News from the Hill

BY JASON DICKSTEIN
AEA GENERAL COUNSEL

Hazmat, HIRF and Software - oh my!

This month's article features something for everyone. The first part of this article warns AEA members about the FAA's latest intentions with respect to hazardous materials training (and yes, this could affect you even if you do not deal in hazardous materials). In the second part, we address the draft HIRF ICA guidance—although intended for engine manufacturers, it is likely to be of use to AEArepair stations who have to create their own ICAs for electronic engine controls (including those ICAs developed to support a field approval or STC project). Anyone who deals in software certification will be interested in the new FAA policy discussed in section three—the new guidance assists in assigning certification levels to software certification projects when RTCA and SAE documents appear to assign conflicting software levels.

HazMat Training for AEA Members with No Hazmat Exposure?

Last summer, the FAA published a notice of proposed rulemaking that would increase the level of hazardous material training required. More importantly, it would extend the training requirements to repair stations that are NOT hazmat employers. The federal regulatory unified agenda confirms that the final rule is now scheduled for early in 2005. While this may seem like a long time off, it is less than a year away!

AEA offered a proposed amendment that would exempt certain repair stations based on their ratings, but this has become a game of international politics so the United States may find itself unable to adopt this exemption. The rule (as proposed) has been submitted to the United Nations' International Civil Aviation Organization (ICAO) and U.S. policy is to harmonize with ICAO hazmat standards.

What would this mean? Every repair station would be required to train its employees in hazardous materials transportation even if the repair station never handled hazmat! If passed as proposed, AEA may consider petitioning for blanket exemptions for repair stations where such training would be an unnecessary and unreasonable burden.

In the meantime, there is a possibility that AEAmembers will be required to undertake hazmat training before next year's annual convention. To address this concern, AEA is offering its members a class in hazmat transportation—comparable training from other sources can cost over a thousand dollars per person.

In addition to the potential for an expanded hazmat training regulation in the near future, the AEA training may also alert you to unexpected hazards in your facility. For example, if you remove fuel control units and transport them then they may be hazmat as long as there is a residue (including vapor) of fuel. Certain avionics include back-up battery power and in these cases the batteries may be hazmat whether shipped alone or installed in the unit (of course, once the unit is installed in the aircraft, it enjoys an exemption from hazmat transportation regulations).

How important is compliance with hazmat training regulations? Well, TSA, FAA, and RSPA employees have all been asking repair stations for copies of their hazmat training certificates, and fines for non-compliance have been proposed in the six-figure and even seven-figure range.

The AEA hazmat training will be one full day long and will be offered on the Fast Trak day at the annual convention in Las Vegas on March 29. We strongly recommend sending at least one of your employees so that you are prepared to meet the training requirements if they are implemented as proposed.

Draft AC On HIRF Maintenance Tasks

As electronic control technology has become more commonplace in aircraft engines, there has been increased concern both in the industry and at the FAA about the vulnerability of these systems to exposure to High-Intensity Radio Frequency (HIRF) or lightning threats. The FAA has issued a draft Advisory Circular (AC) recommending that Instructions for Continued Airworthiness (ICAs) for aircraft engines and, in particular, for Electronic Engine Control (EEC) systems include maintenance tasks specifically aimed at ensuring the effectiveness of HIRF protection features. The guidance is primarily aimed at engine manufacturers, modifiers, foreign regulatory authorities, and FAA engine type certification engineers and their designees. Nonetheless, AEA members developing ICAs for field approvals of STCs should also bear this guidance in mind.

On the whole, the FAAbelieves that the general maintenance practices operators have followed as part of their overall engine maintenance programs have been effective in maintaining the HIRF protective functions. The FAA cites as evidence the 200+ million hours of in-service experience on engines with EEC systems that have not had any known HIRF incidents attributable to in-service environmental degradation effects. Examples of effective maintenance practices include: (1) Inspection and associated procedures linked to troubleshooting and Line Replaceable Unit (LRU) removals;

(2) Fault detection or annunciation of electrical system faults through Built-In-Test;

(3) General Visual Inspection (GVI) associated with scheduled aircraft Zonal Inspection Programs; and (4) Normal scheduled engine shop visits and specific component shop maintenance associated with on-condition maintenance, modification, or upgrade, and soft-time component refurbishment, when applicable.

Nevertheless, the FAA is concerned that typical maintenance on aircraft and engines has not always been adequate to ensure the maintenance of HIRF protection features. Depending upon the complexity of the protection design used, the agency believes that more specific and validated maintenance tasks may be necessary to ensure the effectiveness of protection features in service. Although there have been no known HIRF incidents attributable to in-service environmental degradation effects, the FAA notes with concern one known case of an engine flameout attributed to lightning for which an airworthiness directive (AD) was issued in 1995. Investigation revealed that the engine flameout occurred because several shields for the cable harness of the EEC were not properly grounded to the airframe, possibly due to a previous maintenance action. In the FAA's view, this incident emphasizes the importance of assuring that the effectiveness of HIRF protection features are maintained in service.

What to Do

The draft AC recommends that the first step in developing ICA for HIRF protection features is to identify the critical systems and equipment, their associated wiring, and all the critical design aspects used by the type design to meet its original certificated HIRF threat. The ICA should also address the associated inspection method(s) and acceptance criteria, as well as the current maintenance practices, intervals, etc. that apply to these HIRF protection features. The purpose of HIRF maintenance instructions is to detect the degradation of protection features so that the features can be restored to their original condition. The scope of these instructions will depend on the detailed HIRF protection design approach of a particular engine model and the level of criticality of the systems being protected.

The draft AC offers examples of typical maintenance task elements that could be included in the ICA, and discusses the pros and cons associated with each. They include full aircraft/engine tests, such as high-level RF tests, low-level swept frequency tests, and low level direct drive tests; detailed measurements of bonding resistance; loop resistance or impedance measurements; and complete tear-down inspections. Some of these tasks are labor-intensive, and not every task will catch every potential problem. ICAs will probably include more than one maintenance task.

Draft AC 33.4-3 also provides guidance on when the effectiveness of maintenance tasks must be validated, principally in cases where the task does not directly determine the effectiveness of the HIRF protection features (e.g., visual inspection of wire bundles), as well as examples of recommended criteria for validation activities. It notes that it will sometimes be necessary to conduct separate maintenance validation activity for individual systems, electrical equipment, or EEC for HIRF protection features within the equipment that cannot be effectively verified by aircraft/ engine tests or equipment acceptance tests.

The FAA further recommends that when drafting ICAs, the effect of field modifications and repairs to the original overall system HIRF protection should be considered. When possible, the engine maintenance manual should identify wiring, connectors, and components that should not be modified without additional HIRF protection validation. This could mean that future engine ICAs provide better guidance to those seeking to work on the EEC systems,

Continued on following page

NEWS FROM THE HILL

Continued from page 33

because the AC recommends that engine maintenance manuals provide guidance to assure repairs are able to maintain the desired HIRF protection performance.

Your Input Is Welcome

As of the writing of this article, the guidance was in draft form. Draft AC 33.4-3, Instructions for Continued Airworthiness; Maintenance Tasks for High Intensity Radio Frequency (HIRF)/Electromagnetic Interference (EMI)/Lightning Protection Features, can be accessed on the FAA Aircraft Certification Service website at http://www1.faa.gov/certification/aircraft/ by clicking on the "Regulation, Policy and Guidance" link at the left of the page and following the link to "Draft Advisory Circulars" (it will remain here until finalized). The AC was open for comment through February 16, 2004, but as always, later comments will be considered by the FAA whenever possible.

New FAA Policy Clarifies Safety Assessment Practices for Software Certification Projects

How safe is safe? When designing an aircraft, aircraft electronics systems, or software, safety and reliability levels are key considerations that must be taken into account in any airplane and system safety assessment. Adequately quantifying these factors is an important part of any certification project. In determining system Development or Design Assurance Levels (DALs), engineers rely upon various guidelines published by groups like the Radio Technical Commission for Aeronautics (RTCA) or the Society of Automotive Engineers (SAE). Questions sometimes arise, however, concerning which guidance to use in particular situations, because one available guideline may not be completely consistent with another. The FAA's Transport Airplane Directorate (TAD) has issued a policy memorandum providing a standardized approach to the use and application of these guidelines and industry practices for projects involving transport category airplanes. Although technically applicable only to transport category aircraft, it provides excellent guidance for a wide range of projects, including avionics certification projects.

Traditionally, failure analysis and design validation and verification have been accomplished with extensive tests conducted on the system and its components, direct inspection, and other direct verification methods capable of correctly characterizing the operations of the system. These direct techniques are still appropriate for simple systems which perform a limited number of functions and which are not highly integrated with other aircraft systems. For more complex or integrated systems, however, adequate testing may either be impossible because all of the system states cannot be determined, or it may be impractical due to the large number of tests which must be accomplished. Some practical alternative was needed.

The FAA has not yet formally recognized RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware. Formal recognition through an advisory circular may occur in the future. Nevertheless, the FAA has issued several issue papers on various certification programs that recognize RTCA DO-254 as an acceptable means of compliance for programmed logic devices (PLD).

There are industry guidelines available for the development of airborne systems (SAE ARP4754), software (RTCA DO-178B), and electronic hardware components (RTCA DO-254). Because these documents were not developed simultaneously, they contain different guidance and terminology. For example, SAE ARP4754 and RTCA DO-178B can lead an applicant to two different software levels. Some in the industry have complained that SAE ARP4754 can be too liberal in assigning software DALs. On the other side of the coin, RTCA DO-178B has been accused of leading to a more conservative DAL assignment than is necessary to meet the applicable regulations.

Furthermore, the quantitative differences between the software levels in the various guidelines differs as well.

The FAA has determined that it is appropriate to consider system architecture for the purpose of establishing DALs; however, there was no way to integrate the DAL-assignment mechanisms of the three sets of guidelines. The new FAA policy provides a standardized approach to the use and application of these guidelines in establishing DALs, where more than one guideline may apply.

The Policy

The new policy recommends that the preliminary system safety assessment (PSSA) contain proposals for DALs for the system and each of its software and hardware items. The FAA encourages applicants to submit these safety assessments to the FAA for approval early in the program in order to minimize certification risks (and expenses).

The system, hardware, and software DALs may be assigned based on a direct relationship to the worst-case failure condition; namely, "Catastrophic" corresponds to Level A, "Hazardous/Severe-Major" to Level B, "Major" to Level C, "Minor" to Level D, and "No Safety Effect" to Level E. This method, particularly when applied to a system architecture with redundant elements, may result in a more conservative assignment of the DALs to the redundant elements than is necessary to comply with §§ 25.1301 and 25.1309. Where this is the case, the design approval applicant should present to the ACO the justification for the reduction in DAL from the levels determined by this method – this should be done early in the program for approval, and the applicant may rely on the guidance of the new policy for assistance.

Where a design could contain common mode design errors that are potentially catastrophic, the applicable software and hardware should be assigned Level A. The software and hardware DALs could potentially be reduced as justified by the safety assessment if the system architecture is revised to mitigate the potential catastrophic condition.

The guidance of SAE ARP4754 may be used to assign DALs for a system and its hardware and software components. When application of this guidance leads to assignments of DALs lower than those determined using the “direct assignment” method described above, the applicant should obtain concurrence of the cognizant FAAACO with the results of the proposed PSSAas early as possible in the program in order to minimize certification risks. If the criteria of the SAE ARP4754 are not satisfied, the DALs may need to be assigned a higher level using the direct assignment method or using the guidance of RTCA DO-178B.

Applicants may continue to use the guidance of RTCA DO-178B in the PSSA, as appropriate, to determine software levels, as they have traditionally done. Where apparent differences exist between RTCA DO-178B and SAE ARP4754 on software level determination, the guidance contained in Appendix D of SAE ARP4754 can be used if additional credit is requested for system architecture and justification is provided to the cognizant ACO for concurrence.

For transport category airplanes, RTCA DO-254 is applicable to all electrical and electronic devices whose correct operation cannot be verified by test and/or deterministic analysis if they could cause Major, Severe Major/Hazardous, and Catastrophic failure conditions.

Where used successfully to lessen the software assurance level of a project, this new FAA policy can result in significant savings, and may even turn an impossible software certification project into a reasonable one.

Effects of the Policy

The general policy stated in the FAAmemorandum does not constitute a new regulation or create what the courts refer to as a “binding norm.” The FAA encourages the offices that implement policy to follow this policy when applicable to the specific project. Whenever an applicant’s proposed method of compliance is outside this established policy, it must be coordinated with the policy issuing office, e.g., through the issue paper process or equivalent.

The value of this policy is that it carves a path through the conflicting guidance of SAE ARP4754, RTCA DO-178B, and RTCA DO-254. Although the path is not always clear, it is certainly more useful than the directly conflicting language of those three sets of guidelines. Although this new policy is not legally binding on the FAA, if an ACO becomes aware of reasons that an applicant’s proposal should not be approved despite the fact that it meets this new policy, the office has been directed to coordinate its response with the Transport Airplane Directorate.

Applicants should expect that the certificating officials will consider this information when making findings of compliance relevant to new certificate actions. As with all advisory material, this policy statement identifies one means, but not the only means, of compliance.

The memorandum, titled “Policy Statement on Guidance for Determination of System, Hardware, and Software Development Assurance Levels on Transport Category Airplanes,” was published on January 15, 2004. It can be found on the Regulatory and Guidance section of the FAA website at www.airweb.faa.gov/rgl; search for policy number PS-ANM-03-117-09 to find the document. An appendix to the memorandum contains additional details, as well as tutorial examples to aid in the understanding of the policy.

AD 95-09-04, applicable to certain de Havilland Model DHC-8-100 and 300 series airplanes. ❑