U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

Subject: COMPLIANCE CRITERIA FOR 14 CFR §33.28, AIRCRAFT ENGINES, ELECTRICAL AND ELECTRONIC ENGINE CONTROL SYSTEMS

Date: 6/29/01
Initiated By: ANE-110

AC No: 33.28-1
Change:

1. **PURPOSE**. This advisory circular (AC) provides guidance and acceptable methods, but not the only methods, that may be used to demonstrate compliance with §33.28 of Title 14 of the Code of Federal Regulations (14 CFR 33.28), Electrical and electronic engine control systems. Like all AC material, this AC is not, in itself, mandatory and does not constitute a regulation. While these guidelines are not mandatory, they are derived from extensive Federal Aviation Administration (FAA) and industry experience in determining compliance with the pertinent regulations.

2. **RELATED REGULATIONS**.

a. Part 21. Section 21.16.

b. Part 23. Sections 23.863, 23.901, 23.903, 23.1181, and 23.1309.

c. Part 25. Sections 25.863, 25.901, 25.903, 25.939, 25.1181, and 25.1309.

d. Part 27. Sections 27.863, 27.901, 27.903, and 27.1309.

e. Part 29. Sections 29.863, 29.901, 29.903, 29.1181, and 29.1309.

f. Part 33. Sections 33.4, 33.5, 33.17, 33.19, 33.27, 33.28, 33.49, 33.53, 33.75, 33.91(a), and Appendix A of part 33.

3. **RELATED REFERENCE MATERIAL**.

a. ACs, Notices, and Policy.

(1) AC 20-53A, Protection of Aircraft Fuel Systems Against Fuel Vapor Ignition Due to Lightning, dated April 12, 1985.

(2) AC 20-115B, RTCA, Inc. Document RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification, dated January 11, 1993.

(3) AC 20-136, Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning, dated March 5, 1990.

(4) AC 21-16D, RTCA/DO-160D, Environmental Conditions and Test Procedures for Airborne Equipment, dated July 21, 1998.

(5) AC 23.1309-1C, Equipment, Systems, and Installations in Part 23 Airplanes, dated March 12, 1999.

(6) AC 25.1309-1A, System Design Analysis, dated June 21, 1988.

(7) AC 33-2B, Aircraft Engine Type Certification Handbook, dated June 30, 1993.

(8) AIR-100 Policy, High Energy Radiated Electromagnetic Fields (HERF), Interim Policy Guidelines on Certification Issues, dated 5 December 1989.

(9) Notice N8110.71, Guidance for the Certification of Aircraft Operating in High Intensity Radiated Field (HIRF) Environments, issued April 2, 1998.

(10) Engine and Propeller Directorate Policy, Time Limited Dispatch (TLD) of Engines Fitted with Full Authority Digital Engine Controls (FADEC) Systems, dated June 29, 2001.

(11) Engine and Propeller Directorate Policy Regarding Integrated Full Authority Digital Engine Control (FADEC) and Electronic Propeller Control (EPC) Systems, dated January 30, 1995.

b. Industry Documents.

(1) RTCA Document No. DO-160D (EUROCAE ED14D), Environmental Conditions and Test Procedures for Airborne Equipment, dated July 29, 1997.

(2) RTCA Document No. DO-178B (EUROCAE ED12D), Software Considerations in Airborne Systems and Equipment Certification, dated December 1, 1992.

(3) RTCA Document No. DO-254, Design Assurance Guidance for Airborne Electronic Hardware, dated April 19, 2000.

(4) SAE ARP 926/B Fault/Failure Analysis Procedure, issued June 1997.

(5) SAE ARP 1834/A Fault/Failure Analysis for Digital Systems and Equipment, issued June 1997.

(6) SAE ARP 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems, issued November 1996.

(7) SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, issued December 1996.

(8) SAE ARP 5107, Guidelines for Time-Limited-Dispatch Analysis for Electronic Engine Control Systems, issued June 1997.

(9) IEC/PAS 62239, Electronic Component Management Plans, edition 1.0, dated April 2001.

(10) IEC/PAS 62240, Use of Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges, edition 1.0, dated April 2001.

c. Military Specifications.

(1) MIL-STD-461E, Requirements for the Control of Electromagnetic Interference Characteristics of the Subsystems and Equipment, dated August 20, 1999.

(2) MIL-STD-462D, Measurement of Electromagnetic Interference Characteristics, Test Standard For**,** dated February 5, 1996.

(3) MIL-STD-810E, Environmental Test Methods and Engineering Guidelines, dated July 31, 1995.

(4) MIL-STD-5007D, Engines, Aircraft, Turbojet and Turbofan, General Specification For, dated October 15, 1973.

(5) MIL-HDBK-179A, Microcircuit Acquisition Handbook, dated July 20, 1995.

(6) MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, dated February 28, 1995.

4. **APPLICABILITY**. This AC applies to electrical and electronic engine control (EEC) systems used on aircraft engines certificated under 14 CFR part 33 and intended for use in aircraft certificated under parts 23, 25, 27, and 29. This document also applies to any electrical or electronic systems that control an engine function, for example overspeed or temperature limiting systems. In some cases, controls for functions not normally covered under part 33 or required for engine control are integrated into the EEC (for example, propeller controls regulated under part 35). In these cases, this document also applies to those functions integrated into the EEC system, but only to the extent that those functions affect part 33 requirements. Although sections of this AC provide guidance for compliance with §33.28 for all EECs, the FAA is developing specific guidance for reciprocating engine controls.

Original Signed by JJP on 6/29/01
Jay J. Pardee
Manager, Engine and Propeller Directorate,
Aircraft Certification Service

CONTENTS

Paragraph Page

CHAPTER 1. GENERAL

CHAPTER 2. SECTION 33.28(a)

CHAPTER 3. SECTION 33.28(b)

CHAPTER 4. COMPLIANCE WITH §33.28(b): FAILURE OF AIRCRAFT-SUPPLIED DATA

CHAPTER 5. COMPLIANCE WITH §33.28(b): FAILURE OF AIRCRAFT-SUPPLIED POWER

CHAPTER 6. SECTION 33.28(c)

CHAPTER 7. SECTION 33.28(d)

CHAPTER 8. SECTION 33.28(e)

CHAPTER 1. GENERAL

1-1. Background.

a. Section 33.28 was added to part 33, Airworthiness Standards for Aircraft Engines, as Amendment 15 (58 FR 29095, 5/18/93) and became effective on August 16, 1993. An accompanying advisory circular (AC) was not issued at the time.

b. Initially, EEC technology was primarily applied to engines designed for large transport aircraft applications. The certification practice and implementation of §33.28 was oriented toward these applications. When the use of EEC technology was limited to a small group of manufacturers, the information and guidance provided in the rule itself was adequate. Since the use of EEC controls has spread, a need for an AC has become evident in several recent engine certification programs.

c. In addition, industry representatives from the engine community that design engines for applications other than large transport aircraft certificated under part 25 have questioned the criteria used to determine equivalence to the typical hydromechanical system. A basic criteria for FAA acceptance of the replacement of hydromechanical technology with electronic technology for engine controls is that the new technology must have an equivalent level of integrity and reliability as the technology being replaced. Because the data used to establish the criteria for equivalent reliability of a typical hydromechanical system was based on part 25 certification experience, other industry representatives have presented a valid argument that the equivalence criteria to a hydromechanical system should be based on data for hydromechanical control systems used in their respective part 23, 27, and 29 certifications.

1-2. Introduction. One of the objectives for the engine manufacturer in an engine certification program is to show that the certificated engine will be “installable” in a particular aircraft or aircraft type. If the aircraft application is unknown at the time of engine certification, the engine manufacturer should make reasonable installation and operational assumptions for the anticipated aircraft application.

a. To facilitate achieving this objective, the engine manufacturer should provide a document that describes the EEC system and its operation to both the engine certification office (ECO) and the aircraft certification office (ACO). Using this document, along with other documentation and test results, the ACO will determine if the EEC system has reasonable assurance of being in compliance with the applicable aircraft certification regulations (§§ 901, 903, and 1309 of parts 23, 25, 27, 29).

b. Providing the EEC documentation to the ACO is particularly important when the system is novel or unique and differs from previously certificated systems. The ECO will also coordinate with the appropriate FAA engine controls specialist(s) in this regard. If these reviews indicate that the engine may not be installable in the intended aircraft type, the ECO will inform the applicant and the appropriate ACO of any potential certification issues. The final determination for compliance with these aircraft regulations will be determined by the appropriate ACO at

aircraft certification, when more complete test and analysis data is available. This coordination with the ACO is only necessary for the initial aircraft application of the engine. If an aircraft is not identified as the anticipated installation for the engine, a review may be conducted with the applicable Standards Staff. Any installation limitations or operational issues will be noted in the engine Installation or Operational Manuals and the engine Type Certification Data Sheet (TCDS). Applicants should also be aware that the ACO may require flight testing to fully evaluate engine performance and operability characteristics for all operating modes.

1-3. Definitions.

a. Aircraft-Supplied Data. Aircraft-supplied data is information that is generated in the aircraft systems and used by the engine control system, but whose source is not controlled under the design authority of the engine certification applicant. This does not include input from those sensors that are used by, and normally dedicated to, the engine control system but may be mounted in the airframe.

b. Aircraft-Supplied Power. Aircraft-supplied power is any electrical power source that is an integral part of the aircraft electrical system and whose primary function is to power aircraft systems (for example, an electrical bus).

c. Alternate Control Mode(s). For the purposes of this AC, an alternate control mode is one in which the operating characteristics or capabilities of the engine control are sufficiently different from the "normal mode" that they may significantly impact or change the operating characteristics or capabilities of the aircraft, crew workload, or what constitutes appropriate crew procedures.

d. Commercial and Industrial Grade Electronic Parts. Commercial (consumer quality parts) and industrial grade electronic parts have typical operating ranges of 0 degrees to $^{+}70$ degrees Celsius and $^{-}40$ degrees to $^{+}85$ degrees Celsius, respectively. Vendor parts catalogs typically define commercial and industrial grade electronic parts in these temperature ranges.

e. Electronic Engine Control (EEC) System. The EEC system is the generic family of electrical/electronic engine control systems, including full authority digital engine controls, supervisory controls, and derivatives of these.

f. Fault or Failure. This is an occurrence that affects the operation of a component, part, or element such that it can no longer function as intended, and includes both loss of function as well as a malfunction. Errors that may cause failures are not considered as failures.

g. Fault or Failure Accommodation. This term refers to the capability of the control system or crew to mitigate, either wholly or in part, the failure condition.

h. Fault or Failure Condition. This is a condition having an effect on the airplane or its occupants, either direct or consequential, that is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

i. Fault or Failure Detection. This term refers to the discovery of a fault or failure condition and either announcement of that condition to the flight crew by instrumentation or storage of the detection of that condition, or its results, in a fault memory for later retrieval through a built-in test capability of that control.

j. Full Authority Digital Engine Control (FADEC). FADEC is a control system in which the primary functions are provided electronically and the electronic unit has full-range authority over the engine power or thrust. FADEC systems have been certificated that employ either two identical channels to provide full-operational capability after failure of one channel or a single channel with a simplified electronic or hydromechanical back-up to provide an alternate operating mode. The "FADEC system" includes all the control elements identified in the instruction manual, including: sensors, wiring, mechanical, pneumatic, or hydromechanical components and other limiter or protection devices. If the control requires data from aircraft computers to operate, this data is considered part of the EEC or FADEC system, and the interface requirements for this data should be specified in the engine instruction manual. Mechanical components, such as the fuel pump, that do not interface with the EEC system are generally not included in the definition of FADEC system components.

k. Full-up System or Configuration. For the purposes of the system safety assessment (SSA) analyses described in this AC, the "full-up system" is one that does not have any faults or failures present, detected or undetected, that affect the control of engine power or thrust, engine protection systems, indication of critical engine operating parameters or other safety features of the control. In a "full-up system," everything is operative.

l. Loss of Thrust Control (LOTC). For engines intended for use in airplanes certified under part 23 Commuter Category standards, or part 25 standards (Transport Category), and in rotorcraft certified under part 27 or part 29 standards, this term refers to the loss of capability to modulate and maintain thrust or power between flight idle and 90 percent of maximum rated power or thrust at all operating conditions. For engines intended for use in airplanes certified under part 23 Normal, Utility, or Acrobatic standards, this term refers to the loss of capability to modulate and maintain thrust or power between flight idle and 85 percent of maximum rated power or thrust, at all operating conditions. One engine inoperative (OEI) or automatic take-off thrust control system (ATTCS) ratings and implementations are exempted from an LOTC analysis, because the portion of time spent at these ratings is relatively small, and they are covered by aircraft level analyses.

m. Per Hour. When the term "per hour" or "per flight hour" is used in this AC, the definition is "per engine flight hour."

n. Range of Control. This term refers to modulation of the engine from idle to 100 percent maximum rated thrust or power and includes any red line or higher rotor speed protection controls and any engine temperature, torque, and pressure limits set and implemented by the control.

o. Take-off Envelope. This term refers to the operation of the aircraft at or below 1500 feet above ground level (AGL) during take-off or landing approach. When distant obstacle clearance is involved, the take-off envelope may be increased to a higher altitude than 1500 feet AGL. For rotorcraft, the take-off envelope is 1000 feet AGL for Category A rotorcraft, and within the height-velocity envelope for all others.

p. Uncovered Fault. An uncovered fault is a fault or failure for which either a detection mechanism does not exist or, if there is a detection mechanism, an accommodation does not exist.

q. Unsafe Condition. For purposes of this AC only, an unsafe condition is a condition that, if not corrected, is reasonably expected to result in one or more serious injuries. In this definition, "reasonably expected" means a probability of occurrence unacceptable to both the long-term risk and the intent of the applicable Type Design Standards.

CHAPTER 2. SECTION 33.28(a)

2-1. Rule Text. Section 33.28(a) provides that each EEC must: "Have the control system description, the percent of available power or thrust controlled in both normal operation and failure conditions, and the range of control of other controlled functions, specified in the instruction manual required by §33.5 for the engine."

2-2. Intent of Rule. Section 33.28(a) requires the applicant to provide the necessary information in the form of manuals to ensure safe engine installation and safe engine operation. The data underlying the information provided in the manuals should be created as part of the engine certification program. The manuals should include the following:

a. EEC system information that provides a clear understanding of the control system in the normal and any alternate control or operating modes;

b. Any differences in operation in other than the normal mode;

c. Any subtle interface requirements, such as power interrupt tolerance of the EEC;

d. Percent of available power or thrust in both normal operation and any alternate modes;

e. Range of control of other controlled functions; and

f. The environmental limitations of the engine installation.

2-3. Compliance with §33.28(a). The following is a method, but not the only method, of compliance with §33.28(a):

a. Control System Description. The applicant should include a brief control system description in the instruction manual and may incorporate a more detailed system description document by reference. The applicant should also consider other functions integrated into the EEC system. If functions other than those directly associated with the control of the engine are integrated into the EEC system, (such as thrust reverser control, propeller control, or automatic starting) the applicant should include descriptions of these functions in the instruction manual. Even if the FADEC control is integrated wholly or in part within an aircraft avionics system, the engine manufacturer should provide an engine control system description that meets part 33 engine certification requirements and should include the relationship of the engine control system and the aircraft systems. Engine control systems that are embedded in aircraft avionics may require special conditions as prescribed under §21.16.

b. Interface Description. The instruction manual should include installation interface descriptions, limitations, and requirements of the engine control system. For example, the instruction manual should clearly define the EEC power requirements and quality, including interrupt limitations, for the engine installer. The manual should also specify the impedance and buffering limitations for the signals provided by the EEC system for display and instrumentation, or signals used by the EEC, such as air data information, to ensure that the EEC system is adequately isolated and unaffected by other systems using these signals.

c. Operational Description.

(1) The instruction manual should:

(a) Describe the control system operating characteristics in both the normal and alternate control modes.

(b) Define restrictions in the flight envelope or unusual operating characteristics in these alternate modes.

(c) Identify any abnormal control characteristics in all operational or dispatchable configurations that could have an impact on crew procedures, training, workload, or any other aspect of aircraft performance or operating characteristics, for evaluation during aircraft certification.

(2) If dispatch of the control system with faults has been approved by a time-limited-dispatch (TLD) analysis or other analyses, the instruction manual, or other appropriate documentation, should include the time limitations for this type of operation. If TLD or other appropriate analysis or documentation is not submitted to substantiate the acceptability of dispatching the engine control with faults present or portions of the control inoperative, the control may be restricted to “full-up” dispatch only.

(3) Faults that leave the control in a condition that cannot meet part 33 performance and operability requirements are generally considered non-dispatchable. The instruction manual should indicate how the EEC system would announce that condition to the flight crew. It should also describe how the control system provides output information for such a condition.

(4) The instruction manual should describe the availability of information about ECO-approved dispatchable fault conditions, and the time limits approved for such operations. ECO approval of a particular fault condition as dispatchable does not guarantee that the ACO or the operator’s certificate management office will approve that same condition as dispatchable for the aircraft or operator.

d. Substantiating Data. The instruction manual should include data from analyses conducted to comply with §§33.28(b) and (c), data from the environmental testing conducted to comply with §33.28(d), and data from the software level determinations conducted to comply with §33.28(e). This data will assist the installer in safely installing the engine. The applicant should have available and provide, as required, the following specific data:

(1) Data for all operating modes, to demonstrate that the control meets its design intent.

(2) Data to show that a progressive means of increasing power or thrust with throttle or load demand is provided for all control modes.

(3) Data for the following:

(a) The software level (for each function, if necessary).

(b) The estimated failure rates for:

1. Engine shut-down in-flight due to engine control causes.

2. Loss of engine or propeller control or significant change in power or thrust.

3. Failures to the back-up system.

4. Transmission of faulty parameters that affect cockpit located engine displays, or other safety critical functions.

5. Loss of any critical safeguards, such as overspeed or valves needed for fire protection.

6. Loss of any aircraft-supplied data or power required to assure proper engine operation.

7. Other safety significant failure conditions, such as the probability of an uncontrolled overspeed and the other control system associated events as determined from the system safety analysis (SSA). A control system event is one that the control system causes or is involved in preventing.

(4) The types and levels of environmental exposure for which the EEC system has been successfully qualified; for example, vibration, temperature, HIRF, and lightning. For new applications of a previously certified control system, substantiation of the environmental capability of the EEC system by similarity analyses, as well as tests, may be acceptable. The certification approach to be pursued should be indicated in the certification plan. For HIRF, lightning and electromagnetic interference (EMI) qualification tests, the interfacing aircraft cables used for the tests should be described.

e. Fault Accommodation Logic Data. The applicant should have available and provide, as required, the following:

(1) A tabulation of the fault accommodation logic for the critical parameters used by the control; and

(2) A tabulation of the "default" or "fail-safe" states of all EEC system outputs, and the rationale for their selection.

CHAPTER 3. SECTION 33.28(b)

3-1. Rule Text. Section 33.28(b) provides that each EEC system: "Be designed and constructed so that any failure of aircraft-supplied power or data will not result in an unacceptable change in power or thrust, or prevent continued safe operation of the engine."

3-2. Intent of Rule. Section 33.28(b) requires that the engine and control system continue to function in a safe and reliable manner in the event of the failure of aircraft-supplied power or data, or both, while providing sufficient flexibility to accommodate the increasing engine and aircraft integration that accrues from the use of electronic control technology. For single engine installations, the effects should be reviewed as part of the overall safety and reliability objectives of §33.28(b).

a. Unacceptable Change in Power or Thrust. An "unacceptable change in power or thrust" is a change that has a significant impact on the performance margins of the intended application. Although the complete or partial loss or change of thrust or power in a single engine installed on a multi-engine aircraft is not necessarily an unsafe condition, the ECO will evaluate both partial and complete loss of power or thrust. This evaluation includes the frequency, duration, and percentage of power or thrust change that results from the failure of aircraft-supplied data or power. This evaluation also considers location in the flight regime at the time of the event. The applicant should provide analytical or test data for this evaluation. The data may include worst case plots of percentage power or thrust change over the declared operating envelope for failure of aircraft-supplied data or power.

b. Continued Safe Operation of the Engine. In case of loss, corruption or failure of aircraft-supplied data or power, the engine should continue to function in a safe and acceptable manner, without unacceptable effects on thrust or power, hazardous engine effects, or loss of ability to comply with the operating requirements of §§33.51, 33.65 and 33.73.

CHAPTER 4. COMPLIANCE WITH SECTION 33.28(b): FAILURE OF AIRCRAFT-SUPPLIED DATA

4-1. Failure of Aircraft-Supplied Data. The following guidance provides a method, but not the only method, of compliance with §33.28(b) for failure of aircraft-supplied data. The applicant should define in the instruction manual the effect of the failure of aircraft-supplied data on the engine's output power or thrust characteristic throughout the flight envelope. That data should be provided for all allowable engine control and aircraft dispatch configurations in which the loss of aircraft power or data in that dispatch configuration would result in a different engine control system response.

4-2. System Configurations. Examples of system configurations that have been found to be acceptable under §33.28(b) include the following:

a. Dual Sources. A system may use dual sources of aircraft-supplied data with local engine sensors provided as "voters" and alternate data sources. Sensors that act as "voters" provide a method for the EEC system to determine if one of the primary data sources is providing erroneous data, and to then eliminate that erroneous source from consideration. In the event of a failure in the aircraft-supplied data, the engine sensors act as the primary source of sensed data through the fault accommodation logic. In the event of the loss of this engine-sensed data, the system uses modeled or synthesized parameters.

b. Synthesized Engine Parameters. In some cases, a system may use synthesized engine parameters as voters. The applicant should provide data that gives the worst case percentage change of power or thrust over the declared operating envelope when inaccuracies of the synthesizing process are considered, as well as the environmental effects on the sensors used in the synthesis.

c. Third Source. A system may use a third source of aircraft-supplied data as the voter instead of engine sensors. In this case, when aircraft data is used exclusively, the applicant should address the following items, as applicable, in the SSA or other appropriate documents:

(1) Software in the data path to the EEC should be at a level consistent with that defined for the EEC. The data path may include other aircraft equipment, such as aircraft air data computers (ADC), thrust management computers, or other avionics equipment.

(2) The applicant should state in the instruction manual that the aircraft manufacturer must ensure that changes to aircraft equipment, including software, in the data path to the engine do not affect the integrity of the data provided to the engine as defined by the instruction manual.

(3) If dispatchability of the aircraft without the third source is anticipated, the applicant should provide analysis that demonstrates the acceptability of this dispatch configuration for the minimum maintenance equipment list (MMEL) or the TLD documents, as applicable.

(4) Since aircraft-supplied data has an effect on EEC system operation, the applicant should supply the effects of faulty and corrupted aircraft data on the EEC system in the engine instruction manual. In the three ADC configuration the EEC system could be significantly affected by erroneous or faulty air data information; the engine could experience a significant thrust or power change during such a condition. If this is the case, the applicant should indicate in the instruction manual that air data information, and any other aircraft information that could have a significant impact on engine thrust or power, is considered critical to EEC system operation. Therefore, the instruction manual should state that the installer should ensure that those sensors and equipment involved in delivering information to the EECs are capable of operating in the "severe" HIRF and lightning environments, as defined in the certification basis for the aircraft, without affecting their proper and continued operation.

(5) The applicant should state the reliability level for the aircraft-supplied data that was used as part of the SSA and LOTC analysis as an "assumed value" in the instruction manual.

4-3. Complete Loss of ADC Inputs. The applicant should provide fault accommodation logic for the complete loss of ADC inputs or other aircraft-supplied data, even though this loss may be extremely improbable. In this case, the applicant should conduct sufficient testing or analysis, or both, on the fault accommodated control mode to establish that the engine operating characteristics comply with all operability requirements of part 33.

4-4. Common Mode Faults. In the exchange of data with the aircraft, consideration should be given to elimination of unacceptable common mode faults affecting the operation of more than one engine or propeller. This AC describes limits for unacceptable common mode faults that affect power or thrust in the discussion of §33.28(c). Common faults that affect engine protection limit systems or could hazard the aircraft would generally be unacceptable. The applicant should demonstrate the logic included in the control system to accommodate common faults. Any precautions needed to address common effects should be taken either through the aircraft system architecture or by logic internal to the engine control system. This should be demonstrated as part of the software integration testing during the EEC software verification or EEC system validation test program. Specifically, the applicant should consider the following cases:

a. Erroneous data received from the aircraft by the engine or propeller control system, if the data source is common to more than one engine or propeller; for example, air data sources, autothrottle systems, and synchronizing controls.

b. Control system operating faults propagating through data links between engine or propeller; for example, maintenance recording, common bus, cross-talk, auto-feathering, and automatic power reserve system.

c. Loss or interruption of aircraft data or electrical power used by the engine control, when that loss or interruption is caused by the failure of another engine.

d. Exchange of data between engines to implement control functions, (for example, load sharing and synchrophasing) should be shown to incorporate authority limits to prevent unacceptable common mode loss of power or thrust.

4-5. System Integration. The trend toward system integration may result in EEC systems that use resources distributed within the aircraft in addition to aircraft-supplied data. In these cases, the office responsible for certifying the engine would expect the engine manufacturer to specify the requirements for the EEC system and substantiate the adequacy of those requirements. The engine manufacturer should specify these requirements in the engine instruction manual to ensure that the engine certification basis is maintained.

a. Integration Activities.

(1) Aircraft Functions Integrated into the Engine Control System. This activity involves the integration of aircraft and propeller control functions (that is, those that have traditionally not been considered engine control functions) into the EEC system's hardware and software.

(a) Examples of this integration include: thrust reverser controls; propeller speed governors, which govern speed by varying pitch; and ATTCS systems. When this type of integration activity is pursued, the EEC system becomes part of, and should be included in, the aircraft's SSA. Although the aircraft functions incorporated into the EEC system may receive review at engine certification, the acceptability of the safety analysis involving these functions would be determined at aircraft certification.

(b) The EEC system may be configured to contain only part of the aircraft system's functionality, or it may contain virtually all of it. Thrust reverser control systems are an example in which only part of the functionality is included in the EEC system. In such cases, the aircraft is configured to have separate switches and logic (independent from the EEC system) as part of the thrust reverser control system. This separation of reverser control system elements and logic provides an architectural means to limit the criticality of the functions provided by the EEC system.

(c) However, in some cases the EEC system may be configured to incorporate virtually all of a critical aircraft function. Examples of this "virtual completeness" in aircraft functionality are EEC systems that contain full authority to govern propeller speed in turboprop-powered aircraft and ATTCS systems in turbofan-powered aircraft.

1. The first of these is considered critical because, if an engine fails, the logic in the engine control must be configured to feather the propeller on that engine. Failure to rapidly feather the propeller following an engine failure results in excessive drag on the aircraft; such a condition could be critical to the aircraft.

2. The ATTCS system in turbofan-powered aircraft is considered critical because it is required to increase the thrust of the remaining engine(s) following an engine failure during take-off. The increased thrust on the remaining engines is necessary to achieve the required aircraft performance.

(d) All of these examples of integration involve aircraft functions that would receive significant review during aircraft certification.

(2) Engine Control Functions Integrated into Aircraft Systems. The trend toward systems integration may lead to aircraft systems performing functions traditionally considered part of the engine control.

(a) Some limited designs may have functions traditionally considered part of the engine control system provided by the aircraft, but the EEC system itself, which is part of the type design, provides all the functions required to safely operate the engine in accordance with parts 33, 35, and other applicable regulations. An example of such a "limited design" is an engine control that receives a torque output demand signal from the aircraft and responds by changing the engine's fuel flow and other variables to meet that demand.

(b) Other designs may use aircraft systems to provide a significant number of the engine control system functions. An example of this design is the complex integration of flight and engine control systems (integrated in aircraft avionics units) that govern engine speed, rotor speed, rotor pitch angle, and rotor tilt angle in tilt-rotor aircraft.

(c) Functions provided by the engine system, which is part of the engine type design, would be certified with the engine; functions provided by the aircraft would be certified with the aircraft.

(d) In these designs, aircraft systems may be an integral part of engine regulatory compliance. In such cases, the engine applicant should specify the requirements for the EEC system and substantiate the adequacy of those requirements. The applicant should define these requirements in the engine instructions for installation; the requirements would then become part of the engine type design.

b. Certification Activities.

(1) Objective. To satisfy the aircraft requirements (§§ 901, 903, and 1309 of parts 23, 25, 27, and 29), the consequences of failures of the engine control system on the aircraft must be analyzed. The engine manufacturer and aircraft manufacturer should ensure that the software levels and safety and reliability objectives for the EEC system are consistent with the associated aircraft requirements. The use of electronic technology consistently results in greater integration of engine, propeller, and aircraft systems. For example, in some applications the EEC unit may integrate the control functions for the propeller, or the aircraft computers may integrate the engine control and the propeller control functions. The appropriate engine, propeller, and aircraft certificating offices should define the respective certification tasks of the engine, propeller, and aircraft manufacturers.

(2) Interface Definition and System Responsibilities. Interface definitions and system responsibilities should be identified in the appropriate documents for the functional and hardware and software aspects of the engine, propeller, and aircraft systems. The applicants should summarize these responsibilities in the respective engine, propeller, and aircraft certification plans. Specifically, the engine/propeller/aircraft documents should identify:

(a) Functional requirements and criticality (that may be based on engine, propeller and aircraft considerations).

(b) Fault accommodation strategies.

(c) Maintenance strategies.

(d) The software quality level (per function if necessary).

(e) The reliability objectives for:

1. LOTC events; and

2. Transmission of faulty parameters.

(f) The environmental requirements, including the degree of protection against lightning or other electromagnetic effects (for example, the level of induced voltages that can be supported at the interfaces).

(g) Engine, propeller, and aircraft interface data and characteristics.

(h) Aircraft electrical power supply requirements and characteristics (if relevant).

(3) Distribution of Compliance Tasks.

(a) The tasks for the certification of the aircraft propulsion system equipped with electronic controls should be shared between the engine, propeller, and aircraft manufacturers. The manufacturers should identify the distribution of these tasks in their respective certification plans for the approval of the appropriate engine, propeller, and aircraft authorities.

1. The aircraft certification should address the overall integration of the engine and propeller in compliance with the applicable aircraft requirements.

2. The engine and propeller certification plans should address the functional aspects of the engine and propeller control systems for compliance with the applicable engine and propeller control system requirements.

(b) Evidence provided for engine certification could be used for aircraft certification, if appropriate. For example, if the applicant has demonstrated the quality of any aircraft-implemented software and aircraft/engine interface logic for engine or propeller certification, additional substantiation for aircraft certification should not be necessary.

(c) For example, if an EEC unit were performing the functions for the control of the engine and the functions for the control of the propeller:

1. The engine certification would address all general requirements such as software quality assurance procedures, EMI/lightning protection levels, and effects of loss of aircraft supplied power.

2. The engine certification would address the functional aspects for the engine functions such as safety analysis, rate for LOTC events, and effect of loss of aircraft supplied data. For example, the fault accommodation logic affecting the control of the engine would be reviewed at that time.

3. The propeller certification would similarly address the functional aspects for the propeller control functions. For example, the fault accommodation logic affecting the control of the propeller would be reviewed at that time.

4. In this example, the propeller functions and characteristics that the propeller manufacturer defines as provided by the engine control system would normally need to be refined during flight test. However, the propeller manufacturer is responsible for ensuring that these requirements that would be certificated as part of the engine certification program, although not refined during flight test, define an airworthy configuration. The Engine and Propeller Directorate Policy Regarding Integrated Full Authority Digital Engine Control (FADEC) and Electronic Propeller Control (EPC) Systems, dated June 30, 1995, provides additional clarification.

5. All manufacturers involved should agree on the change control process, so that changes to the engine control system that affect the propeller system or changes to the propeller control system that affect the engine control system do not lead to an inadvertent change to the type design of either system.

(d) For example, if an aircraft computer were performing the functions for the control of the engine, the propeller, or both:

1. The aircraft certification would address all general requirements such as software quality assurance procedures and EMI/lightning protection levels.

2. The aircraft certification would address the functional aspects for the aircraft functions.

3. The engine certification would address the functional aspects for the engine functions (such as safety analysis, rate for LOTC events, and effect of loss of aircraft supplied data). For example, the fault accommodation logic affecting the control of the engine would be reviewed at that time.

4. The propeller certification would address the functional aspects for the propeller control functions (such as safety analysis, contribution to LOTC events, and effect of loss of aircraft supplied data). For example, the fault accommodation logic affecting the control of the propeller would be reviewed at that time.

4-6. Fault Accommodation Logic. The applicant should perform an SSA to determine the adequacy of the EEC fault accommodation logic. The applicant should also demonstrate the functionality of the fault accommodation logic; this demonstration may be conducted as part of the system integration testing.

4-7. Control System Elements Mounted in the Aircraft. Elements of the control system that are mounted in the aircraft may be powered by and dedicated to the EEC, such as a throttle position transducer. In this case, the element would be considered an integral component of the EEC system, and faults should be accommodated as part of the EEC, rather than accommodated as aircraft-supplied data. The applicant should document the method used for addressing single and dual failures of these signals and demonstrate the fault accommodation for these signals. The demonstration may be conducted as part of the software integration testing during the EEC software verification testing.

CHAPTER 5. COMPLIANCE WITH SECTION 33.28(b): FAILURE OF AIRCRAFT-SUPPLIED POWER

5-1. Failure of Aircraft-Supplied Power. The following guidance provides a method, but not the only method, of compliance with §33.28(b) for failure of aircraft-supplied power for engines intended for multiple engine installations.

a. The applicant should demonstrate that the EEC control system can continue to function normally with the failure or interruption of aircraft-supplied power at any point within the declared engine operating envelope.

b. The capacity of any engine dedicated power source required for compliance with §33.28(b) should provide sufficient margin to ensure that the engine control system would continue to function in all anticipated engine operating conditions in which the control system is designed and expected to recover engine operation in-flight. This margin should account for any other anticipated variations in the output of the dedicated power source, such as those due to temperature variations, manufacturing tolerances, and idle speed variations. The applicant should substantiate the design margin by test, analysis, or a combination of both. This substantiation should consider deterioration over the life of the engine.

5-2. All Engine Out Restart Requirement. If aircraft-supplied battery power is required to meet an "all engine out" restart requirement, an analysis should result in a definition of the requirements for this aircraft-supplied power. In any application in which aircraft electrical power is used to operate the engine control system (such as low engine speed in-flight re-starting conditions), the effects of any aircraft electrical bus-switching transients or power transients associated with application of electrical loads, which could cause an interruption in voltage or a decay in voltage below that level required for proper control functioning, should be considered.

5-3. Exceptions. Some engine control functions that have traditionally relied exclusively upon aircraft electrical power are excepted from compliance with this aspect of §33.28(b) because their good service history indicates they provide an equivalent level of safety. The loss of power requirement of §33.28(b) applies to the ability to control the functions exempted, for example, anti-icing and ignition. The exception applies only to the electrical power necessary to drive the function. The applicant should define in the instruction manual the impact of the failure of aircraft-supplied electrical power on the output power or thrust characteristics of the engine throughout the flight envelope. The following are examples of these excepted functions:

a. Non-critical functions;

b. Engine start;

c. Ignition;

d. Thrust reverser;

e. Anti-icing; and

f. Fuel shut-off.

5-4. Aircraft-Supplied Power as Backup Power. In the event of an alternator failure, aircraft-supplied power may be used as a source of backup power for the dedicated engine-mounted alternator. If the control is not required to have a dedicated power source and uses aircraft power as its normal power supply (such as a system with a full hydromechanical back-up), and the transition from the electronic to the hydromechanical control is acceptable, then this does not apply.

5-5. Control Systems Integrated with Avionics. For control systems integrated with avionics, aircraft-supplied power may be used as primary power for the EEC. The power should be able to meet the EEC quality and reliability requirements for operating the engine under all normal electrical load conditions (such as no dropout during engine/APU start and bus switching). The EEC should also have backup power from a battery capable of allowing a safe landing after loss of all generators and alternators, without loss of engine control. The required amount of battery backup power should be determined from the maximum certificated altitude of the aircraft and should include at least one missed approach and go-around.

CHAPTER 6. SECTION 33.28(c)

6-1. Rule Text. Section 33.28(c) provides that each EEC must: "Be designed and constructed so that no single failure or malfunction, or probable combination of failures of electrical or electronic components of the control system, results in an unsafe condition."

6-2. Intent of Rule. Section 33.28(c) ensures that the complete engine control system, including the electrical and electronic parts, provides a system that is considered equivalent in safety and reliability to engine control systems that are based on hydromechanical technology.

a. Current regulations (based on hydromechanical technology) rely on testing and mechanical inspection intervals to ensure control system reliability and airworthy operation. Electronic technology does not lend itself to mechanical inspection. Therefore, to ensure safe operation after an electrical or electronic component failure, redundancy techniques and self-monitoring have been required in EEC systems to achieve equivalent control system integrity. The predicted reliability of the control system should be determined by completing a loss-of-thrust-control (LOTC) analysis of the system.

b. Previous EEC systems have used the design approach of showing that the EEC system is essentially single fault tolerant with respect to electrical or electronic failures when establishing safety and reliability equivalence to conventional hydromechanical systems. The word "essentially" is used because it may not be practical to accommodate all failures. In the TLD analysis a two to five percent default value is assigned in some cases to these uncovered faults for a full dual channel redundant system. The value used should be substantiated by tests, analysis, or both.

6-3. Compliance with §33.28(c). The objective in accepting the transition from hydromechanical control (HMC) technology to electronic control technology is to maintain at least an equivalent level of system reliability and safety. The following guidance provides a method, but not the only method, of compliance with §33.28(c).

a. Engine Controls for Different Aircraft and Rotorcraft Applications.

(1) Part 25 Aircraft Applications (and Part 23 Aircraft Applications Certifying to Part 25 Rules). For engines intended for use in transport aircraft, the criteria used in early certification programs to establish that an EEC had an equivalent level of safety and reliability to an HMC was that an EEC system should not cause more than one LOTC event per 100,000 engine operating hours. In addition, compliance with an LOTC criteria of 100,000 hours per event would generally meet the aircraft level requirement of §25.1309(b)(1). This section requires that any aircraft system failures that would prevent continued safe flight and landing of the airplane must be extremely improbable. EECs that comply with the LOTC criteria should comply with this aircraft rule (that is, have a failure probability of 10^{-5} for a flight duration of one hour that would yield the probability $(10^{-5})^2$ for the failure of both EECs. This is less than the 10^{-9} failure limitation described in AC 25.1309-1A for catastrophic failures. Redundancy techniques may be

provided in the system by electronic, HMC, or other means. Generally, engines designed for installation on transport category airplanes use a fully capable dual channel FADEC or a single channel FADEC with a fully capable HMC.

(2) Aircraft Applications Other Than Transport Category Aircraft. For applications other than transport category airplanes, such as general aviation aircraft certified under part 23 and both normal and transport category rotorcraft, certified under parts 27 and 29, the LOTC rate should be one event per 100,000 engine hours. However, criteria other than this rate may be appropriate, depending on the reliability demonstrated by the previous control systems used on those engines and provided that in-service experience has proven the reliability of those previous systems to be satisfactory. In this case, a rate equivalent to that of the HMC systems of more than one event per 100,000 engine hours may be acceptable. An LOTC rate of 40,000 hours has been shown to be acceptable for airplanes certified in the Normal, Utility, or Acrobatic categories under part 23. In addition, it may be acceptable to modify the upper limit of the LOTC criteria from the 90% defined for part 25 applications to 85%. This modification would be acceptable because the loss of one magneto in a dual magneto system for reciprocating engines has usually resulted in a maximum power loss of 15% and has historically been determined to be acceptable by the FAA in general aviation applications. Applicants proposing alternate LOTC rates should comply with guidance for hazard levels for system failures applicable to EEC system installation (see AC23.1309-1C). Turbine engine powered rotorcraft certificated under parts 27 and 29 have demonstrated a need for controls systems with a higher degree of integrity. The 100,000 hours integrity level would be appropriate for these applications.

b. Alternate Mode(s). The EEC systems should be essentially single fault tolerant with respect to electrical or electronic failures. In these systems, transfer to an alternate mode(s) should not be considered an LOTC event in the analysis, if the alternate mode(s) does not exceed the applicable LOTC guidelines in this AC. A functionally dissimilar hydromechanical or electronic system with reduced capability may be used to achieve an acceptable system reliability rate.

(1) The acceptability of these alternate modes should be assessed based on the following criteria:

(a) Compliance of the alternate mode with the requirements of part 33. Any exceptions should be identified and assessed with respect to proposed operational usage. Backup or alternate modes should not result in an unsafe condition.

(b) The failure rate from the primary control mode to the alternate mode.

(c) The LOTC rate of the control system.

(d) Pilot workload and performance during transition to or operation in an alternate control mode. This issue may need evaluation at the aircraft level. The engine manufacturer should coordinate with the aircraft manufacturer and the ACO to determine if the alternate control modes comply with the applicable aircraft certification standards. These issues have been significant for some programs.

(2) The applicant should consider the following factors in the design and evaluation of any alternate control mode(s):

(a) Automatic protection from surge or lean limit blow-out.

(b) Acceleration and deceleration times.

(c) Altitude relight capability.

(d) Dormant failures of the alternate control mode and documentation of any automatic or manual checks to ensure the availability of the mode.

(e) Dispatchability, if any alternate modes are intended to be dispatchable.

c. Control System LOTC Analysis. The applicant should submit a system reliability analysis to substantiate the LOTC rate for the control system. The analysis should be a numerical analysis, such as a Markov model, fault tree or equivalent approach. The applicant should consider the following guidance for LOTC analyses:

(1) The analysis should address all components in the system that could contribute to LOTC events. This includes all electrical, mechanical, hydromechanical, and pneumatic elements of the system. This should also include aircraft signals or data used by the engine control when the failure or malfunction of those signals or data can contribute to LOTC events. The analysis should also include failures and malfunctions that contribute to the transmission of incorrect information if that incorrect information would lead to a flight crew initiated engine shutdown or thrust reduction to a level within the LOTC definition. The fuel pump is generally not included, as it is usually considered part of the fuel delivery system. The system definition includes those sensors or elements that may not be part of the engine type design, but are dedicated to the system and contribute to LOTC events. An example of this is the throttle or power lever transducer, which is usually supplied by the installer. The engine instructions for installation should include reliability and interface requirements for these other than engine type design elements.

(2) The analysis should consider all fault types, including both covered and uncovered faults.

(3) The airworthiness limitations section of the engine instructions for continued airworthiness (ICA) should contain periodic maintenance actions necessary for finding and repairing both covered and uncovered fault conditions to meet the LOTC rate.

d. System Safety Analysis (SSA).

(1) The applicant should complete and have available for review and acceptance an SSA for the EEC control system, addressing all declared dispatchable control configurations. Data used in the SSA should be substantiated. The SSA should include, but not necessarily be limited to, the following events caused by engine control system malfunctions:

(a) Failures affecting thrust:

1. Loss of the ability to modulate power or thrust between the selected idle and 90 percent of maximum rated power or thrust at all operating conditions. This failure mode is considered an LOTC event. A fault that increases idle thrust too much may be a concern in the aircraft approach configuration, because it affects the aircraft's ability to maintain the desired approach angle or glide-slope. A fault that decreases idle thrust too much may affect cowl anti-icing and go-around thrust capabilities. Therefore, while faults that result in not setting the proper idle thrust do pose a concern, small deviations from the correct, selected idle thrust due to small sensor errors, for example, should be acceptable. The engine failure modes and effects analysis (FMEA) and the aircraft SSA should examine these conditions.

2. Engine shutdown (a subset of all LOTC events).

3. Unwanted changes in magnitude or direction of power or thrust.

4. Instability in the control of a critical function.

(b) Transmission of faulty parameters, including engine indications such as oil pressure, rotor speed, inter-turbine or exhaust gas temperature, or the engine's thrust parameter.

(c) Unwanted action of a critical control function, such as deployment of reversers.

(d) Degraded capability of executing a critical function, such as failure to auto feather.

(e) Inability of the engine to meet part 33 requirements, such as loss of engine protection features.

(2) When applicable, the SSA should also provide failure rates for loss of ancillary control functions and engine indications that directly or indirectly lead to engine shutdown, such as the following:

(a) Stability augmentation.

(b) Oil, engine case, or component cooling.

(3) The SSA should consider the extent of power or thrust changes resulting from undetected faults:

(a) When operating in the take-off envelope, an uncovered fault in the control system or undetected fault in an aircraft signal used by the engine control system that results in a thrust or power change of greater than 3% thrust loss would generally be considered unacceptable for engines in installations that are required to meet part 25 requirements that include "obstacle clearance" requirements. The 3% requirement may not apply to engines for parts 27 and 29 rotorcraft and part 23 (non-commuter) aircraft installations. The applicant should still ensure that the full-up system is capable of providing the declared minimum rated thrust or power during take-off. Such faults should be random and should be detectable and correctable during routine inspections, overhauls, or power-checks. The applicant may have valid reasons for proposing thrust change levels that result from faults in aircraft-supplied data instead of the levels in this AC. In addition, the applicant may show that the particular guidance is not applicable to the specific engine installation. The ECO will consider these proposals and decide for each program, on a case-by-case basis, if they comply with the definition of unacceptable change in power or thrust.

(b) Undetected faults in an aircraft signal that result in a thrust or power change greater than three percent should be declared in the approved engine instruction manual. This data should describe the magnitude of the thrust or power change and the flight condition associated with the condition. Undetected faults resulting in thrust or power changes larger than three percent have generally been considered acceptable when operating outside the take-off envelope. In previous aircraft applications, these "outside the take-off envelope" thrust or power changes have been limited to less than approximately 15 percent and have been allowed in conditions involving high altitude, high-speed aircraft operations, or both.

(4) During take-off, detected faults in aircraft signals used by the engine control system that result in a thrust or power change of less than or equal to 10 percent may be acceptable if their frequencies of occurrence are relatively low. In previous applications, frequencies of less than 10^{-5} events per flight hour have been accepted.

(5) Single or multiple electrical or electronic failures, as well as hydromechanical system failures, that cause a greater than 10 percent change in power or thrust should be included in the control system's LOTC analysis. A safety factor or margin should be used for the frequencies of occurrences for single electrical or electronic failures that result in a greater than 10 percent thrust or power change when a field service database is not available to support the data used in the analysis. A factor of two is typically acceptable. If a single electrical or electronic failure can result in an engine configuration that does not comply with part 33, this should be included in the SSA. The frequencies of occurrence of single electrical or electronic failures that cause thrust or power changes of less than 10 percent, but greater than three percent, or result in the engine not meeting part 33 requirements, should be approved by the ECO.

(6) The SSA should provide an allowance for uncovered faults and their effects on the control system. This acknowledges the potential presence of faults that can affect thrust or power yet may not be recognized in the FMEA and SSA and, therefore, for which no fault accommodation is provided. Uncovered faults that can have a greater than 10 percent influence on engine thrust or power could lead to LOTC events. Therefore, the fault rate for these uncovered faults should be included in the LOTC analysis, and the rate used should be substantiated.

(7) If the SSA assumes that a particular crew action would reduce the impact of a fault condition, that assumed crew action should be clearly detailed in the instruction manual. This crew action may need to be validated at the aircraft level during aircraft certification. If the applicant requires a particular crew action to avoid an unsafe condition, the applicant should specify the display requirements associated with the failure condition in the instruction manual.

(8) The SSA should consider potential faults in aircraft wiring associated with the engine control. The engine instruction manual should state the effect of a grounding or over-voltage condition on any EEC system wiring caused by opens or shorts in that wiring to other aircraft wiring or structures. The manual should also note any dispatch configuration in which the open, short, or over-voltage condition would cause an LOTC event. In addition, opens and shorts in the engine harness wiring should be shown to result in a safe engine response by test, analysis, or both.

(9) The applicant should have an FMEA available for review. The FMEA can be based on a piece part failure analysis or a functional analysis. Since FMEAs are usually completed from a complete type design configuration, performing an FMEA by completing a piece part failure analysis on redundant electrical or electronic components may not be particularly useful because the result for most of these failures is “no effect.” To understand the failure modes of a redundant EEC system, the intent of the propulsion control system FMEA should be to understand the system with regard to single failures. The analysis should be focused on those single elements of the control that cause an impact on the control system and, therefore, on engine operation. Single electrical or electronic and mechanical or hydromechanical failures that affect the operation of the control system are of particular interest. These may include undetected or uncovered faults, as well as detected faults. Mechanical or hydromechanical failures that cause the engine to possibly increase in power or thrust and disable or reduce the capability of a protective function, like the overspeed protective function, should be investigated, and the design should be altered or changed to avoid such a situation. The FMEA should determine the criticality of single failures. Single electrical or electronic and mechanical or hydromechanical failures that should be considered include those that cause the control system to:

(a) Change engine power or thrust;

(b) Not respond to throttle inputs;

(c) Lose the capability of shutting off fuel;

(d) Cause the engine to overspeed;

(e) Cause loss of a protective function;

(f) Cause the control to "fail fixed" or change modes; and

(g) Cause the control to fail to a state that requires pilot intervention.

e. Control Mode Transitions. Systems that use alternate control modes as a backup system, including supervisory control systems, should incorporate automatic control features to transfer to the alternate mode when electrical or electronic failures that are otherwise not accommodated in the normal mode are detected. In some applications a "fail fixed" fuel flow followed by a manually activated switch to the alternate mode has been accepted. In these applications, there should be provisions for announcing the "fail fixed" condition to the flight crew by cockpit instrumentation. The alternate mode may be implemented using hydromechanical, electrical or electronic means, or any combination of these. The power or thrust change associated with an automatic transfer to the alternate mode should be declared in the approved engine instruction manual. Generally, designs involving automatic transfers have been limited to thrust changes of less than approximately 10 percent. Thrust changes greater than 10 percent have been accepted when they result from a crew-selected transfer. Acceptable transition between all control modes should be demonstrated for engine certification. During development, transition between control modes should be flight-tested, if possible. If pilot action is required in the fault accommodation and transfer of control, the faults involved in such a situation should be declared in the engine instruction manual, and the condition(s) should be evaluated during aircraft certification. For transfers that occur automatically, the following factors should be considered:

(1) The frequency of occurrence of transfers to any alternate control mode. Computed frequencies of transfer to any alternate control modes should be supported with data from endurance or reliability testing, in-service experience on similar equipment, or other acceptable data.

(2) Faults that would result in transfer to any alternate mode, and the capability for detection of these faults.

(3) Self-test coverage and diagnostics. Sufficient self-test coverage and diagnostics should be provided to enable detection of error conditions that are critical to system performance.

(4) Time delays in the transfer of control. The engine instruction manual should indicate if there are time delays in the transfer of control. The engine certification engineer may not be able to determine that the mode transition provides a safe and acceptable system in accordance with part 33 based solely on analytical or simulation data. In those cases, the applicant should propose a brief flight test program to support the data. In any case, such control transition delays may or may not be acceptable for aircraft certification, depending on the installation. Therefore,

the engine manufacturer should coordinate with the aircraft manufacturer and the aircraft certification office to evaluate this configuration early in the program. Control mode transitions should also be fully evaluated during aircraft certification.

(5) Availability of the alternate mode. If the alternate mode is not exercised during normal mode operation, an inspection interval or procedure for exercising the alternate mode should be specified to ensure that it remains functional and available. Inspection intervals or procedures may result in an operational limitation and will require the approval of the ECO.

(6) Provisions for signal(s) to indicate a mode transition.

f. Overspeed Protection System Requirements. For engine designs that require an overspeed protection control function, two categories of overspeed malfunction should be considered: those caused by shaft failure or loss of load, and those caused by control or fuel system failures. For shaft failure cases, the engine design may have some alternate methods of protection against rotor overspeed to comply with §33.75, such as "blade-shedding" or a "mash-and-clash" turbine design. In cases in which the basic engine design protects the rotor from an overspeed above structural limits, a control system overspeed protection system is usually unnecessary. If a control system overspeed protection function is necessary, the overspeed protection system should be evaluated with regard to its functionality and reliability as part of the engine control system.

(1) For overspeed protection systems, the following guidance provides one method, but not the only method, of compliance with both §§33.28 and 33.75.

(a) The combined engine and overspeed protection system should be at least two faults removed from a potential rotor burst event, when one of the faults induces the overspeed. In this respect, a potential rotor overspeed burst should only be possible as a result of a first fault inducing an overspeed and an independent fault preventing the overspeed protection system from operating.

(b) The analysis should show that the probability per engine flight hour of an uncontrolled overspeed condition from any cause in combination with overspeed protection system failure is one event per 100 million hours (a failure rate of 10^{-8} events per hour). Due to the severity of an uncontained engine failure in some installations, certification of the aircraft may require the rate for this combined event to be demonstrated to be less than one event per billion hours (10^{-9}).

(c) The failure rate of the overspeed protection system, itself, should be on the order of one event per 10,000 hours ($E10^{-4}$).

(d) The probability of an inadvertent activation of the overspeed protection system should be commensurate with the fault consequences. The LOTC analysis should include the frequency of inadvertent activations of the overprotection protection system that cause a greater than 10% thrust or power change.

(e) Overspeed protection is a necessary function for dispatch, required by §§33.28(c) and 33.75. Therefore, when the overspeed protection function is part of the control system, and its implementation involves the use of electrical or electronic components, a self-test of the overspeed protection system to ensure that the system is functional before each flight should be performed. Verification of the overspeed protection system at engine shutdown of the previous engine run has been acceptable.

(f) When multiple paths can invoke the overspeed protection system, a test of a different path should be performed each engine cycle, so that a complete test of the overspeed system can be achieved in a minimum number of engine cycles. If a path is found to be inoperative, the failure rate of the remaining path(s) should be less than 10^{-4} failures per hour, and combinations of failure leading to an uncontrolled overspeed event should still be extremely improbable. The control system should not be knowingly dispatched with the overspeed protection system failure rate greater than 10^{-4} failures per hour, or if the system is known to be inoperative.

(g) The applicant may provide data that demonstrates that the mechanical part of the overspeed protection system, such as the fuel shut-off mechanism, can operate without failures between stated periods. The applicant may also propose establishing a periodic inspection and test interval for the shut-off mechanism instead of testing the shut-off mechanism operation as part of the self-test conducted for each flight. When this approach is used, the self-test conducted for each flight should be limited to the electrical and electronic components of the overspeed protection system.

(h) Use of shared resources between the control system and the overspeed protection system should be evaluated. An analysis should show that the probability of faults of shared resources that could cause or contribute to an overspeed event as well as inhibit the overspeed protection function is extremely improbable, that is less than one event per billion engine flight hours ($10E^{-09}$). Single failures should not cause such a condition. The overspeed protection system should be independent from the normal control.

(i) When the overspeed control function is implemented through mechanical or hydromechanical means only, such as a fly-ball governor system, a periodic inspection and test interval for compliance with the requirement for “continued system availability” is acceptable. The periodic inspection and test interval should be based on test or in-service data that demonstrates that the system operates without failure between intervals.

(2) The overspeed malfunctions used in the failure analysis should be addressed when complying with §33.27.

g. Guidance for Use of Commercial or Industrial Grade Electronic Parts. Two recently published documents provide guidance on the application of commercial or industrial grade components: IEC/PAS 62239, Electronic Component Management Plans, edition 1.0, dated April 2001, and IEC/PAS 62240, Use of Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges, edition 1.0, dated April 2001. These should be used with the following guidance. When the engine type design specifies commercial or industrial grade electronic components, the applicant should have the following data available for review, as required:

(1) For each commercial and industrial grade electrical component specified in the design, reliability data that substantiates the failure rate for each component used in the EEC reliability analysis and the SSA.

(2) Procurement, quality assurance, and process control plans established for the vendor-supplied commercial and industrial grade parts. These plans should assure that the parts would maintain the reliability level specified in the approved engine type design.

(3) Unique databases for similar components procured from different vendors, because commercial and industrial grade parts may not all be manufactured to the same accepted industry standard, such as military component standards

(4) Substantiation that the proposed extended range of the specified components is suitable for the application, if the declared installation temperature environment for the EEC is greater than that of the electronic components specified in the engine type design. Additionally, if commercial or industrial parts are used in an environment beyond their specified rating and cooling provisions are required, the applicant should specify these provisions. Failure modes of the cooling provisions that cause these limits to be exceeded should be considered in determining the probability of failure.

h. Consideration of Local Events. When designing an electronic control system to meet the requirements of §33.28, the engine manufacturer should provide a control system with at least an equivalent level of safety and reliability as that of engines or propellers equipped with HMC systems. HMC systems have been shown to perform safely and reliably in the face of "local events." In some cases, a comparison to HMC systems is not practical because the EEC system either provides functions not previously provided by HMC systems or is implemented differently. In these cases the acceptability of the effect of local events should be based on their effect on aircraft safe flight and landing. Examples of local events include: engine overheating conditions or fires, electrical problems, hydraulic and lubricating fluid leaks, and mechanical disruptions.

(1) Whatever the local event, the behavior of the EEC system should not cause a hazard to the continued safe flight and landing of the aircraft. Effects such as the control of the thrust reverser deployment, an overspeed of the engine, transients effects, or inadvertent propeller pitch change under any flight condition should be considered.

(2) When demonstrating that local events do not cause a hazard to the continued safe flight and landing of the aircraft, the applicant should show that any other function necessary to provide protection would be available at the time of the local event and would not be rendered inoperative by the same local event (such as destruction of wires, ducts, or power supplies). This includes proposed designs in which the engine manufacturer assumes that the aircraft (or aircraft components) provides the necessary protection. This engine failure modes effects and criticality analysis (FMECA) should document this assumption.

(3) When the temperature to which the EEC is exposed is greater than the maximum safe design operating temperature declared by the engine manufacturer, an overheat condition results. The electronic portions of the control should not cause a hazardous condition when the EEC is exposed to a continuous overheat or over-temperature condition, such as a duct burst or leak within a nacelle. Specific design features or analysis methods may be used to show compliance with respect to the prevention of hazardous effects. When this is not possible due to the variability or complexity of the failure sequence, acceptable testing may be required. Computer simulation techniques similar to those discussed for fire testing have also been acceptable. The compliance criteria requires that when the EEC system is exposed to an overheat condition, the system should not cause the engine to behave in an unsafe manner and should allow a safe engine shut down.

(4) To show compliance with fire as a local event, the EEC system must comply with fire test requirements when the system is located in a fire zone. Fire zones are defined in the appropriate aircraft certification standards. Fire requirements for the electronic parts of the EEC system are not covered precisely in the regulations with regard to the length of time they are required to function when exposed to fire. Therefore, the FAA has developed compliance criteria for EEC systems. When exposed to fire, the EEC system should allow a safe engine shut down without an unwanted action during the exposure that could become hazardous to the aircraft.

(a) The fuel handling parts of the EEC system, including the fuel shut-off valve (SOV), should comply with §33.17, which requires that these parts be fire resistant. Section 33.17 requires that the engine design minimize the probability of the occurrence and spread of fire. Therefore, consideration should be given to those parts of the EEC system that control airflow, which could fail and contribute to the fire when the system is exposed to fire.

(b) In addition, §33.75 requires that fire cannot cause the engine to lose the capability to shut down. For system designs that depend on electric power to actuate the SOV, high temperature wire or other protective means should be used to ensure that the capability to shut down the engine is maintained when the EEC is exposed to fire.

(c) To demonstrate compliance with fire resistance requirements, computer simulations of EEC exposure to fire may be used instead of fire tests on production hardware. Approved computer simulations should be validated by analysis, test, or both, including all assumptions upon which the computer simulation is based.

(d) Hardware emulations for use in fire tests may also be acceptable. Approved hardware emulations should be validated by analysis, test, or both.

(e) The engine manufacturer should note that as part of aircraft certification for transport aircraft, the Transport Airplane Directorate (TAD) has required actual fire tests on all elements of systems in which there is the potential for fire causing a catastrophic failure, such as elements that could cause a catastrophic reverser deployment or an uncontained rotor burst.

(5) The applicant should demonstrate by analysis or test that when any EEC system component input or output electrical connection opens or shorts to ground, the system behaves in a safe and predictable manner. In addition, the applicant should show that any EEC system component connector that becomes disconnected while the engine is operating does not cause a hazard to the continued safe flight and landing of the aircraft.

(a) EEC aircraft interface wiring should be tested or analyzed for shorts to aircraft power; these "hot" shorts should result in an identified and non-hazardous effect. When aircraft interface wiring is involved, the installer should be informed of the potential effects of wiring faults on aircraft interface wiring in the engine instructions for installation.

(b) When physical separation of conductors is not practical, the engine manufacturer and the installer should coordinate to ensure that the potential for common mode faults between engine controls is eliminated and that the potential for common mode faults between channels on one engine is minimized.

(6) The applicant should demonstrate by analysis or test that hydraulic or lubricating leaks impinging on the EEC control system do not cause a hazard to the continued safe flight and landing of the aircraft.

(7) The applicant should demonstrate by test, analysis, or both, that mechanical disruptions that could sever connections or damage EEC system components do not result in a hazard to the continued safe flight and landing of the aircraft. The evaluation of this design feature is installation dependent in many cases; these considerations in the design for mechanical disruptions should be considered on a case-by-case basis.

CHAPTER 7. SECTION 33.28(d)

7-1. Rule Text. Section 33.28(d) provides that each EEC must: "Have environmental limits, including transients caused by lightning strikes, specified in the instruction manual."

7-2. Intent of Rule. Section 33.28(d) ensures that the engine and control system meet acceptable environmental operating conditions. The instruction manual should clearly define EEC system operational limitations, for the benefit of the engine installer, and provide assurance that the EEC system is functional in a reasonably designed aircraft environment.

7-3. Compliance with §33.28(d). The following guidance provides a method, but not the only method, of compliance with §33.28(d).

a. General Test Requirements. Section 33.28(d) requires that the EEC system have environmental limits specified in the engine instruction manual, including those associated with lightning and high intensity radiated fields (HIRF). Environmental tests conducted on an individual system component basis in accordance with test procedures defined in RTCA Document DO-160D (see AC 21.16D), or equivalent, have been acceptable, except for temperature variation, HIRF, and lightning tests.

(1) A minimum of 10 temperature cycles should be performed for temperature variation tests.

(2) Adaptations and combinations of the test procedures in RTCA Document DO-160D should be used for the HIRF, lightning, and electromagnetic interference (EMI) system tests. The test procedures in RTCA Document DO-160D are directed toward tests of individual pieces of equipment rather than systems, such as EEC controls.

(3) EMI tests conducted in accordance with MIL-STD-461/462 have been accepted as providing procedures and test levels equivalent to those in RTCA Document DO-160D. When the two test procedures differ for a particular test case, the more rigorous test procedure should be used unless use of the alternate test can be justified. HIRF and lightning tests should be conducted using the procedures described in paragraphs 7-3.b., 7-3.c., and 7-3.d. of this AC.

(4) Environmental tests in accordance with MIL-STD-810E may be accepted instead of RTCA Document DO-160D tests when the MIL-STD-810E tests are equal to or more rigorous than those defined in RTCA Document DO-160D.

b. System Test Configuration Considerations. EEC manufacturers and engine manufacturers have conducted HIRF, lightning, and EMI tests as system tests on closed loop laboratory setups. The closed loop setup is usually provided with hydraulic pressure to move actuators to close the inner actuating loops. A simplified engine simulation may be used to close the outer engine loop.

(1) Open Loop Laboratory Tests. In some cases, open loop laboratory setups with EEC test software have been accepted. If the applicant conducts open loop setups, the following factors should be considered:

(a) The EEC test software should be developed and implemented by guidelines defined for software levels of at least Level 2 or Level C, in RTCA Document DO-178A and RTCA Document DO-178B, respectively. In some cases, the application code should be modified to include the required test code features.

(b) The system test setup should be instrumented to monitor both the output drive signals and the input signals.

(c) Anomalies observed on inputs or outputs should be duplicated on the engine simulation to determine if the resulting power or thrust perturbations comply with the pass/fail criteria.

(2) Pass/Fail Criteria. The tests should be conducted with the EEC system controlling the engine at the most sensitive operating point, as selected by the applicant. This may be a different operating point for the three different tests. The system should be exposed to the HIRF, lightning, and EMI environmental threats while operating at the selected condition. The pass criteria for HIRF and lightning is that there is "no effect" on the operation or operational characteristics of the system. "No effect" is defined as less than $\pm$2 percent of power or thrust change from the normal control governing capability for a period of less than one second. For EMI testing, the limits selected from the appropriate section of RTCA/DO-160D should be used. The following results are considered test failures:

(a) Transfers to alternate channels, backup HMC systems, or reversionary modes.

(b) Component damage.

(c) Significant fault codes recorded in the fault memory.

(d) False fault announcements to the crew that could cause unnecessary or inappropriate crew action.

(e) Erroneous operation of overspeed or reverser circuits.

c. HIRF Test Requirements. For HIRF testing, systems have been accepted for engine certification using an interim high energy radiated fields (HERF) policy memo dated December 5, 1989. That interim policy memo served as the basis for Notice N8110.67, Guidance for the Certification of Aircraft Operating in High Intensity Radiated Fields (HIRF) Environments, which was later reissued as N8110.71 in April 1998. Using 100 volts per meter average from 10 KHZ to 18 GHZ is an acceptable level for conducting HIRF bench tests for systems that perform critical functions. For rotorcraft applications, the HIRF bench test level should be 200 volts per meter average from 10 KHZ to 18 GHZ.

(1) The Engine and Propeller Directorate has used 200 volts per meter average over the entire frequency range from 10 KHZ to 18 KHZ as the standard for testing EEC systems.

(2) At a minimum, the modulations specified in RTCA Document DO-160D, Section 20, for categories W or Y should be used. Additional modulations based on the EEC operating frequencies or control loop bandwidth should be used for the system HIRF tests.

(3) In many cases, additional pulse modulation tests in the microwave range are specified by the aircraft manufacturers. These additional tests are generally at field levels in excess of 1000 volts per meter. Experience to date has shown that EECs that pass 200 volts per meter average will also pass tests at the higher pulse modulated field levels at the higher frequencies. However, it should not be assumed that the system is hardened to these levels without completing the high-level pulse tests. Test procedures generally follow the guidelines of Section 20 of RTCA Document DO-160D.

d. Lightning Test Requirements. Lightning tests should follow the guidelines of AC 20-136 and Section 22 of RTCA Document DO-160D. Multiple stroke (MS) and multiple burst (MB) tests should be conducted on the system connected on the test bench (see paragraph 7-3.b. of this AC).

(1) EEC MS Lightning Tests. Low-level lightning test(s) should be conducted to establish the engine cable shield current levels. Low-level tests have been used to establish the waveforms and current levels coupled on to the cables for the MS tests. The shield current level for large engines has been on the order of 1000 to 2000 amperes. For smaller engines, shield current levels have been higher. These levels are typically determined by low current level lightning tests on the engine without the full benefit of nacelle attenuation and, therefore, should be conservative. Although the shield current level is not a requirement of an MS lightning test, the applicant should demonstrate that it is a realistic level for the category of engine and its application.

(2) EEC MB Lightning Tests. Past MB tests have been conducted using the chattering relay test defined in Section 19.3.4.1 of RTCA Document DO-160D. However, the chattering relay test has been superseded by MB tests using Waveform 3 or Component H (see AC 20-136).

(3) EEC Pin Injection Tests (PIT). PITs should be conducted on the EEC. PIT levels should be appropriately selected from the tables of Section 22 of RTCA Document DO-160D. PITs should be conducted on other system components as required.

(a) PITs should be used to verify that equipment does not exhibit permanent upset or damage when subject to the pin-injected transient waveforms. During these tests, the transient waveforms are applied directly to the designated pins on the equipment connector, normally between each pin and the equipment chassis ground, as described in Section 22 of RTCA Document DO-160. This method assesses the dielectric withstand voltage or damage tolerance of the equipment interface circuit. For equipment electrical interface circuits that are electrically isolated from the equipment chassis or grounds, the applicant can perform a dielectric withstand or high-potential (hi-pot) test that meets or exceeds the peak transient waveform voltage amplitude in place of the PIT.

(b) Equipment interface circuits with low impedance with respect to the equipment chassis should be subjected to the PIT. For pin injection purposes, low impedance should be considered less than 100 ohms at any frequency below 10 KHZ. Shunt filters and transient suppression devices such as Tranzorbs(tm) normally produce low impedance to chassis to provide transient protection and should be subjected to the PITs at the selected waveform levels.

(4) Aircraft and Engine Certification Lightning Tests.

(a) For engine-mounted EECs, lightning tests conducted on an EEC system may be adequate to cover aircraft certification, as well as engine certification, provided the aircraft-engine interface cables and current levels are adequately represented in the test. The test levels should be at a level compatible with the installation. The applicant and the ECO should mutually agree on the test level in the test plan. To account for the aircraft contribution to the test levels, the applicant should coordinate with the ACO to determine a mutually acceptable test level for the category of aircraft involved.

(b) The engine manufacturer should note that each aircraft manufacturer installing an engine must determine the levels to which the installed engine and EEC system will be exposed for the particular aircraft. The aircraft manufacturer should demonstrate that these levels are equal to or less than the levels used for engine certification testing. If the aircraft manufacturer cannot demonstrate this, then EEC system lightning tests may be needed to show compliance with aircraft certification standards.

e. Maintenance Requirements. Section 33.4 and Appendix A to part 33 require that the engine manufacturer prepare ICA for all engine parts. A maintenance plan must be part of the ICA. Therefore, as part of the environmental protection system that is part of the engine type design and is used to protect the EEC system from HIRF and lightning, a maintenance plan must be provided to ensure the continued airworthiness of the installed systems. Notice 8110.71 provides some guidance that can be used to meet the ICA requirement. Maintenance requirements may include periodic inspections or tests for required structural shielding, wire shields, connectors, and equipment protection components. The applicant should provide the engineering validation and substantiation of these maintenance requirements.

f. Environmental Testing. All components of the EEC system, including all electronics units, sensors, harnesses, hydromechanical elements, and any other relevant elements or units, should be tested to establish that they will operate properly in their declared environment. When applicable, tests defined in RTCA Document DO-160D have been accepted. Environmental test plans should be approved by the ECO before the tests are conducted.

(1) Although environmental test limits are not specified in this AC, environmental tests should be representative of the environments that are expected to be encountered in the engine installation. Special attention should be given to any condition that could affect more than one engine or propeller control system, such as a faulty operation during hot day ambient conditions. The environment for which the component is qualified should be entered into the instruction manual and is considered an installation limitation for the installer.

(2) The applicant should prepare an environmental test plan summarized in an environmental test matrix that defines the method to be used to qualify the component for each of the environments. The environments and test procedures defined in RTCA Document DO-160D have been acceptable to the FAA for electrical and electronic components. Generally, only the environments that are expected to be encountered should be tested. The matrix can note other environments as "not applicable." The components should be qualified by test, similarity, analysis, or any combination of these.

(3) The applicant should provide the proposed test plan for approval before conducting tests of fuel handling, hydraulic, and pneumatic components, such as the fuel metering unit (FMU) and actuators. These components should be qualified by test, similarity, analysis or any combination of these. In some cases, the testing required for the engine block tests under §§33.49 or 33.87 may be adequate to qualify these components. Otherwise, additional tests are required under §§33.28(d) and 33.91(a).

(4) The explosion proof testing verifies that a component cannot cause an explosion of flammable fluids or vapors. If applicable, explosion proof testing may be performed as defined in Section 9 of RTCA DO-160. Section 9 of DO-160D applies to demonstrating compliance with §§33.28 and 33.91. DO-160D defines Environment I as equipment mounted in fuel tanks or within fuel systems and Environment II as an atmosphere in which flammable mixtures can be expected to occur as the result of a "fault causing spillage or leakage." These definitions for the equipment environment may not be in complete agreement with definitions for aircraft engine installations.

(a) For installations in designated fire zones as defined in §§23.1181, 25.1181, 27.1181, and 29.1181, the fire zone should have extinguishing provisions so that the explosion proof test given by Section 9 of Environment II of DO-160D would be adequate. However, flammable fluid leakage areas as defined in §25.863 and other sections may not have fire extinguishing provisions or any of the other safety requirements associated with fire zones, due to the assumption that there are no ignition sources in those areas. In these cases, the applicant should be aware that the explosion proof test given by Section 9 of Environment I of DO-160D,

although not a requirement for engine certification, might be a requirement for aircraft installation. The applicant may also demonstrate by test or analysis that the EEC system is not an ignition source.

(b) The applicant should state the type of explosion proof test that has been conducted in the installation instructions. In addition, if the applicant anticipates installations in a zone where flammable fluid requirements may be imposed, the test or analysis that demonstrates that the EEC system is not an ignition source should be referenced or included in the installation instructions.

g. Time Limited Dispatch (TLD) Environmental Tests. Although TLD is not a requirement for certification, HIRF and lightning tests for TLD should be conducted with the tests conducted for certification. To get approval for the use of TLD, applicants should demonstrate that dispatchable EEC configurations continue to meet the environmental requirements of the certification basis. SAE Document ARP 5107 contains applicable TLD information. For HIRF and lightning, applicants have usually determined that the single channel dispatch configuration is the worst case dispatch configuration; they have conducted HIRF and lightning tests with one channel inoperative to demonstrate compliance. For other environments, the applicants have complied by analysis and statements of compliance.

CHAPTER 8. SECTION 33.28(e)

8-1. Rule Text. Section 33.28(e) provides that each EEC must: "Have all associated software designed and implemented to prevent errors that would result in an unacceptable loss of power or thrust, or other unsafe condition, and have the method used to design and implement the software approved by the Administrator."

8-2. Intent of Rule. Section 33.28(e) requires that electrical and electronic engine control systems have all associated software designed and implemented to prevent errors that would result in a unacceptable loss of power or thrust, or other unsafe condition, and have the method used to design and implement the software approved for the application.

8-3. Compliance with §33.28(e). The following guidance provides a method, but not the only method, of compliance with §33.28(e).

a. Software Level Requirements. Software should be designed and implemented according to the standards established as Level 1 or Level A, as provided in RTCA documents DO-178A and DO-178B, respectively; the applicant should complete any additional testing required by the Administrator. RTCA Document DO-178A has been superseded by RTCA Document DO-178B; engine certification projects with a date of application after January 11, 1993, should use RTCA Document DO-178B. Part 23 applications not intended to be certificated to part 25 requirements should use the standards of DO-178B level B or C for the control. The applicant should coordinate this with the airframe manufacturer and the ACO early in the certification program.

b. Software Partitioning. It may be possible to partition non-critical software from the critical software to allow the non-critical software to be designed and implemented at a lower level than that established in the RTCA documents. Applicants should substantiate the adequacy of the partitioning method and should consider if the lower levels of the partitioned software are appropriate for the anticipated installations. If the criticality level requirement were higher in subsequent applications, it would be difficult to raise the software level without repeating the software life cycle processes for the new level.

c. Software Integrity. RTCA Document DO-178B provides guidance for software used at specified hazard levels. As with all guidance in this document, this may be modified due to future events or advancements in technology.

d. Programmed Logic Devices. Due to the nature and complexity of systems containing digital logic, programmed logic devices should be developed using a structured development approach, equivalent to the hazard associated with failure or malfunction of the system in which the device is contained. Programmed logic devices include application specific integrated circuits (ASIC) and programmable logic devices (PLDs). An ASIC is defined as any masked programmed integrated circuit that requires physical customization of the device die by an ASIC

vendor. Gate array, cell-based and custom designs are included, as they involve some level of customization of the mask sets used in the fabrication of the devices. A PLD is defined as any device that is purchased as an electronic part and altered to perform an application specific function. PLDs usually require programming by the equipment manufacturer.

(1) PLDs include, but are not limited to, the following:

(a) Programmable array logic (PAL) devices;

(b) Programmable logic array (PLA) devices;

(c) General array logic (GAL) devices;

(d) Field programmable gate array (FPGA) devices; and

(e) Electrically or erasable programmable logic devices (EPLD).

(2) RTCA Document DO-254 provides guidance for the criticality, failure condition categories, and design assurance levels associated with development of programmed logic devices. This is an acceptable means, but not the only means, for demonstrating compliance with §33.28(e).

(3) For off-the-shelf equipment or modified equipment, service experience may be used to demonstrate compliance. This should be acceptable if the worst case failure or malfunction of the device for the new installation is not more severe than that for the original installation of the same equipment on another application. The applicant should also consider significant differences related to the environmental or operational category of the aircraft in which the original system was installed and certified.

APPENDIX 1. REGULATORY BASIS FOR REQUIRING AN EEC SSA AND LOTC ANALYSIS UNDER §33.28

1. This appendix explains the basis for requiring an SSA as part of an applicant's demonstration of compliance with §33.28. Before §33.28 was added to part 33, EEC systems were certified only upon demonstration of complete redundancy in the electronic portions of critical loops of the system. Applicants that did not perform an SSA were required to demonstrate sufficient similarity to earlier EEC accepted designs that had adequate redundancy. Section 33.28 codified for general applicability the practices used in these early EEC engine certification programs. If changes in EEC design make it no longer possible to accept EECs based on similarity with earlier accepted designs, then future applicants must, in order to demonstrate compliance with §33.28, submit an SSA for each EEC design.

2. The FAA will accept new technologies on the basis that the safety and reliability of that new technology are equivalent to, or an improvement over, current technologies. On this basis the EECs were accepted in place of HMC designs after establishing the basis for comparison as one LOTC event per 100,000 hours of service. An LOTC event is one in which there is a loss of the ability to control engine thrust from flight idle to 90 percent of maximum rated thrust. This basis for comparison was established after extensive review, by FAA and industry, of in-service reliability data of existing engine control systems. The results of that review were documented in issue papers and technical memoranda.

3. To meet this reliability standard, early EEC systems were designed with dual channel redundancy from the sensed inputs to the dual output devices for the critical control loops, defined as the fuel, stator vanes, and bleed control loops. Parts of the engine control system that remained with HMC technology generally were not made redundant.

4. A means, but not the only means, of compliance with §33.28 is provided in this AC through analysis that demonstrates that the proposed EEC system meets the LOTC criteria and that the EEC system has adequate redundancy and fault accommodation.

5. Section 33.28 provides that "no single failure or malfunction or probable combination of failures of electrical or electronic components of the control system, results in an unsafe condition." The term unsafe condition as used in this context is not limited to those specific conditions described in §33.75. While changes in thrust alone, however, will not always constitute an unsafe condition, the FAA will continue to evaluate unwanted changes in thrust or power with regard to the frequency of those events, their magnitude, and their occurrence in the flight envelope in determining whether an LOTC constitutes an unsafe condition for a particular engine design. New technology electrical and electronic EEC systems introduce potential failures that could result in unsafe conditions requiring an SSA under §33.28. Those failures include, but are not limited to, the following:

a. Complete loss of control over the engine.

b. Instability in the control of a critical function of the engine.

c. Unwanted change in magnitude or direction of power or thrust in some operating conditions.

d. Unwanted action of a critical control function, such as the uncommanded deployment of thrust reversers.

6. Early EEC system designs have full redundancy on electronic parts of the system that control critical loops and, therefore, were found to provide reliability equivalent to the HMC systems they replaced based on the established reliability criteria of one LOTC event in 100,000 hours of service. These systems are essentially single fault tolerant. They cannot be considered fully single fault tolerant because a small percentage of failure types either cannot be addressed or are not detectable and as such cannot be accommodated. Using this criteria, subsequent systems can be accepted based on their similarity in design with these early redundant EEC systems. In recent certification programs, however, applicants have proposed engine designs using EEC systems that offer less than full redundancy. In these newer EEC designs significant unwanted changes in thrust or power could occur as a result of single system failures. Therefore, since these newer systems were not similar in design and did not meet the LOTC reliability criteria equivalent to HMC systems, the FAA could not accept these systems without an SSA to demonstrate compliance with §33.28.

7. The FAA has recognized that a uniform method for demonstrating how newer EEC systems comply with §33.28 would both promote safety in air commerce and aid industry. This AC provides that method based on meeting the LOTC reliability criteria for HMC designs through tests, analysis, or both. The FAA also recognizes that the LOTC reliability criteria for HMC designs was established through review of service experience data for aircraft certified under part 25 only, and an acceptable reliability criteria for aircraft certified under other standards (parts 23, 27 or 29) may differ from the part 25 criteria. Applicants are cautioned, however, that engines certified under part 33 are generally not restricted to a specific operational use. Therefore, the FAA may have to apply the more conservative part 25 criteria in a particular certification program if it determines that the engine involved in that program may be eligible for installation on an aircraft that may be certified under part 25.