the FAA must take to addressing this very complex issue, all parties within industry also must shoulder some of the responsibility. Ensuring compliance to the regulations is the responsibility of the applicant, not the FAA. Industry cannot simply view IMA systems as just “more of the same” that they have been working with since the first generation digital aircraft systems. The highly integrated and complex nature of these systems requires a higher level of care and oversight than did past digital avionics systems. Increased diligence on the part of industry is imperative to ensure that the enhanced capabilities of IMA systems are not compromised by introduction of unforeseen failure effects or unexpected behavior on the part of the IMA systems.

References

Disclaimer
This paper does not represent the official Federal Aviation Administration (FAA) position. The authors are FAA employees, and while the paper is intended to be consistent with FAA policy, it has not been coordinated through the FAA’s approving officials and represents solely the opinions of its authors.

Biographies
Gregg Bartley is an engineer with the FAA Transport Airplane Directorate Standards Staff in Seattle, Washington. He has responsibilities in the areas of complex avionics systems, flight guidance systems, fly-by-wire flight controls, airborne software and complex hardware. Mr. Bartley holds an MS in Physics from the University of Washington and a BS in Electrical Engineering from Mississippi State University.

Barbara Lingberg is the Computer Software Program Manager for the FAA’s Aircraft Certification Service. She is sponsor of FAA Software and Digital Systems Research Program, and Designated Federal Official to RTCA/SC-205. Ms. Lingberg holds a BS in Mathematics and MS in Software Systems Engineering from George Mason University, Fairfax, VA.

27th Digital Avionics Systems Conference
October 26-30, 2008