JOURNAL OF AEROSPACE COMPUTING, INFORMATION, AND COMMUNICATION
Vol. 1, October 2004

Certification Concerns with Integrated Modular Avionics Projects

John Lewis*
Federal Aviation Administration, Washington, DC 20591

and
Leanna Rierson†
Federal Aviation Administration, Wichita, Kansas 67230

Aircraft manufacturers are proposing the implementation of Integrated Modular Avionics (IMA) into a number of new and modified aircraft. This paper addresses some of the major certification concerns that should be considered by IMA manufacturers, aircraft applicants, and certification authorities when developing, selecting, or approving IMA technology.

I. Introduction

AIRCRAFT manufacturers are proposing the implementation of Integrated Modular Avionics (IMA) into a number of new and modified aircraft. This paper addresses some of the major certification concerns that should be considered by IMA manufacturers, aircraft applicants, and certification authorities when developing, selecting, or approving IMA technology. The issues discussed in this paper do not represent all of the certification concerns with IMA, since there are unique issues associated with every IMA implementation. Also, this paper is not intended to provide specific IMA design or implementation techniques, and it does not represent FAA policy, guidance, or regulations.

Although the use of IMA technology is not new to aviation, the broad application of IMA systems, which can be installed on a variety of different aircraft types, represents a growing trend by avionics suppliers and aircraft manufacturers. To be competitive in today's aviation industry, aircraft manufacturers are procuring modularized components, such as

1) generic IMA hardware that can be customized by a systems "integrator" or an avionics manufacturer with field-loadable software,
2) real-time operating systems, and
3) other software components.

There are at least three basic objectives that must be met when dealing with new technology proposed for aviation use: performance, reliability, and safety. IMA is only one of several new technologies being proposed on multiple civil aircraft. Other technologies include object-oriented software, commercial-off-the-shelf (COTS) real-time operating systems, and qualifiable development tools. Regardless of the technology being proposed, performance, reliability, and safety must be achieved when implementing that technology into safety-critical avionics systems. This paper addresses the third objective, safety, by covering some of the certification concerns with IMA technology.

II. Background

Terminology is important when dealing with any new technology, but it is especially important when dealing with technical and certification issues related to IMA. Recognized and accepted terminology allows multiple manufacturers and industries to comply with certification requirements. A common understanding of terms also

---

Presented at the Digital Avionics Systems Conference, Indianapolis, Indiana, 13-17 October 2003; received 20 April 2004; accepted for publication 22 July 2004.

*Software Program Manager, 800 Independence Avenue, SW.
†Chief Scientific and Technical Advisor, 1600 Wooddale Street.

allows certification authorities to standardize their approach in determining when applicants comply with the applicable guidance and regulations.

Since there are multiple ways to define IMA, this paper uses the definition of Modular Avionics as stated in the terms of reference (TOR)[1] of the Joint Committee for Modular Avionics, RTCA Special Committee #200 (SC-200)/EUROCAE Working Group #60 (WG-60): “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, to host applications performing aircraft-related functions.”

It’s noteworthy to mention that this current definition is missing the word integrated; however, SC-200/WG-60 is in the process of updating their TOR to include the word integrated. Thus, this paper assumes the SC-200/WG-60 definition is actually for IMA versus Modular Avionics. With a closer look at this definition, we see words like shared, flexible, reusable, and interoperable. These descriptors give us insight into a few of the novel characteristics of this technology. Another key word worth noting is the word platform, which may enable reuse of type design data and permit incremental certification processes.

A. Evolution of IMA

Now that we have some knowledge of how IMA is currently described and defined, it is worthwhile to look at the evolution of avionics over the years to help us differentiate IMA systems from more traditional and older avionics systems. Traditional avionics systems are comprised of Line Replace Units (LRU). An LRU is typically characterized as a stand-alone box with a single function, a lack of interdependency (e.g., failure of single LRU does not affect other LRUs), and a lack of data sharing (e.g., no data coupling or control coupling issues). LRUs have traditionally communicated with each other, but the interaction has been limited and well controlled (e.g., only passing parameters in one direction). Also, the certification approach for most LRU equipment is well known and understood, since it has been used for a number of years. That is, the approach for safety analysis, verification, validation, and so forth of traditional LRU systems is well understood by experienced manufacturers and certification authorities.

The next evolutionary step for avionics equipment produced federated systems, which typically involved varying degrees of integration with different LRUs. Integration usually comes in the form of a communication link or a data bus. Federated systems are typically characterized as being custom-oriented, having less flexibility for modifications or changes, and having very limited or no shared resources. Also, certification of federated systems is usually more difficult because of the higher levels of integration, coupled with subsystems or LRUs that are usually implemented with dissimilar architecture.

Federated systems can look very similar to IMA, since the level of integration can be very high and result in complex implementations. For example, a federated system may include an LRU that integrates several aircraft functions such as Traffic Collision Avoidance Systems (TCAS), Global Positioning System (GPS), and Terrain Avoidance Warning System (TAWS). This LRU is comprised of different subsystems that share data over a common data bus (e.g., GPS data supports TCAS and TAWS functions). In this particular case, removal of the GPS subsystem would have significant ramifications, because of the tightly coupled nature of the data with the LRU’s integrated architecture. Also, installation of a different GPS subsystem would most likely require a significant redesign, due to the custom-oriented design of the LRU. One may argue that this federated system is really integrated avionics system. Whether it’s a federated system or an integrated system, it cannot be called IMA. Since this paper uses SC-200/WG-60’s definition of IMA, then we have to conclude that this particular system would not be classified as IMA based on its lack of flexibility, modularity, and reusability.

The next and current evolutionary step for avionics is the production of IMA systems. The FAA’s Technical Standard Order, TSO-C153, “Integrated Modular Avionics Hardware Elements”[2] provides an example of an IMA system, as illustrated in Fig. 1. The IMA hardware modules and racks are depicted as those elements within the dash lines. It should be noted that FAA TSO-C153 and Advisory Circular, AC 20-145, “Guidance for Integrated Modular Avionics (IMA) That Implement TSO-C153 Authorized Hardware Elements,”[3] represent a limited approach to IMA. Components such as displays, sensors, and actuators are not addressed by these FAA documents.

On the other hand, the efforts of SC-200/WG-60 represent a broader approach to IMA. Besides the SC-200/WG-60 definition, an IMA system can be characterized as having many integrated functions that have been previously contained in separated systems. It is the integration of these many functions onto shared resources that poses significant obstacles for determining compliance to the regulations and for verifying that all the required safety objectives are met.

To obtain some understanding of these obstacles, it is helpful to look at SC-200/WG-60’s list of key and novel characteristics of Modular Avionics:[4]

1) Shared resources
2) Capable of running multiple applications
3) Robust partitioning
4) Defined interfaces
5) Modular, pieces that don't perform aircraft functions
6) Reusable (software and hardware)
7) Multi-purpose platform
8) Flexible
9) Certifiable
10) Maintainable
11) Field loadable applications (independently)
12) Interoperable communications
13) Independent Development of Applications from Platform
14) Reconfigurable (static – retargeting of applications to line replaceable modules)
15) Software and hardware are modular by design
16) Increased complexity for configuration reporting/control
17) Deterministic behavior
18) Different set of roles and responsibilities for each key stakeholder

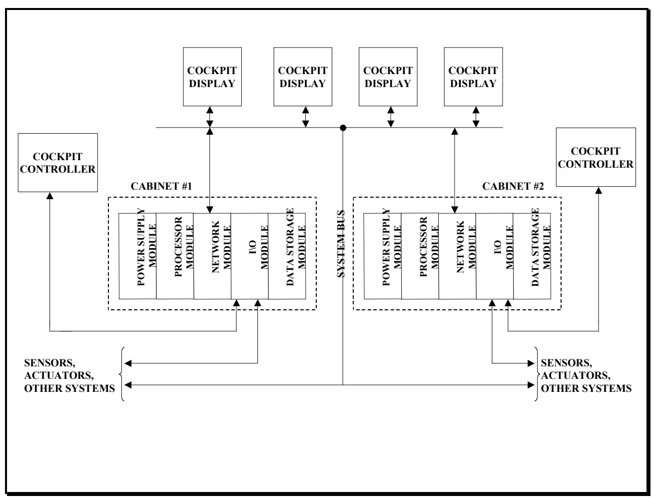

Fig. 1 Example of IMA system using TSO-C153 hardware elements.

B. Development of IMA Certification Guidance

There have been a number of phases in the development of certification guidance on IMA. Figure 2 shows the phases thus far; each phase is then described next.

The industry standard outlined in RTCA/DO-255, "Requirements Specification For Avionics Computer Resource (ACR)"[5] was the first attempt by the civil aviation industry to provide certification guidance for IMA technology. DO-255 focuses on the concept of an ACR. The ACR is a platform to be used by multiple applications or certification projects. Also, DO-255 covers key topics found in modern IMA systems, such as partition management, health monitoring, field loading of software, and other services. Additionally, Appendix B of DO-255 describes an Application Programming Interface (API) specification example for use in an IMA environment.

Although DO-255 contains information that may apply to IMA systems, the FAA was unable to officially recognize the standard as an acceptable means to obtain FAA installation or certification approval of avionics computer resources. Several factors have contributed to the FAA's decision to not officially recognize DO-255. It does not completely address the certification process and means to satisfy the regulations (i.e., it does not provide the big picture for certification of IMA systems). Therefore, it cannot be called out in an Advisory Circular (AC) without the addition of the certification framework. It does not adequately define an acceptable minimum operating performance specification (MOPS). Therefore, it cannot be called out through a Technical Standard Order (TSO). Although it represents a consensus document, the aviation community has been slow to embrace the use of open standards and open architecture because of the competitive and proprietary nature of the aviation industry. It does not adequately address the integration issues of the ACR onto the aircraft.

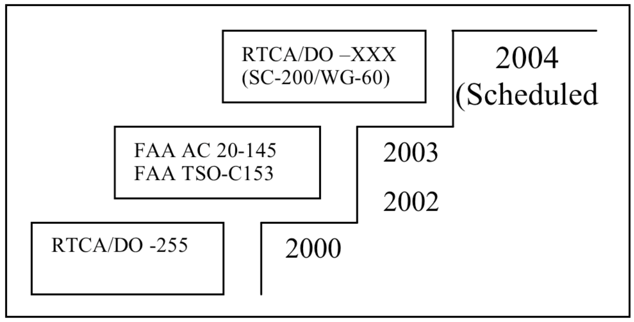

Fig. 2 Development phases of IMA certification guidance.

The next phase for creating IMA guidance was performed by the FAA, when it developed a TSO and an AC for IMA hardware elements. In the late 1990s, a variety of certification projects were being initiated or planned that involved the development of new IMA systems. Consequently, the aviation industry desired an alternate approval process to avoid costly recertification of IMA hardware elements (e.g., IMA cabinets and hardware modules).

To meet industry's requirements and to respond to the rapidly expanding growth of the regional and business aircraft markets, the FAA chartered the IMA team, which consisted of FAA certification and technical specialists, to develop a new TSO and AC for IMA hardware elements. As a result of the IMA team's effort, both the TSO and AC were developed within a two-year timeframe, in order to support domestic and international aircraft projects that used IMA. Accordingly, the FAA published TSO-C153 (Ref. 2) and AC 20-145 (Ref. 3).

Unlike traditional FAA TSOs, TSO-C153 does not reference an existing industry developed standard or Minimum Operating Performance Specifications (MOPS). Instead, TSO-C153 contains a list of applicable technical requirements that must be addressed when creating a minimum performance standard (MPS) document. Also, TSO-C153 introduces the concept of a non-functional TSO with its brain dead hardware elements that have no application software installed. The only software allowed with the TSO-C153 hardware elements is software that enables electronic identification and field-loadable software (FLS). The limitation on application software or the brains is why TSO-C153 is considered a non-functional TSO. Without the application software, TSO-C153 authorized equipment cannot perform aircraft functions like existing TSOs (such as, TSO-C118/Traffic Alert and Collision Avoidance System (TCAS), TSO-C147/Traffic Advisory System (TAS), and so forth). The FAA's intent was that hardware equipment authorized under TSO-C153 would be the building blocks for other existing or functional TSOs. Functional TSO authorizations would be granted once the hardware and software were integrated and approved. Thus, TSO-C153 and AC 20-145 provide a limited approach to IMA.

Although TSO-C153 was the first FAA recognized standard for IMA, it should be noted that a TSO authorization is an FAA approval for the design and production of equipment but is not approval for installation onto the aircraft. Installation approval is typically granted under a Type Certificate, Supplement Type Certificate, Amended Type Certificate, or Amended Supplemental Type Certificate (TC/STC/ATC/ASTC).

The IMA guidance development phase that is currently underway involves the ongoing effort of the joint international SC-200/WG-60 team. SC-200/WG-60 is striving to produce a harmonized guidance document before the end of 2004. To better understand the purpose of SC-200/WG-60, it is helpful to look at the committee's TOR,[1] which include the following primary objectives:

1) propose and document means to support the certification (or approval) of modular avionics, systems integration, and hosted applications, including considerations for installation and continued airworthiness in all categories and classes of aircraft,

2) define and document the essential characteristics of modular avionics.

3) provide a method for the stand-alone approval of modular avionics separate from the applications.

4) identify specific modular avionics issues in current regulatory materials and industry practices, and make recommendations to the document sponsor.

5) propose and document methods for transfer and reuse of certification credit.

6) create guidance to address the following safety and performance issues (at a minimum):

7) partitioning and resource management

8) fault management and health monitoring
9) safety and security
10) flight operations, installation, and instructions for continued airworthiness
11) environmental qualification
12) configuration management
13) design/development assurance (e.g., verification, processes, life cycles, etc.)

III. IMA Certification Concerns

The FAA and other certification authorities [such as the Joint Aviation Authorities (JAA)] have identified a number of common certification concerns that must be addressed in IMA systems. TSO-C153 and AC 20-145 addressed these in a limited fashion, since the IMA TSO-C153 hardware element approach is a limited implementation of IMA. SC-200/WG-60 is striving to more fully address these concerns in their forthcoming guidance. The remainder of this paper identifies the ten major certification concerns that need to be addressed in IMA certification efforts.*

A. Managing Multiple Levels of Requirements

Proper management of the aircraft's systems requirements is needed throughout its development life cycle (e.g., planning, design, integration, testing, verification, and maintenance). From a certification perspective, the applicant is responsible for performing the proper management of requirements, both at the aircraft level and system level, in order to validate that all the requirements are correctly implemented, and each of the resulting systems can be verified to meet their intended functions. Because of the multiple stakeholders involved, this requirements management is not a trivial task. Furthermore, proper management of requirements is required for continued airworthiness and continued operational safety as changes and modifications are incorporated into IMA systems installed on multiple aircraft.

Reuse of IMA components poses significant challenges, when validating and verifying system requirements. These challenges are due to the following factors:

1) IMA systems are typically highly integrated and complex systems.

2) Aircraft manufacturers and IMA manufacturers now have to manage a myriad of requirements (e.g., high-level, low-level, and derived requirements).

3) Reuse of IMA complicates follow-on projects in the requirements management process and may lead to incorrect or incomplete system requirements definition.

4) Reuse must take into account the requirements for stable and unique IMA components, including both hardware and software. Stable components are intended for multiple aircraft applications, whereas unique components are customized or tailored for a specific aircraft type. Tracking of the requirements for these different components is essential in determining whether or not a component is reusable for follow-on certification projects.

B. Performing the Safety Assessment

Traditional safety assessment guidance such as Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754 (Ref. 6) and SAE ARP 4761 (Ref. 7) are being applied to IMA. Currently, there is an SAE airplane safety assessment committee (S-18), which is revising the standards for safety assessment of airplanes and their related systems. The existing ARP guidance is well suited for an individual system tied directly to an aircraft function. However, the existing safety assessment guidance lacks focus on the integration aspects of an IMA system. As opposed to traditional avionics, IMA's integration of multiple functions with shared resources requires the system safety assessment (SSA) process to more focus more on common mode, common cause, and cascading effects, in addressing the integration of functions and the multiple loss of functions (e.g., common circuit breakers, power supplies, processors, data bus, operating systems, and software modules).

C. Managing the System Configuration with Multiple and Reconfigurable Components

IMA systems often contain components from multiple suppliers. Many of the components are programmable and reconfigurable. One of the keys to managing this complex system configuration is a robust automated configuration management system that handles field-loadable software and modular hardware elements. A smart box concept that implements a robust configuration management system is needed to ensure that the configuration approved as part of the certification effort (through TC, STC, ATC, or ASTC) is the configuration installed in the aircraft. The robust

*It should be noted that this is not an exhaustive list, since each project will have specific implementation issues. Also, solutions are not proposed, since the point of this paper is to highlight the concerns. There are likely many ways to address each concern.

automated configuration management system should manage and maintain IMA system configuration files, automatically track software and hardware changes, annunciate unapproved configurations to the ground and flight crews, and ensure that safety requirements are met prior to dispatching the aircraft.

D. Identifying Parts Via Electronic Means

In order to identify the part number and related parameters with limited real estate and to allow for flexibility, electronic part marking is being proposed for many IMA systems. Some of the concerns of electronic part marking are

1) survivability of the part marking information in case of an aircraft accident,
2) controllability of part loads, to ensure that only approved parts are loaded onto the aircraft,
3) verifiability of the IMA configuration, to know the configuration of the IMA system at any given time, and
4) compliance to the regulations. Both the TSO and type certificate regulations provide specific part marking requirements.

The regulations require TSO authorized articles to be permanently and legibly marked.[13] TSO-C153 allows electronic identification, if the appropriate parameters are stored in non-volatile memory (to support survivability) and the part identification can be read at any geographical location on the ground (to support verifiability).

Systems must still be approved through a TC, STC, ATC, ASTC, or TSO authorization before electronic part marking can be used – i.e., the electronic parts must still be approved by the FAA and meet the regulations.

When electronic identification is used, it should be supported by some type of ground configuration system – to ensure that the configuration of the aircraft is always know (again, to support verifiability and continued airworthiness). To address this concern TSO-C153 requires a separate process that records the IMA system configuration off-board the aircraft so that verification of the electronic identification is possible (e.g., top-level drawings, configuration management (CM) records, etc).

E. Assuring Software

Guidance from RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," [8] FAA Order 8110.49, "Software Approval Guidelines,"[9] and draft FAA Advisory Circular, "Reusable Software Components"[12] apply to software developed for IMA systems. Common software concerns related to IMA are

1) Field-Loadable Software – ensuring that the software component to be loaded is approved and performs its intended function.

2) Robust partitioning/protecting – ensuring that the multiple levels of software installed in an IMA system do not interfere with each other (e.g., ensuring that a Level C function doesn't corrupt or provide inadequate data to a Level A function).

3) Reusable software components – ensuring that all components meet the DO-178B objectives and fit into the overall system (e.g., software components are traceable to the systems requirements).

4) Dead or deactivated code – ensuring that reused components do not have features that could lead to safety problems (e.g., unintended activation of deactivated code).

5) Commercial-off-the-shelf (COTS) software – ensuring that COTS software meets DO-178B objectives or an acceptable alternate and fits into the overall system (e.g., real-time operating systems are a common COTS component used in IMA systems).

F. Assuring Complex Electronic Hardware

RTCA/DO-254, "Design Assurance Guidance For Airborne Electronic Hardware,"[10] provides applicable guidance to complex electronic hardware implemented in IMA systems. Although DO-254 is not yet officially recognized, the FAA is currently developing and coordinating an advisory circular to recognize RTCA/DO-254 as a means of compliance to the regulations for complex electronic components (e.g., application specific integrated circuits (ASIC), programmable logic devices (PLD), field programmable gate arrays (FPGA), custom micro-coded components, and similar electronic hardware) that cannot be exhaustively tested.

SAE ARP 4574 and ARP 4561 should also be considered when using complex electronic hardware in IMA systems.

G. Qualifying Components for the Environment

The environment of an aircraft can be very extreme. For example, the temperature range in a non-pressurized nose may vary from a hot day in the desert on a ramp to the cold temperatures at altitude. IMA systems are composed of many components that may be put together in multiple configurations. Qualifying modules for temperature, electromagnetic effects, vibration, and so forth, apart from an actual installation is difficult.

TSO-C153 and AC 20-145 attempts to address the concerns regarding environmental testing of IMA components by defining what may or may not be qualified apart from the installation. These documents consider the various levels of testing, such as the module, sub-system, and installation.

RTCA/DO-160, "Environmental Conditions and Test Procedures for Airborne Equipment"[11] guidance applies to IMA systems; however, it becomes more difficult to apply it to modular components. Applicants will need to provide end-to-end qualification strategies to address environmental qualification of IMA systems (e.g., the strategy must address the installed system, as well as its components).

H. Monitoring the System Health

Management of the IMA system health is essential for supporting safety assessment and ensuring proper fail-safe functionality. Some of the common health monitoring and fault management issues are

1) Levels of errors – addressing the multiple component levels, such as partition, module, system, and so forth.
2) Errors in modules – addressing errors in modules, such as initialization and normal operation.
3) Single event upset (SEU) – monitoring for SEU. SEU may be caused by cosmic particles and is a significant concern for high-speed processors and complex electronic hardware.
4) Power management – ensuring that essential power is provided at all times. This becomes more difficult to address, since the IMA system itself may manage some of its own power during normal and degraded operations.
5) Redundancy management – ensuring that redundant components are functioning properly.
6) Degraded modes of operations – ensuring that reduced modes of operation are acceptable and provide the flight crew the necessary information for continued safe flight and landing.
7) Recovery – recovering from faults that have been determined to be recoverable.
8) Reset – resetting power through warm and cold starts, as well as the procedures for the flight crew to perform such functions, when needed.

I. Defining the Roles and Responsibilities for All Stakeholders

There are typically multiple stakeholders involved in the development of IMA systems. Such stakeholders include: hardware component manufacturers, application software manufacturers, IMA system integrators, third party system manufacturers, aircraft and engine manufacturers, TSO authorized equipment manufacturers, and certification authorities. Many stakeholders with different roles and responsibilities make the certification process more difficult to manage and track. Every IMA project should develop a strategy to define roles and responsibilities of all stakeholders.

J. Integrating Multiple Components

Proper and safe integration of multiple components provided by multiple suppliers can be a challenge in IMA systems, particularly when the components are designed to be reconfigurable. Without careful control of interfaces and configuration, it is easy for something to go unnoticed until late in the program. Developing clear and comprehensive guidance on IMA integration poses one of SC-200/WG-60's greatest challenges.

In an IMA system, the multiple levels of integration include

1) aircraft integration,
2) system integration (integrating multiple subsystems into a system),
3) subsystem integration (integrating multiple components into a subsystem: typically the highest level for hardware and software integration), and
4) integration of multiple elements into a component.

It is likely that tools will be heavily used in the integration process. Therefore, the integrity of these tools will also need to be addressed.

IV. Summary

This paper provides an overview of some of the most common concerns when certifying aircraft with IMA systems. The issues are by no means an exhaustive list of things to consider in the evaluation and certification of IMA projects. Applicants and all stakeholders should develop proactive means for addressing these concerns early in the project life cycle. Early and frequent interaction with the certification authority (e.g., FAA or JAA) is also highly recommended.

References

[1]RTCA SC-200/WG-60 Terms of Reference, Washington, DC, 31 July 2002.

[2]FAA Technical Standard Order, TSO-C153, "Integrated Modular Avionics Hardware Elements," Washington, DC, May 2002.

[3]FAA Advisory Circular, AC 20-145, "Guidance for Integrated Modular Avionics (IMA) That Implement TSO-C153 Authorized Hardware Elements," Washington, DC, Feb. 2003.

[4]RTCA SC-200/WG-60 Working Paper, WP#203, "Scope and key attributes of MA," Washington, DC, July 2002.

[5]RTCA/DO-255, "Requirements Specification For Avionics Computer Resources (ACR)," Washington, DC, June 2000.

[6]ARP 4754, "Certification Considerations for Highly-Integrated or Complex Aircraft Systems," Warrendale, PA, Nov. 1996.

[7]ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," Warrendale, PA, Dec.1996.

[8]RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," Washington, DC, Dec. 1992.

[9]Federal Aviation Administration Order 8110.49, "Software Approval Guidelines," Washington, DC, June 2003.

[10]RTCA/DO-254, "Design Assurance Guidance for Airborne Electronic Hardware," Washington, DC, April 2000.

[11]RTCA/DO-160, "Environment Conditions and Test Procedures for Airborne Equipment," Washington, DC, July 1997.

[12]Federal Aviation Administration Draft Advisory Circular, AC 20-RSC, Reusable Software Components, draft 8.3, Washington, DC, 11 June 2003.

[13]Title 14 of the Code of Federal Regulations, Part 21.607(d), Sept. 1989.

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.

Useful Websites

FAA policy memos, Orders, Advisory Circulars are available at http://www.airweb.faa.gov/rgl.

FAA Technical Standard Orders (TSO) are available at http://www.faa.gov/certification/aircraft/.

FAA software-related certification information is available at http://av-info.faa.gov/software/.

RTCA documents may be purchased online at http://www.rtca.org/.

SAE documents may be obtained at http://www.sae.org.