23

Certification of Civil Avionics

Frank McCormick
Certification Services, Inc.

23.1 Introduction

Almost all aspects of the design, production, and operation of civil aircraft are subject to extensive regulation by governments. This chapter describes the most significant regulatory involvement a developer is likely to encounter in the certification of avionics.

Certification is a critical element in the safety-conscious culture on which civil aviation is based. The legal purpose of avionics certification is to document a regulatory judgment that a device meets all applicable regulatory requirements and can be manufactured properly. At another level, beneath the legal and administrative machinery of regulatory approval, certification can be regarded differently. It can be thought of as an attempt to predict the future. New equipment proposed for certification has no service history. Certification tries, in effect, to provide credible predictions of future service experience for new devices — their influences on flight crews, their safety consequences, their failure rates, and their maintenance needs. Certification is not a perfect predictor, but historically it has been quite a good one.

In this chapter, for the most part, certification activities appropriate to the U.S. Federal Aviation Administration (FAA) are discussed. However, be aware that the practices of civil air authorities elsewhere, while generally similar to those of the FAA, often differ in detail or scope. Toward the end of this chapter,

some differences between the FAA and the European Joint Aviation Authorities, or JAA, headquartered in Hoofddorp, the Netherlands, will be illustrated.

Expensive misunderstandings can result from differences among regulators. Moreover, the rules and expectations of every authority, the FAA included, change over time. For current guidance, authoritative sources should be consulted.

This chapter discusses the following topics:

- The FAA regulatory basis
- The Technical Standard Order (TSO) system for equipment approval
- The Supplemental Type Certificate (STC) system for aircraft modification
- Use of FAA designees in lieu of FAA personnel
- System requirements definition
- Safety assessments
- Environmental qualification
- Software assurance
- Production approvals
- The Joint Aviation Authorities

Conceptually, the certification of avionics is straightforward, indeed almost trivial: the applicant simply defines the product, establishes its regulatory requirements, and demonstrates that those requirements have been met. The reality is, of course, more problematic.

It is a truism that for any proposed avionics system a suitable market must exist. As with any commercial pursuit, adequate numbers of avionics units must be sold at margins sufficient to recover investments made in the product. Development costs must be controlled if the project is to survive. Warranty and support costs must be predicted and managed. The choices made in each of these areas will affect and be affected by certification.

This chapter is an introduction to certification of avionics. It is not a complete treatment of the subject. Some important topics are discussed only briefly. Many situations that come up in real-life certification projects are not addressed.

Good engineering should not be confused with good certification. A new avionics device can be brilliantly conceived and flawlessly designed, yet ineligible for certification. Good engineering is a prerequisite to good certification, but the two are not synonymous.

Certification has a strong legalistic element and is more craft than science. Almost every project raises some odd regulatory-approval quirk during its development. Certification surprises are rarely pleasant, but surprises can be minimized or eliminated by maintaining open and honest communication with the cognizant regulators.

23.2 Regulatory Basis of the Federal Aviation Administration

The FAA, created in 1958, acts primarily through publication and enforcement of the Federal Aviation Regulations, or FARs. FARs are organized by sections known as Parts. The FAR Parts covering most avionics-related activity are listed below:

- Part 1 — Definitions and Abbreviations
- Part 21 — Certification Procedures for Products and Parts
- Part 23 — Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes
- Part 25 — Airworthiness Standards: Transport Category Airplanes
- Part 27 — Airworthiness Standards: Normal Category Rotorcraft
- Part 29 — Airworthiness Standards: Transport Category Rotorcraft
- Part 33 — Airworthiness Standards: Aircraft Engines

- Part 34 — Fuel Venting and Exhaust Emission Requirements for Turbine Engine-Powered Airplanes
- Part 39 — Airworthiness Directives
- Part 91 — General Operating and Flight Rules
- Part 121 — Operating Requirements: Domestic, Flag, and Supplemental Operations
- Part 183 — Representatives of the Administrator

Only a subset of these regulations will apply to any given project. Much of the job of managing a certification program well lies in identifying the complete but minimum set of regulations applicable to a project.

23.3 FAA Approvals of Avionics Equipment

The FARs provide several different forms of approval for electronic devices installed aboard civil aircraft. Of these, most readers will be concerned primarily with approvals under the Technical Standard Order (TSO) system, approvals under a Supplemental Type Certificate (STC), or approvals as part of a Type Certificate, Amended Type Certificate, or Service Bulletin.*

23.3.1 Technical Standard Order

An approval under the Technical Standard Order (TSO) system is common. TSOs are regulatory instruments that recognize the broad use of certain classes of products, parts, and devices. TSOs apply to more than avionics; they can apply to any product with the potential for wide use, from seat belts and fire extinguishers to tires and oxygen masks. Indeed, that is the guiding principle behind TSOs — they must be widely useful. Considerable FAA effort goes into the sponsorship and adoption of a TSO. The agency would have little interest in publishing a TSO for a device with limited application.

TSOs contain product specifications, required data submittals, marking requirements, and various instructions and limitations. Many TSOs are associated with avionics: flight-deck instruments, communications radios, ILS receivers, navigation equipment, collision avoidance systems, and flight data recorders, to name just a few.

TSO-C113, "Airborne Multipurpose Electronic Displays," is representative of avionics TSOs. Electronic display systems are used for various purposes: display of attitude, airspeed, or altitude, en route navigation display, guidance during precision approach, display of engine data or aircraft status, maintenance alerts, passenger entertainment, and so on. The same physical display device could potentially be used for any or all of these functions, and on many different aircraft types. Recognizing this broad applicability, the FAA published TSO-C113 so that developers could more easily adapt a generic display device to a variety of applications. TSO-C113 is typical, calling out requirements for the following data:

- Explanation of applicability
- Exceptions and updated wording
- References to related regulations, data, and publications
- Requirements for environmental testing
- Requirements for software design assurance
- Requirements for the marking of parts
- Operating instructions
- Equipment limitations
- Installation procedures and limitations
- Schematics and wiring diagrams
- Equipment specifications

*Newly developed equipment has sometimes been installed as part of a field approval under an FAA Form 337, though this has become rarer and is disallowed in most cases.

- Parts lists
- Drawing list
- Equipment calibration procedures
- Corrective maintenance procedures

When an avionics manufacturer applies for a TSO approval, and the manufacturer's facilities and data comply with the terms of the TSO, the manufacturer receives a TSO Authorization from the FAA. A TSO Authorization represents approval of both design data and manufacturing rights. That is, the proposed device is deemed to be acceptable in its design, and the applicant has demonstrated the ability to produce identical units.

In TSO-based projects, the amount of data actually submitted to the FAA varies by system type, by the FAA's experience with particular applicants, and by FAA region. In one case, an applicant might be required to submit a great deal of certification data; in another, a one-page letter from an applicant might be adequate for issuance of a TSO Authorization. On any new project, it is unwise to presume that all regulatory requirements are known. Consistency is a high priority for the FAA, but regional differences among agency offices do exist. Early discussion with the appropriate regulators will ensure that the expectations of agency and applicant are mutually understood and agreed on.

For more information on TSOs, see FAA Advisory Circular 20-110J, "Index of Aviation Technical Standard Orders;" FAA Order 8110.31, "TSO Minimum Performance Standard;" and FAA Order 8150.1, "Technical Standard Order Procedures."

Note that a TSO does not grant approval for installation in an aircraft. Although data approved under a TSO can be used to support an installation approval, the TSO Authorization itself applies only to the equipment in question. Installation approvals must be pursued through other means (see next section) and are not necessarily handled by an avionics equipment manufacturer.

23.3.2 Supplemental Type Certificate

A Supplemental Type Certificate (STC) is usually granted to someone other than the aircraft manufacturer, who wishes to modify the design of an existing aircraft. Retrofits and upgrades of avionics equipment are common motivations for seeking STC approvals from the FAA.

In an STC, the applicant is responsible for all aspects of an aircraft modification. Those aspects typically include the following:

- Formal application for a Supplemental Type Certificate (STC)
- Negotiation of the certification basis of the relevant aircraft with the FAA
- Identification of any items requiring unusual regulatory treatment
- Preparation of a certification plan
- Performance of all analyses specified in the certification plan
- Coordination with the FAA throughout the project
- Physical modification of aircraft configuration
- Performance of all conformity and compliance inspections
- Performance of all required lab, ground, and flight testing
- Preparation of flight manual supplements
- Preparation of instructions needed for continued airworthiness
- Preparation of a certification summary
- Support of all production approvals

An applicant for an STC must be "a U.S. entity," although the exact meaning of this phrase is not always clear. One common case is that of a nominally foreign firm with an office in the U.S. It is acceptable to the FAA for that U.S.-based office to apply for and hold an STC.

An applicant for an STC begins the process officially by completing and submitting FAA Form 8110-12, "Application for Type Certificate, Production Certificate, or Supplemental Type Certificate," to the cognizant FAA Aircraft Certification Office. Accompanying the application should be a description of the project and the aircraft type(s) involved, the project schedule, a list of locations where design and installation will be performed, a list of proposed Designees (discussed later in this chapter), and, if desired, a request for an initial meeting with the FAA. The FAA will assign a project number, appoint a manager for the project, schedule a meeting if one was requested, and send to the applicant an acknowledgment letter with these details.

The applicant must determine the certification basis of the aircraft to be modified. The certification basis is the sum of all applicable FAA regulations (at specified amendment levels) and any binding guidance that apply to the aircraft and project in question. Regulations tend to become more stringent over time, and complying with later rules may be more time-consuming and expensive than with earlier rules.

A certification basis is established by reference to the Type Certificate Data Sheet (TCDS) for each affected aircraft and through negotiation with the FAA. For example, an applicant might propose that a certification basis be those rules in effect at the time of original aircraft certification, whereas the FAA may require the applicant to comply with regulations in effect at the time of STC application. The differences between these two positions can be numerous and significant. Except in the simplest cases, they are a crucial topic for early discussions with the FAA.

Complex avionics systems, extensive aircraft modifications, and novel system architectures all raise the odds that something in a project will be unusual and will not fit neatly into the normal regulatory framework. For such activities, an applicant might wish to propose compliance based on other regulatory mechanisms: alternative means of compliance, findings of equivalent safety, exemptions, or special conditions. If so, generic advice is largely useless. By their nature, these activities are unusual and require close coordination with the FAA.

An STC applicant must prepare a certification plan. The plan should include the following:

- A brief description of the modification and how compliance is to be substantiated
- A summary of the Functional Hazard Assessment (see "Safety Assessment" later in this chapter)
- A list of proposed compliance documentation, including document numbers, titles, authors, and approving or recommending Designees, if applicable (the role of Designees is described in more detail later in this chapter)
- A compliance checklist, listing the applicable regulations from the certification basis, their amendment number, subject, means of compliance, substantiating documents, and relevant Designees
- A definition of Minimum Dispatch Configuration
- If used, a list of the proposed FAA Designees, including name, Designee number, appointing FAA office, classification, authorized areas, and authorized functions
- A project schedule, including dates for data submittals, test plan submittals, tests (with their locations), conformity inspections, installation completion, ground and flight testing, and project completion

Some FAA Aircraft Certification Offices require all Designated Engineering Representatives (see next section) participating in a project to sign an FAA Form 8110-3, "Statement of Compliance with the Federal Aviation Regulations," recommending approval of a certification plan.

Extensive analysis and testing are generally required to demonstrate compliance. Results of these analyses and tests must be preserved. Later in this chapter, three of the most important of these activities — safety assessments, environmental qualification, and software assurance — will be discussed along with another engineering topic, development and handling of system requirements.

The FAA's involvement in an STC is a process, not an act. Most FAA specialists support multiple projects concurrently, and matching the schedules of applicant and agency requires planning. This planning is the applicant's responsibility. Missed deadlines and last-minute surprises on the part of an

applicant can result in substantial delays to a project, as key FAA personnel are forced to reschedule their time, possibly weeks or months later than originally planned.

The STC process assumes modification of at least one prototype aircraft. It is in the aircraft modification that all the engineering analysis — aircraft performance, structural and electrical loading, weight and balance, human factors, and so on — comes together. Each component used in an aircraft modification must either be manufactured under an approved production system or examined formally for conformance to its specifications. This formal examination is known as "parts conformity inspection." A completed aircraft modification is then subject to an "installation conformity inspection." In complex installations or even complex parts, progressive conformity inspections may be required. Conformity inspections are conducted by an FAA Inspector or a Designee authorized by the FAA — a Designated Manufacturing Inspection Representative (DMIR) or Designated Airworthiness Representative (DAR) (see next section).

Compliance inspections, as distinct from conformity inspections, verify through physical inspection that a modification complies with the applicable FARs. Typical of compliance inspections is an examination of modified wiring on an aircraft. A compliance inspection is conducted by an FAA engineer or authorized Designated Engineering Representative (again, see next section).

For significant projects involving ground and flight testing, the FAA will issue a Type Inspection Authorization (TIA). The TIA details all the inspections, ground tests, and flight tests necessary to complete the certification program. Prior to issuing a TIA, the FAA should have received and reviewed all of the descriptive and compliance data for the project. The FAA has recently added an item to its TIA procedures: the flight test risk assessment. The risk assessment seeks to identify and mitigate any perceived risks in flight tests that include FAA personnel, based on data supplied by the applicant.

New avionics equipment installed as part of an STC will usually impose new and different procedures on flight crews. An applicant will, in most cases, document new procedures in a supplement to an approved flight manual. In complex cases, it may also be necessary to provide a supplement to an operations manual.

An applicant must provide instructions for the continued airworthiness of a modified airplane. Penetrations of the pressure vessel by, say, wiring or tubing may require periodic inspection. Actuators associated with a new subsystem may need scheduled maintenance. Instructions for continued airworthiness are usually a supplement to a maintenance manual but may also include supplements to an illustrated parts catalog, a structural repair manual, structural inspection procedures, or component maintenance manuals.

Much of this discussion has been more applicable to transport aircraft than to smaller aircraft. Regulatory requirements for the smaller (FAR Part 23) aircraft are, in some respects, less stringent than for transport aircraft. Yet even for transports, not everything described above is required in every circumstance. Early discussion between applicant and regulator is the quickest way to determine what actually needs to be done.

Some avionics developers may find it desirable to pursue an STC through an organization called a Designated Alteration Station (DAS). A DAS can, if properly authorized by the FAA, perform all the work associated with a given aircraft modification and issue an STC. In this approach, the developer might not deal with FAA personnel at all. Key issues are ownership of the STC rights and handling of production approvals.

For more information on STCs, see FAA Advisory Circular 21-40, "Application Guide for Obtaining a Supplemental Type Certificate." For more information on DASs, see FAA Advisory Circular 21.431-1A, "Designated Alteration Station Authorization Procedures."

23.3.3 Type Certificate, Amended Type Certificate, and Service Bulletin

Approvals as part of a Type Certificate, Amended Type Certificate, or Service Bulletin are tied to the certification activities of airframers or engine manufacturers. For development programs involving these kinds of approvals, an avionics supplier's obligations are roughly similar to those imposed by an STC project, though detailed requirements can vary greatly. Avionics suppliers participating in an aircraft- or engine-development program can and should expect to receive certification guidance from the manufacturer of the aircraft or engine. Hence, these cases will not be considered further here.

23.4 FAA Designees

In the U.S., any applicant may deal directly with the FAA. Unlike many other civil air authorities, the FAA does not collect fees for its services from applicants. However (and also unlike other agencies), the FAA can at its discretion appoint individuals who meet certain qualifications to act on its behalf. These appointees, called Designees, receive authorizations under FAR Part 183 and act in a variety of roles. Some are physicians authorized to issue medical certificates to pilots. Others are examiners authorized to issue licenses to new pilots. Still others are inspectors authorized to approve maintenance work.

Avionics developers are most likely to encounter FAA Designated Engineering Representatives (DERs) and either Designated Manufacturing Inspection Representatives (DMIRs) or Designated Airworthiness Representatives (DARs).

All Designees must possess authorizations from the FAA appropriate to their activities. DERs can approve engineering data just as the FAA would. Flight Test Pilot DERs can conduct and approve the results of flight tests in new or modified aircraft. DMIRs and DARs can perform conformity inspections of products and installations, and DARs can issue Airworthiness Certificates. When acting in an authorized capacity, a Designee is legally a representative of the FAA; in most respects, he or she is the FAA for an applicant's purposes. Nevertheless, there are practical differences in conduct between the FAA and its Designees.

The most obvious difference is that an applicant actually hires and pays a Designee, and thus has more flexibility in managing his or her time on the project. The resulting benefits in project scheduling can more than offset the costs of the Designee. In addition, experienced Designees can be sources of valuable guidance and recommendations. The FAA, by contrast, restricts itself to findings of compliance. That is, the agency will simply tell an applicant whether or not submitted data complies with the regulations. If data are judged noncompliant, the FAA will not, in most cases, tell an applicant how to bring it into compliance. A Designee, however, can assist an applicant with recovery strategies or, better yet, steer an applicant toward compliant approaches in the first place.

The FAA often encourages the use of Designees by applicants. An applicant must define and propose the use of Designees, by name, to the FAA Aircraft Certification Office (ACO) for each project. If the proposed Designees are acceptable to the ACO, the ACO will coordinate with its manufacturing counterpart and delegate certain functions to the specified Designees. Those Designees are then obliged to act as surrogates for the relevant FAA personnel on that project, providing oversight and ultimately approving or recommending approval of compliant data.

Although an applicant's use of Designees is discretionary, the realities of the FAA workload and scheduling may make the use of Designees a pragmatic necessity. Whenever Designees are considered for inclusion in a project, their costs and benefits should be evaluated with the same care devoted to any other engineering resource. For more information, see FAA Order 8100.8, "Designee Management Handbook;" FAA Order 8110.37C, "Designated Engineering Representatives (DER) Guidance Handbook;" and FAA Order 8130.28A, "Airworthiness Designee Management Program."

This chapter has so far dealt mainly with the definitions and practices of FAA regulation. There is, of course, a great deal of engineering work to be done in any avionics development. Four engineering topics of great interest to the FAA are the handling of system requirements, performance of a safety assessment, environmental qualification, and software assurance.

23.5 System Requirements

Avionics developers must document the requirements of their proposed systems, ideally in ways that are easily controlled and manipulated. Many experienced practitioners regard the skillful capture of requirements as the single most important technical activity on any project. A system specification is the basis for descriptions of normal and abnormal operation, functional testing, training and maintenance procedures, and much else. A brief treatment of the topic here does not imply that it can be approached

superficially. On the contrary, system specification is so important that a large body of literature exists for it elsewhere (see Chapter 21 for a starting point). Requirements definition is supported by many acceptable methods. Each company evolves its own practices in this area.

Over the years, many types of avionics systems have come to be described by *de facto* standardized requirements, easing the burden of both engineering and certification. New systems, though, are free to differ from tradition in arbitrary ways. Applicants should expect such differences to be scrutinized closely by regulators and customers, who may demand additional justification and substantiation for the changes.

Proper requirements are the foundation for well-designed avionics. Whatever the sources of requirements, and whatever the methods used for their capture and refinement, an applicant must be able to demonstrate that a new system's requirements — performance, safety, maintenance, continued airworthiness, and so on — have been addressed comprehensively. Some projects simply tabulate requirements manually, along with the means of compliance for each requirement. Others implement large, sophisticated databases to control requirements and compliance information. Compliance is generally shown through analysis, test, inspection, demonstration, or some combination thereof.

23.6 Safety Assessment

Early in a project — the earlier the better — developers should consider the aircraft-level hazards associated with their proposed equipment. This is the first of possibly several steps in a safety assessment of a new system.

There is an explicit correlation between the severity of a system's hazards and the scrutiny to which that system is subjected. With a few notable exceptions,* systems that are inconsequential from a safety standpoint receive little attention. Systems whose improper operation can result in aircraft damage or loss of life receive a great deal of attention and require correspondingly greater engineering care and substantiation.

Unsurprisingly, there is an inverse relationship between the severity of a system's hazards and the frequency with which those hazards can be tolerated. Minor annoyances might be tolerable every thousand or so flight hours. Catastrophic hazards, by contrast, must occur less frequently than once in every billion flight hours. In addition, the regulations for transport aircraft require that no single failure, regardless of probability, result in a catastrophic hazard, implying that any such hazard must arise from two or more independent failures occurring together.

Initial considerations of hazards should be formalized in a Functional Hazard Assessment (FHA) for the proposed system. An FHA should address hazards only at levels associated directly with operation of the system in question. For example, an autopilot FHA would consider the hazards of an uncommanded hardover or oscillation of a control surface. A display-system FHA would consider the hazards of blank, frozen, and active-but-misleading displays during various phases of flight.

In general, if an FHA concludes that misbehavior of a system has little or no effect on continued safe flight and landing, no further work is needed for the safety assessment. On the other hand, if the FHA confirms that a system can pose nontrivial risk to the aircraft or its occupants, then investigation and analysis must continue. The additional work, if needed, will likely involve preparation of a Preliminary System Safety Assessment, Fault Tree Analysis, Failure Modes and Effects Analysis, Common Cause Analysis, and a final System Safety Assessment.

In the absence of a specific aircraft installation, assumptions must be made regarding avionics usage to make progress on a safety assessment. This is true in TSO approvals, for example, if design assurance levels are not specified in the TSO or if developers contemplate hazards or usage different from those assumed

*For example, failures of flight data recorders, cockpit voice recorders, and emergency locator transmitters have no effect on continued safe flight and landing. Conventional safety-assessment reasoning would dismiss these devices from failure-effect considerations. However, the systems obviously perform important functions, and the FAA defines them as worthy of more attention than suggested by a safety assessment. For more discussion of this topic, refer to Software Assurance in this chapter for a description of software levels assigned to flight data recorders.

in the TSO. There are pitfalls* in unthinking acceptance and use of generic hazard classifications and software levels (see Software Assurance later in this chapter and in Chapter 27), even for standard products. Technologies can change quickly; regulations cannot. The gap between what is technically possible and what can be approved sometimes leads to conflicting requirements, bewildering difficulties, and delays in bringing to market devices that offer improvements to safety, operating economics, or both. The solution is early agreement with the appropriate regulators concerning the requirements applicable to a new device.

The details of safety assessments are outside the scope of this chapter. For an introduction to safety-related analysis, refer to the following:

- Chapters 21 and 22 of this book
- ARP4754 — Systems Integration Requirements Guidelines; Society of Automotive Engineers Inc., 1994
- ARP4761** — Guidelines and Tools for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment; Society of Automotive Engineers Inc., 1994
- NUREG-0492 — Fault Tree Handbook; U.S. Nuclear Regulatory Commission, 1981
- FAA Advisory Circular 25.1309-1A — System Design Analysis, 1988
- FAA Advisory Circular 23.1309-1C*** — Equipment, Systems, and Installations in Part 23 Airplanes, 1999
- Safeware: System Safety and Computers — Nancy G. Leveson, Addison-Wesley Publishing Company, 1995
- Systematic Safety: Safety Assessment of Aircraft Systems — Civil Aviation Authority (UK), 1982

Customers routinely demand that some failures, even those associated with minor hazards, be less frequent than required by regulation — that is, the customer's requirement is more stringent than the FAA's. Economic issues such as dispatch reliability and maintenance costs are the usual motivation, and meeting the customer's specification automatically satisfies the regulatory requirement.

Some TSOs refer to third-party guidance material, usually in the form of equipment-performance specifications from organizations such as RTCA**** and the Society of Automotive Engineers. TSOs, Advisory Circulars, and these third-party specifications can explicitly call out hazard levels and software assurance levels. If such prescriptions apply to a given project, developers may simply adopt the prescriptions given for use in their own safety assessments. Developers, of course, must still substantiate their claims to the prescribed levels.

In addition to a safety assessment, an analysis of equipment reliability may be required to predict average times between failures of the equipment. Although this analysis is often performed by safety analysts, the focus is different. Whereas a safety assessment is concerned with the operational consequences and

*A given TSO might specify a software level (see Software Assurance section in this chapter), and a TSOA could certainly be granted on that basis. However, actual installation of such a device on an aircraft might require a higher software level. For example, an airspeed sensor containing Level C software could be approved under TSO-C2d, but the sensor could not then be used to supply a transport aircraft with primary air data, because that function requires Level A software.

**ARP 4754 and ARP 4761 are expected to be recognized by a new FAR/JAR advisory circular, AC/ACJ 25.1309-1B. At this writing, the advisory circular has not been adopted.

***An applicant developing avionics exclusively for general aviation airplanes should pay special attention to Advisory Circular 23.1309-1C. The Advisory Circular offers regulatory relief from many requirements that would otherwise apply. In particular, for some functions on several classes of small airplanes it allows software assurance at lower levels than would be the case for transport aircraft.

****RTCA Inc., formerly known as Radio Technical Corporation of America, is a nonprofit association of U.S.-based aeronautical organisations from both government and industry. RTCA seeks sound technical solutions to problems involving the application of electronics and telecommunications to aeronautical operations. RTCA tries to resolve such problems by mutual agreement of its members (*cf.* EUROCAE).

probabilities of system failures, a reliability analysis is concerned with the frequency of failures of particular components in a system.

23.7 Environmental Qualification

Environmental qualification is invariably required of avionics. The standard in this area is RTCA/DO-160D, "Environmental Conditions and Test Procedures for Airborne Equipment" (RTCA, 1997). DO-160D specifies testing for temperature range, humidity, crashworthiness, vibration, susceptibility to radiated and conducted radio frequencies, lightning tolerance, and other environmental factors.

It is the responsibility of applicants to identify environmental tests appropriate to their systems. Whenever choices for environmental testing are unclear, guidance from FAA personnel or DERs is in order.

To receive certification credit, environmental testing must be performed on test units whose configurations are controlled and acceptable for the tests in question. Conformity inspection may be necessary for test articles not manufactured in accordance with a production approval. An approved test plan, test setup conformity inspection, and formal witnessing of tests by FAA specialists or Designees are often required. In all cases, an applicant must document and retain evidence of equipment configurations, test setups, test procedures, and test results.

For further information on environmental testing, see Chapter 25.

23.8 Software Assurance

Software has become increasingly important in avionics development and has assumed a correspondingly higher profile in certification. It is frequently the dominant consideration in certification planning.

Regulatory compliance for software can be shown by conforming to the guidelines described in RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification" (RTCA, 1992). DO-178B was developed jointly by RTCA and the European Organisation for Civil Aviation Equipment (EUROCAE).*

DO-178B is not a development standard for software. It is an assurance standard. DO-178B is neutral with respect to development methods. Developers are free to choose their own methods, provided the results satisfy the assurance criteria of DO-178B in the areas of planning, requirements definition, design and coding, integration, verification, configuration management, and quality assurance.

DO-178B defines five software levels, A through E, corresponding to hazard classifications derived from the safety assessment discussed earlier. At one extreme, Level A software is associated with functions whose anomalous behavior could cause or contribute to a catastrophic failure condition for the aircraft. Obvious examples of Level A software include fly-by-wire primary control systems and full-authority digital engine controllers. At the other extreme, passenger entertainment software is almost all Level E, because its failure has no safety-related effects.

A sliding scale of effort exists within DO-178B: the more critical the software, the more scrutiny that must be applied to it. Level A software generates more certification data than does Level B software, Level B generates more than does Level C, and so on.

Avionics customers sometimes insist on software assurance levels higher than those indicated by a safety assessment. This is purely a contractual matter. Confusion can be avoided by separating a customer's contractual wishes from regulatory compliance data submitted to the FAA or to DERs. Certification submittals should be based on the safety assessment rather than on the contract. If a safety assessment concludes that a given collection of software should be Level C, but that software's customer wants it to be Level B, then the applicant should submit to the FAA plans and substantiating data for Level C software.

*RTCA/DO-178B is equivalent to EUROCAE/ED-12B, "Considerations sur le Logiciel en Vue de la Certification des Systemes et Equipments de Bord." (EUROCAE, 1992.)

Any additional evidence needed to demonstrate contractual compliance to Level B should be an issue between supplier and customer. That evidence is not required for certification and should become a regulatory matter only in unusual circumstances.*

FAA guidance itself sometimes requires that software be assured to a level higher than indicated by the safety assessment. This is not uncommon in equipment required for dispatch but whose failures do not threaten continued safe flight and landing. For example, a flight data recorder must be installed and operating in most scheduled-flight aircraft, but failure of a recorder during a flight would have no effect on the ability of a crew to carry on normally. Thus, from a safety assessment viewpoint, a flight data recorder has no safety-related failure conditions. Based on that, the recorder's software would be classified as Level E, implying that the software need not receive any FAA scrutiny. This, of course, violates common sense — the FAA plainly has a regulatory interest in the proper operation of flight data recorders. To resolve this mismatch, the FAA requires at least Level D compliance for any software associated with a dispatch-required function.

Digital technology predates DO-178B. Many software-based products were developed and approved before DO-178B became available. If an applicant is making minor modifications to equipment approved under an older standard, it may be possible to preserve that older standard as the governing criteria for the update. More frequently, the FAA will require new or changed software to meet the guidelines of DO-178B, with unchanged software "grandfathered" in the new approval. When transport airplanes are involved in such cases, an Issue Paper dealing with use of "legacy" software is likely to be included in the certification basis of the airplane by the FAA's Transport Airplane Directorate. In a few cases, the FAA may require a wholesale rework of a product to meet current standards.

The question of how much software data to submit to the FAA arises routinely. It is impractical to consider submitting all software data to the FAA. An applicant can realistically submit only a fraction of the data produced during software development. Applicants should propose and negotiate that data subset with the FAA. Whether submitted formally or not, an applicant should retain and preserve all relevant data (see DO-178B, Section 9.4, as a starting point). The FAA can examine applicants' facilities and data at any time. It is the applicant's responsibility to ensure that all relevant data are controlled, archived, and retrievable.

For more information on software-assurance guidelines, see Chapter 27 of this book, the FAA software home page on the World Wide Web at ⟨www.faa.gov/avr/air/air100/sware/sware.htm⟩, and the supplemental information to DO-178B published by RTCA.

In recent years, the FAA has paid growing attention to programmable logic devices: application-specific integrated circuits, field-programmable gate arrays, and so on. Findings of compliance for these devices are often handled by FAA software specialists or delegated to DERs with software authorizations. The agency's increased scrutiny is intended to ensure that acceptable processes are being followed during development of such devices. The FAA has a generic issue paper addressing compliance for the devices. If proposed electronic equipment contains programmable logic devices, an applicant should expect the FAA to tailor its generic issue paper to the project and to include the tailored issue paper in the certification basis of that project.

Though little guidance is available officially at this writing, applicants should also note that FAA concern has increased with respect to assurance of all avionics hardware design processes. A great deal of effort in industry and government has been spent to specify acceptable practices in this area, primarily through the joint efforts of RTCA Special Committee 180 and EUROCAE Working Group 46 ("Design Assurance Guidance for Airborne Electronic Hardware"). See RTCA document DO-254 (2000) for further information.

*It is usually prudent to avoid setting precedents of additional work beyond that required by regulations. Of course, applicants are always free to do additional work — developers often do, for their own reasons — and if the regulations seem inappropriate or inadequate, applicants should seek to improve the regulations. Precedents are powerful things, for both good and ill, in any regulatory regime. New precedents often have unintended and surprising consequences.

23.9 Manufacturing Approvals

It is not enough to obtain design approval for avionics equipment. Approval to manufacture and mark production units must be obtained as well. Parts manufactured in accordance with an approved production system do not require parts conformity inspections.

With a TSO, as explained earlier, the approvals of design and manufacturing actually go together. In order to receive a TSO Authorization, the applicant must demonstrate not just an acceptable prototype but also an ability to manufacture the article.

An STC holder must demonstrate production capabilities separately. After obtaining an STC approval the holder may apply for Parts Manufacturer Approval (PMA) authority to produce the parts necessary to support the STC. PMA approvals are issued by the FAA Manufacturing Inspection District Office responsible for the applicant. An STC applicant who will need subsequent PMA authority should plan and prepare for PMA from the beginning of a project. Alternatively, an STC holder may assign production rights to others, who would then hold PMA authority for the parts in question.

23.10 The Joint Aviation Authorities

The European Joint Aviation Authorities (JAA) is an influential aviation body internationally. The JAA represents European states (32 at this writing) that have agreed to cooperate in developing and implementing common safety standards and procedures for civil aviation. These standards and procedures are codified in the Joint Aviation Requirements (JARs).

Although the JAA develops and adopts JARs in the areas of aircraft operations, aircraft maintenance, and the licensing of aviation personnel, this chapter is mainly concerned with the JARs affecting aircraft design and certification. These include rules for the certification of airplanes (JAR-23, JAR-25), sailplanes and powered sailplanes (JAR-22), helicopters (JAR-27, JAR-29), engines (JAR-E), auxiliary power units (JAR-APU), and equipment (JAR-TSO).

There is a great deal of similarity between the JARs and the FARs, as well as between the JAA's and FAA's advisory material. Indeed, the JAA and the FAA made commitments in 1992 to harmonize "where appropriate, to the maximum extent possible" the JARs and FARs. The harmonization effort for airworthiness rules is expected to be completed in the year 2000. After that, the JAA and the FAA intend to engage in joint rulemaking to encourage the uniformity of new regulatory material. On at least four new aircraft programs, the JAA and the FAA have agreed to work together in a process dubbed "Cooperative and Concurrent Certification."

Still, there are differences. The following list illustrates a few of the differences:

- The JAA is not a regulatory body. Whereas the FAA defines and enforces its rules under its own authority, JAA actions are carried out through its member states and their national authorities. For example, on a development program for a new aircraft or engine, the JAA member states will assign specialists to a Joint Certification Team that acts on behalf of all the JAA members. At the successful completion of the team's evaluations, Type Certificates for the new aircraft or engine are issued not by the JAA itself, but by the member state. Thus, each Type Certificate remains a national artifact, subject to regulation by the national authority of the issuing state.
- Although JAA member countries have various forms of delegation to organizations, the JAA has no individual delegation mechanism equivalent to the FAA Designee system. Certification work is performed by JAA specialists directly or in concert with their counterparts at other non-JAA civil air authorities.
- Fees are charged to each applicant for JAA certification work.
- On some certification programs, the JAA and FAA have disagreed over the intensity of disruptive electromagnetic fields to which aircraft should be subjected during tests.
- The JAA requirements in some areas, such as operation with two engines failed on a three-engine airplane, and operation at negative load factors, differ from those of the FAA.

These examples are chosen largely at random. They serve only to illustrate that JAA/FAA harmonization is not complete. Any U.S. applicant whose certification project has a European or, for that matter any other international component, should investigate the implications thoroughly.

23.11 Summary

Certification can be straightforward, but like any other developmental activity, it must be managed. At the beginning of a project, applicants should work with their regulators to define expectations on both sides. During development, open communication should be maintained among suppliers, customers, and regulators. In a well-run project, evidence of compliance with regulatory requirements will be produced with little incremental effort, almost as a side-effect of good engineering during the normal course of work. The cumulative result will, in the end, be a complete demonstration of compliance, soon followed by certification.

Regulatory officials, whether FAA employees or Designees, work best and are most effective when they are regarded as part of an applicant's development team.

An applicant is obliged to demonstrate compliance with the applicable regulations, nothing more. However, partial information from an applicant can lead to misunderstandings and delays, and attempts to resolve technical disagreements with regulators through nontechnical means rarely have the desired effect.

In the past, regrettably, large investments have been made in systems that could not be approved by the FAA. In order to avoid such outcomes, applicants are well advised to hold early discussions with appropriate FAA personnel or Designees.

Defining Terms

Certification: Legal recognition, through issuance of a certificate by a civil aviation authority, that a product, service, organization, or person complies with that authority's requirements.

Certification basis: The sum of all current regulations applicable to a given project at the time application is made to a civil aviation authority to begin a certification process.

Designee: An individual authorized by the FAA under FAR Part 183 to act on behalf of the agency in one or more specified areas.

Issue Paper: Instrument administered by an FAA Directorate to define and control a substantial understanding between an applicant and the FAA, such as formal definition of a certification basis or a finding of equivalent safety, or to provide guidance on a specific topic, such as approval methods for programmable logic devices.

PMA: Parts Manufacturer Approval, by which the FAA authorizes the production of parts for replacement and modification, based on approved designs.

Special Condition: A modification to a certification basis, necessary if an applicant's proposed design features or circumstances are not addressed adequately by existing FAA rules; in effect, a new regulation, administered by an FAA Directorate, following public notice and a public comment period of the proposed new rule.

STC: Supplemental Type Certificate, by which the FAA approves the design of parts and procedures developed to perform major modifications to the design of existing aircraft.

TSOA: Technical Standard Order Authorization, the mechanism by which the FAA approves design data and manufacturing authority for products defined by a Technical Standard Order (see also ⟨http://www.faa.gov/avr/air/AIR100/tsohome.htm⟩).

Further Information

Certification Services, Inc.: www.certification.com
European Organisation for Civil Aviation Equipment (EUROCAE): www.eurocae.org
Federal Aviation Administration (FAA): www.faa.gov
Joint Aviation Authorities (JAA): www.jaa.nl
RTCA: www.rtca.org
Society of Automotive Engineers (SAE): www.sae.org