



U.S. Department  
of Transportation  
**Federal Aviation  
Administration**

# Advisory Circular

---

**Subject:** GUIDANCE MATERIAL FOR 14  
CFR § 33.28, ENGINE CONTROL  
SYSTEMS

**Date:** DRAFT  
**Initiated by:** ANE-111

**AC No:** 33.28-1X  
[DRAFT]  
**Change:**

---

1. Purpose. This advisory circular (AC) provides guidance and describes acceptable methods, but not the only methods, for demonstrating compliance with the engine control systems requirements of § 33.28 of Title 14 of the Code of Federal Regulations (14 CFR part 33). The information provided in this AC replaces the guidance in AC 33.28-1, issued on June 29, 2001.

2. Applicability.

a. The guidance provided in this document is directed to the engine manufacturer, modifier, or Federal Aviation Administration (FAA) engine type certification designee. This guidance should also assist the engine installer in understanding the interface between certification of the engine and the aircraft and the assumptions made by the engine manufacturer concerning the engine/aircraft interface.

b. This material is neither mandatory nor regulatory in nature and does not constitute a regulation. It describes acceptable means, but not the only means, for demonstrating compliance with the applicable regulations. The FAA will consider other methods of demonstrating compliance that an applicant may present. Terms such as “should,” “shall,” “may,” and “must” are used only in the sense of ensuring applicability of this particular method of compliance when the acceptable method of compliance in this document is used. While these guidelines are not mandatory, they are derived from extensive FAA and industry experience in determining compliance with the relevant regulations. On the other hand, if we become convinced that following this AC would not result in compliance with the applicable regulations, we will not be bound by the terms of this AC, and we may require additional substantiation as the basis for finding compliance.

c. Applicants for engines equipped with electronic engine control systems (EECS) may require additional guidance, especially with regard to the interface of these engines with the certification of the aircraft and/or propeller. This AC discusses the tasks related to the engine, propeller, and aircraft certification processes generally, and indicates to a limited extent, how these tasks might be allocated among product manufacturers. This document applies to functions

DRAFT

integrated into the EECS to the extent that these functions affect compliance with federal aviation regulations.

d. This material does not change, create any additional, authorize changes in, or permit deviations from existing regulatory requirements.

3. Related References.

a. Related Regulations in 14 CFR. Sections 25.901, 25.903, 25.939, 25.1181, 25.1309, 27.901, 27.903, 27.1309, 29.901, 29.903, 29.1309, 33.4, 33.5, 33.17, 33.19, 33.27, 33.29, 33.49, 33.53, 33.75, 33.91(a), and Appendix A of part 33.

b. FAA Documents.

(1) AC 20-115B, RTCA, Inc. Document RTCA/DO-178B; January 11, 1993.

(2) AC 20-136A, Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning; December 21, 2006.

(3) AC20-152, RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware; June 30, 2005.

(4) AC21-16E, RTCA, Inc. Document RTCA/DO-160E, Environmental Conditions and Test Procedures for Airborne Equipment; December 20, 2005.

(5) AC 33.2B Aircraft Engine Type Certification Handbook; June 30, 1993.

(6) AC 33.4-3, Instructions For Continued Airworthiness; Aircraft Engine High Intensity Radiated Fields (HIRF) And Lightning Protection Features, September 16, 2005.

(7) AC 33.17-1, Fire Prevention, June 28, 2002.

(8) FAA Order 8110.49, Software Approval Guidelines; June 2, 2003.

(9) FAA Policy Memorandum PS-ANE100-1993-00131, FAA Engine and Propeller Directorate Policy Regarding Time Limited Dispatch (TLD) Of Engines Fitted With Full Authority Digital Engine Control (FADEC) Systems; October 28, 1993.

(10) FAA Policy Memorandum, PS-ANE100-2001-1993-33.28TLD-R1, Policy for Time Limited Dispatch (TLD) of Engines Fitted with Full Authority Digital Engine Controls (FADEC) Systems; June 29, 2001.

(11) FAA Policy Letter PL-45, [Time Limited Dispatch \(TLD\) Authorization for Full Authority Digital Electronic Control \(FADEC\) Engines](#), Rev 2, March 4, 2004.

DRAFT

DRAFT

c. EASA Advisory, AMC 20-115B, General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances, Recognition of Eurocae ED-12B/RTCA DO-178B, November 5, 2003.

d. Industry Documents.

(1) International Electrotechnical Commission (IEC).

(a) IEC/TS 62239, Process Management for Avionics – Preparation of an Electronic Components Management Plan, First edition 2003-05.

(b) IEC/TR 62240, Process Management for Avionics - Use of Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges, First edition 2005-06.

(2) RTCA Documents available at: RTCA, Inc. 1828 L Street, NW, Suite 805, Washington, DC 20036 or EUROCAE, 17, rue Hamelin, 75116, Paris, France.

(a) RTCA DO-178A, Software Considerations in Airborne Systems and Equipment Certification; March 22, 1985.

(b) RTCA DO-178B/EUROCAE ED-12B, Software Considerations in Airborne Systems and Equipment Certification; December 1992.

(c) RTCA DO-254/EUROCAE ED-80, Design Assurance Guidance for Airborne Electronic Hardware; April 19, 2000/April 2000.

(d) RTCA DO-160E/EUROCAE ED-14E, Environmental Conditions and Test Procedures for Airborne Equipment, December 9, 2004/March 2005.

(3) Society of Automotive Engineers (SAE).

(a) SAE ARP5107A, Guidelines for Time Limited Dispatch (TLD) Analysis for Electronic Engine Control Systems; January 2005.

(b) SAE ARP5415A/EUROCAE ED-91, Users Manual for Certification of Aircraft Electrical/Electronic Systems for the Indirect Effects of Lightning, May 2002.

(c) SAE ARP5416/EUROCAE ED-105, Aircraft Lightning Test Methods; March 2005/April 2005.

(d) SAE ARP5583, Guide to Certification of Aircraft in a High Intensity Radiated Field (HIRF) Environment; January 2003.

(e) SAE ARP5757, Guidelines for Engine Component Tests; March 2008.

DRAFT

DRAFT

(f) SAE ARP5890, Guidelines for Preparing Reliability Assessment Plans for Electronic Engine Controls; November, 2002.

e. Military Specifications.

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

(2) MIL-STD-810 E or F, Test Method Standard for Environmental Engineering; E July 14, 1989; F January 1, 2000.

(3) MIL-E-5007E, Engines, Aircraft, Turbojet and Turbofan, General Specification For; September 1, 1983.

f. Reference Addresses. The following addresses are provided in order to aid in accessing some of the reference documents. The addresses are subject to change and it is advised to confirm them via internet searches.

(1) EASA documents are available online at [www.easa.eu.int](http://www.easa.eu.int).

(2) IEC documents are available at: IEC, Central Office, 3, rue de Varembe, P.O. Box 131, CH - 1211 GENEVA 20, Switzerland. They are also available online at [www.iec.org](http://www.iec.org).

(3) RTCA documents are available at: RTCA, Inc. 1828 L Street, NW, Suite 805, Washington, DC 20036 or EUROCAE, 17, rue Hamelin, 75116, Paris, France. Also available online at [www.rtca.org](http://www.rtca.org) or [www.eurocae.org](http://www.eurocae.org).

(4) SAE documents are available at: Society of Automotive Engineers (SAE), 400 Commonwealth Drive, Warrendale, PA 15096-0001 USA or EUROCAE, 17, rue Hamelin, 75116 Paris, France. Also available online at [www.sae.org](http://www.sae.org).

(5) MIL STD documents may be available at:  
<http://www.dtc.army.mil/publications/milstd.html>.

4. Definitions. For the purposes of this AC, the following definitions apply:

Aircraft-supplied Data	Data supplied by or via aircraft systems
Aircraft-supplied Electrical Power	Any electrical power supplied by or via aircraft systems and used by the engine/propeller control system.
Alternate Mode	Any control mode that is not the primary mode.

DRAFT

Analysis	A specific and detailed qualitative or quantitative evaluation of the engine relative to the requirements of § 33.75 and other applicable requirements of the EECS. Examples include: Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA) and Markov Analysis.
Automatic Takeoff Thrust Control System (ATTCS)	The entire automatic system used on takeoff, including all devices, both mechanical and electrical, that sense engine failure, transmit signals, actuate fuel controls or power levers, or increase engine power by other means on operating engines to achieve scheduled thrust or power increases and to furnish cockpit information on system operation.
Back-up Mode	The back –up system control mode. The alternate channel in a dual channel system with identical channels is not a backup mode. Any additional backup means provided differing from the two channels are back-up modes under the definition.
Back-up System	A part of the engine/propeller control system where the operating characteristics or capabilities of the engine control are sufficiently different from the primary system that the operating characteristics or capabilities of the aircraft, crew workload, or what constitutes appropriate crew procedures may be significantly impacted or changed.
Control Mode	Each defined operational state of the engine control system in which the crew can exercise satisfactory engine control, which may involve evaluation in the aircraft/rotorcraft.
Covered Fault	A fault which is detected and/or accommodated.
Dispatchable Configuration	All control system configurations approved for dispatch.
Electronic Engine Control System (EECS)	An engine control system in which the primary functions are provided using electronics. It includes all the components (e.g. electrical, electronic, hydromechanical and pneumatic) necessary for the control of the engine and may incorporate other control functions where desired. Components of the system provided by the installer may be considered part of the system.
Engine Control System (ECS)	Any system or device that controls, limits or monitors engine operation.
Engine Dedicated Power Source	An electric power source providing electrical power generated and supplied solely for use by a single engine control system

DRAFT

Engine / Propeller Control System (ECS/PCS)	Any system that is an integrated engine and propeller control system. The system then contains elements of both ECS and PCS.
Error	An omission or incorrect action by a person, a mistake in requirements, in design, or in implementation. An error may result in a failure, but an error is not a failure in and of itself.
Failure Condition	A condition with a direct, consequential engine-level effect, caused or contributed to by one or more failures. Examples include any unwanted limitation of thrust to idle or total loss of a signal.
Failure Mode	The cause of the failure or the manner in which an item or function can fail. Examples include failures due to corrosion or fatigue, opens and shorts in circuits, and malfunctions of electronic components.
Fault (or) Failure	A condition where the operation of a component, part, or element can no longer function as intended, including loss of function.
Fault (or) Failure Accommodation	The capability to mitigate, either wholly or in part, the effects of a fault or failure.
Full Authority Digital Engine Control (FADEC)	An engine control system in which the primary functions are provided using digital electronics and in which the electronic engine control (EEC) unit has full-range authority over the engine power or thrust.
Full-up Configuration	An EECS that has no known faults or failures present that affect the LOTC/LOPC rate.
Primary Mode	The mode for controlling the engine under normal operation; often referred to as the 'normal mode.'
Primary System	The part of the engine/propeller control system normally used for controlling the engine/propeller operation.
Programmable Logic Device (PLD)	An electronic component that is altered to perform an installation specific function. PLDs include, but are not limited to, Programmable Array Logic (PAL) components, General Array Logic (GAL) components, Field Programmable Gate Array (FPGA) components, and Erasable Programmable Logic Devices (EPLDs).
Propeller Control System (PCS)	Any system or device that is part of the propeller type design, which controls, limits or monitors propeller operation.

DRAFT

## DRAFT

Redundancy	Multiple independent methods incorporated within a system to accomplish a given function.
Uncovered Fault	A fault or failure for which either no detection mechanism exists or, if detected, no accommodation exists.

### 5. Background.

a. Section 33.28 regulates the general design and functioning of the ECS. This regulation does not replace or supersede other regulations governing individual ECS components. These components, such as alternators, sensors, and actuators, are regulated under other part 33 sections, such as § 33.67 for the fuel system and § 33.91 for individual component tests.

b. This guidance focuses on electrical and electronic issues related to aircraft engine control systems. For EECSs, this AC also provides guidance for compliance with § 33.28 with special consideration to interfaces with the aircraft and the propeller.

(1) This AC gives guidance on the precautions to be taken when using electrical and electronic technology for engine control, protection, limiting and monitoring functions, and, where applicable, for integration of functions specific to the aircraft or to the propeller. In these latter cases, this AC applies to functions integrated into the EECS, but only to the extent that these functions affect compliance with part 33. Functions that are added to the EECS, which are not required for compliance with part 33, but are required for installation compliance, must be documented in the engine installation manual.

(2) This guidance primarily addresses the thrust and power functions of an EECS, since thrust and power are the prime functions of the engine. Other functions, such as bleed air valve control, that may be integrated into the system for control of engine operation are also addressed in this AC. The principles outlined in this AC apply to the whole ECS.

(3) Finally, introducing electronic engine control technology entails increased engine and aircraft control and control indicator integration, and an increased risk of failures affecting more than one engine. The applicant should, therefore, take special design precautions to minimize any adverse effects which might occur. For example, the design should minimize adverse effects that develop because of any of the following:

(a) Insufficient protection from electromagnetic disturbance (lightning, internal or external radiation effects),

(b) Insufficient integrity of the aircraft electrical power supply,

(c) Insufficient integrity of data supplied from the aircraft,

(d) Hidden design faults or discrepancies within the design of the propulsion system control software or electronic hardware, or

DRAFT

DRAFT

(e) Omissions or errors in the system/software/ electronic hardware specification.

This AC, therefore, provides the applicant with additional guidance on design precautions needed due to the increased complexity of electronic engine control technology.

DRAFT

DRAFT

CONTENTS

1. Purpose	1
2. Applicability	1
3. Related References	2
4. Definitions	4
5. Background	7
6. Section 33.28 – General	10
7. Section 33.28(a) - Applicability	10
8. Section 33.28(b)(1) - Validation	11
9. Section 33.28(b)(2) – Environmental Limits	12
10. Section 33.28(c) – Control Transitions	15
11. Section 33.28(d) – Engine Control System Failures	19
12. Section 33.28(e) – System Safety Assessment	26
13. Section 33.28(f) – Protection Systems	29
14. Section 33.28(g) –Software	31
15. Section 33.28(h) – Aircraft-Supplied Data	35
16. Section 33.28(i) – Aircraft-Supplied Electrical Power	40
17. Section 33.28(j) – Air Pressure Signal	43
18. Section 33.28(k) – Automatic Availability and Control of Engine Power for a 30-Second OEI rating	44
19. Section 33.28(l) – Engine Shut Down Means	44
20. Section 33.28(m) – Programmable Logic Devices (PLD)	45
21. Other Considerations: Engine, Propeller and Aircraft Systems Integration and Relations between Engine, Propeller and Aircraft Certification Activities	46

DRAFT

6. Section 33.28 - General. One of the objectives for the engine manufacturer in an engine certification program is to show that the certificated engine should be "installable" in a particular aircraft or aircraft type. We recognize that the determination of compliance of the engine control system with applicable aircraft certification regulations will only be made during aircraft certification. When the aircraft application is unknown at the time of engine certification, the engine manufacturer should make reasonable installation and operational assumptions for the target application. Any installation limitations or operational issues must be noted in the engine installation or operating instructions and/or the type certification data sheet (TCDS). We also recommend that the engine and aircraft manufacturers coordinate with the appropriate FAA certification offices, as discussed further in this AC.

7. Section 33.28(a) - Applicability.

a. Rule Text. Section 33.28(a) reads: "Applicability. These requirements are applicable to any system or device that is part of engine type design, that controls, limits, or monitors engine operation, and is necessary for the continued airworthiness of the engine."

b. Guidance: Applicability.

(1) Section 33.28 applies to all types of Engine Control Systems (ECS) including any of the following ECS types:

- hydromechanical
- hydromechanical with a limited authority electronic supervisor
- single channel full authority electronic engine control with hydromechanical back-up
- dual channel full authority EEC without back-up, or
- any other combination.

(2) In accordance with the definition, the ECS includes all equipment necessary for controlling the engine and ensuring safe operation of the engine within its limits as specified in § 33.28. Since § 33.28 is so broad, many components, including electronic control unit(s), variable-geometry actuators, cables, wires, sensors, overspeed, over-torque, and over-temperature protection systems, and fuel metering unit(s), are part of the ECS. Similarly, some engine monitoring systems, specifically those that are physically or functionally integrated with the engine control system, perform functions that affect engine safety, or are used in the context of continued-operation or return-to-service decisions are also ECS. Even low cycle fatigue (LCF) cycle counters for engine critical parts, as well as some trend monitors and devices that provide information for maintenance, are part of the ECS.

(3) Some exclusions exist. For example, fuel pumps aren't included; even though often engine-mounted and integrated with the fuel metering unit. They are excluded since they are generally considered part of the fuel delivery system. However, as demand control pumps are introduced they will need to be considered to a part of the ECS. Any other engine overspeed design feature that is purely mechanical, like rotor interference, or fuel cutoff methods through rotor axial movement, is not considered part of the ECS. For example, overspeed protection via

DRAFT

blade shedding is a purely mechanical protection means, so blade shedding is not part of the ECS.

8. Section 33.28(b)(1) - Validation.

a. Rule Text. Section 33.28(b)(1) reads: “Validation.

(1) Functional Aspects. The applicant must substantiate by tests, analysis, or a combination thereof, that the engine control system performs the intended functions in a manner which:

(i) enables selected values of relevant control parameters to be maintained and the engine kept within the approved operating limits over changing atmospheric conditions in the declared flight envelope;

(ii) complies with the operability requirements of §§ 33.51, 33.65 and 33.73, as appropriate, under all likely system inputs and allowable engine power or thrust demands, unless it can be demonstrated that this is not required for non-dispatchable specific control modes in the intended application, in which case the engine would be approved;

(iii) allows modulation of engine power or thrust with adequate sensitivity over the declared range of engine operating conditions; and

(iv) does not create unacceptable power or thrust oscillations.”

b. Guidance: Validation.

(1) The specific exclusion for non-dispatchable modes in § 33.28(b)(1)(ii) is intended to create the opportunity to maintain engine operation, even if limited, to support a “get home” configuration.

(2) When evaluating adequate sensitivity in compliance with § 33.28(b)(1)(iii), the applicant should consider two additional aspects of power or thrust modulation. First, the power or thrust setting regions should be void of any inversions. Second, flats, or “no response” regions, in the power or thrust setting implementation, other than at the ends of range are undesirable, except for positions that represent fixed power settings like maximum climb or cruise power. The applicant should also show that a continuous positive relationship exists between increasing the power lever setting in the cockpit and the resultant engine thrust or power output, unless the applicant shows that in special applications safety is enhanced by deviating from this relationship.

(3) For engine control systems that have a power turbine speed governing mode, § 33.28 (b)(1)(iii) refers to the ability to manage power as required to maintain power turbine speed within specified limits.

(4) Power and thrust oscillations are discussed further in paragraph 11 below.

9. Section 33.28(b)(2) – Environmental Limits.

a. Rule Text. Section 33.28(b)(2) reads: “Environmental Limits. The applicant must demonstrate, when complying with §§ 33.53 or 33.91, that the engine control system functionality will not be adversely affected by declared environmental conditions, including electromagnetic interference (EMI), High Intensity Radiated Fields (HIRF), and lightning. The limits to which the system has been qualified must be documented in the engine installation instructions.”

b. Guidance: Environmental Limits. Environmental conditions include temperature, vibration, humidity, EMI, HIRF and lightning, among others. The environmental conditions requirements are addressed under §§ 33.53 and 33.91.

(1) Environmental Test Procedures and Test Limits. To understand further what you will need to do to show compliance with §§ 33.53, 33.91, and 33.28, we recommend SAE ARP5757 and AC 21-16E. The AC generally advocates use of RTCA DO-160E for testing, but MIL STD 810 may be used when the tests are equal to or more rigorous than those defined in RTCA DO-160E/EUROCAE ED14E. We also recommend that installers use AC 20-136A to show compliance at the aircraft level.

(2) Radio Frequency (RF) Emission Test Procedures and Test Limits. The procedures and limits in MIL-STD-461 or RTCA DO-160E Section 21 are acceptable.

(3) HIRF and Lightning Tests.

(a) Test Levels. The engine control system should be tested with HIRF and lightning test levels determined and agreed upon by the engine and aircraft applicants. Applicants should select these HIRF and lightning test levels so that the installation meets the aircraft certification regulations. Successful completion of the engine control system HIRF and lightning tests at these levels must be declared for engine type certification and documented in the engine installation instructions.

1 Aircraft Installation Relevance. The HIRF and lightning test levels are typically determined through lightning transient and HIRF attenuation characterization tests on the aircraft with the engines installed. If the HIRF and lightning test levels for the engine installation on a particular aircraft are not known at the time of the engine certification, the engine applicant may choose to use the HIRF and lightning test levels in the following paragraphs. However, these test levels should be confirmed by lightning transient characterization and HIRF attenuation tests on the aircraft with the engines installed before aircraft certification. Additional engine control system HIRF and lightning tests may be required if the aircraft characterization shows that these test levels are not high enough.

2 HIRF Levels. The minimum levels for system laboratory HIRF conducted RF susceptibility tests must be RTCA/DO-160E Category W (150 mA). The minimum levels for system laboratory HIRF radiated RF susceptibility continuous wave (CW) and square wave

## DRAFT

(SW) modulation tests must be RTCA/DO-160E Category W (100 v/m). The minimum levels for system laboratory HIRF radiated RF susceptibility pulse modulation tests must be RTCA/DO-160E Category D (up to 750 v/m). For engine control systems intended for rotorcraft installations, the minimum levels for system laboratory HIRF radiated RF susceptibility CW and SW modulation tests must be RTCA/DO-160E Category Y (200 v/m) and the minimum levels for radiated RF susceptibility pulse modulation tests must be RTCA/DO-160E Category J (up to 1800 v/m).

3 Lightning Levels. The minimum levels for system laboratory lightning tests must be RTCA/DO-160E Section 22 Level 3 for cable bundle injection tests and pin injection tests. The waveform set that includes single stroke, multiple stroke, and multiple burst waveforms for shielded wire bundles should be selected. This is represented by Category A3J33 in RTCA/DO-160E Section 22.

(b) Test Procedures. The engine control system used for the lightning and HIRF tests should include sensors, actuators, and engine and engine-aircraft interface wire bundles. The applicant should use the HIRF and lightning test procedures provided in RTCA DO-160E/EUROCAE ED14E Sections 20 and 22. However, the test procedures defined in RTCA DO-160E/EUROCAE ED14E Sections 20 and 22 are oriented to equipment tests. Therefore, the applicant must adapt these test procedures to a system level HIRF test to demonstrate compliance with §§ 33.53 and 33.91. Further guidance on system level HIRF tests is available in SAE ARP5583. SAE ARP5415 and ARP5416 provide guidance on system level lightning tests. The applicant should conduct lightning pin injection tests on the electronic engine control and other system components that are part of the engine control system.

(c) Open Loop and Closed Loop Testing. The applicant should conduct HIRF and lightning tests on the engine control system operating in closed loop or open loop control. The closed loop set-up is usually provided with power to move actuators to close the inner actuating loops. A simplified engine simulation may be used to close the outer engine loop. HIRF and lightning tests should be conducted with the engine control system controlling at the most sensitive operating point, as selected and detailed in the test plans by the applicant. The system should be exposed to the HIRF and lightning environments while operating at the selected condition. HIRF and lightning environments may have different most sensitive operating points.

(d) Test Considerations. The following factors should also be considered:

- If special engine control system test software is used, that software must be developed and implemented by guidelines defined for software levels of at least Level 2 in DO-178A, Level C in DO-178B, or equivalent. In some cases, the application code is modified to include the required test code features.
- The system test set-up must be capable of monitoring both the output drive signals and the input signals.
- Anomalies observed during open loop testing on inputs or outputs must be duplicated on the engine simulation to determine whether the resulting power or thrust perturbations comply with the pass/fail criteria.

DRAFT

## DRAFT

(e) Pass/Fail Criteria. To comply with §§ 33.53 and 33.91, the HIRF and lightning tests must cause no adverse effects on the functionality of the engine control system. The following are considered adverse effects:

- A change greater than 3% of point or 1% of take-off power and/or thrust, whichever is greater, for a period of more than 2 seconds
- Transfers to alternate channels, back-up systems, or alternate modes
- Component damage
- False annunciation to the crew that could cause unnecessary or inappropriate crew action
- Erroneous operation of protection systems, such as over-speed or thrust reverser circuits

Note: Hardware or software design changes implemented after initial environmental testing should be evaluated for their effects with respect to the EMI, HIRF and lightning environment.

### (4) Maintenance Actions.

(a) Section 33.4 requires that the applicant prepare Instructions for Continued Airworthiness (ICA). AC 33.4-3 specifically addresses the ICA related to the aircraft engine HIRF and lightning protection. These ICA include a maintenance plan. Therefore, the applicant must provide a maintenance plan for any protection system that is part of the type design of the engine control system and is required to meet the qualified levels of EMI, HIRF and lightning to ensure the continued airworthiness for the parts of the installed system that are supplied by the engine type certificate holder.

(b) The maintenance actions to be considered include periodic inspections or tests for required structural shielding, wire shields, connectors, and equipment protection components. The applicant may also consider inspections or tests when the part is exposed. The applicant must provide the engineering validation and substantiation of these maintenance actions.

(5) Time Limited Dispatch Environmental Tests. Although TLD is only an optional requirement, the applicant should conduct EMI, HIRF and lightning tests for TLD together with tests for certification. See paragraph 7.c. of the Policy Memorandum, PS-ANE100-2001-1993-33.28TLD-R1, for the TLD requirements related to environmental compliance.

### 10. Section 33.28(c) – Control Transitions.

#### a. Rule Text. Section 33.28(c) reads: “Control Transitions.

(1) The applicant must demonstrate that, when fault or failure results in a change from one control mode to another, from one channel to another, or from the primary system to the back-up system, the change occurs so that:

- (i) the engine does not exceed any of its operating limitations,

DRAFT

DRAFT

(ii) the engine does not surge, stall, or experience unacceptable thrust or power changes or oscillations or other unacceptable characteristics; and

(iii) there is a means to alert the flight crew if the crew is required to initiate, respond to, or be aware of the control mode change. The means to alert the crew must be described in the engine installation instructions, and the crew action must be described in the engine operating instructions; and

(2) The magnitude of any change in thrust or power and the associated transition time must be identified and described in the engine installation instructions and the engine operating instructions.”

b. Guidance: Control Transitions.

(1) General.

(a) Under § 33.28(b)(1), the applicant must perform all necessary testing and analysis to ensure that all control modes, including those that occur as a result of control fault accommodation strategies, are implemented as required.

(b) All declared dispatchable control modes must be capable of performing their intended functions in the environmental conditions, including EMI, HIRF and lightning, declared in the engine installation instructions.

(c) The need to provide protective functions, such as over-speed protection, for all control modes, including any alternate modes, must be reviewed under the regulations of § 33.28(d), (e), and (f) and § 33.75.

(d) The above requirements apply to the engine control system operating in any dispatchable configuration.

(e) Any limitations on operations in alternate modes must be clearly stated in the engine installation and operating instructions.

(f) Descriptions of the functioning of the engine control system operating in its primary and any alternate modes must be provided in the engine installation and operating instructions.

(g) Analyses and/or testing are necessary to substantiate that changing to and operating in the alternate modes has no unacceptable effect on engine durability or endurance.

(h) Demonstration of the durability and reliability of the control system in all modes may be primarily addressed by the engine system and component testing of §§ 33.53 and 33.91. Performing some portion of the engine certification testing in the alternate mode(s) and

DRAFT

during transition between modes can be used as part of the system validation required under § 33.28(b)(1).

(i) Engine Test Considerations.

1 If the engine certification tests defined in part 33, Subpart F, are performed using only the engine control system's primary mode in the full-up configuration and if the applicant requests approval for dispatch in the alternate mode under TLD, the applicant must demonstrate, by analysis and/or test, that the engine can meet the defined test-success criteria when operating in any alternate mode that is proposed as a dispatchable configuration. This applies to test requirements that demonstrate capabilities such as operability or rain, hail, or bird ingestion.

2 Some capabilities, such as operability or rain, hail, or bird ingestion, may be lost in some control modes that are not dispatchable. These modes do not require engine test demonstration as long as the engine installation and operating instructions reflect this loss of capability.

(j) Availability. Availability of any back-up mode must be established by routine testing or monitoring to ensure that the back-up mode will be available when needed. The applicant must document in the ICA the minimum frequency of inspection or testing needed to ensure the availability of the back-up mode.

(2) Crew Training Modes. This acceptable means of compliance is not specifically intended to apply to any crew training modes. These modes are usually installation, and possibly operator, specific, and need to be negotiated on a case-by-case basis. As an example, one common application of crew training modes is for simulation of the 'failed-fixed' mode on a twin-engine rotorcraft. Training modes must be described in the engine installation and operating instructions as appropriate. Also, precautions must be taken in the design of the engine control system and its crew interfaces to prevent inadvertent entry into any training modes. Crew training modes, including lock-out systems, must be assessed as part of the System Safety Assessment (SSA) of § 33.28 (e).

(3) Non-Dispatchable Configurations and Modes.

(a) For control configurations which are not dispatchable, but for which the applicant seeks to take credit in the system LOTC/LOPC analysis, specific operating limitations may be acceptable. This means that the system will not be charged with a LOTC/LOPC event when the fault is covered by a back-up means that allows the system to continue to function safely, even though it would not be dispatchable in this configuration. In addition, compliance with § 33.28(b)(1) does not imply strict compliance with the operability regulations of § 33.65 and § 33.89 in these non-dispatchable configurations if it can be demonstrated that, in the intended installation, no likely pilot control system inputs will result in engine surge, stall, flame-out or unmanageable delay in power recovery. For example, in a twin-engine rotorcraft, a rudimentary back-up system may be adequate since frequent and rapid changes in power setting

## DRAFT

when operating in the back-up system may not be necessary. In this example, it is very unlikely that dispatch would be allowed with the engine controlled by this rudimentary back-up system.

(b) In addition to these operability considerations, other factors that should be considered in assessing the acceptability of a reduced-capability back-up mode include:

- The installed operating characteristics of the back-up mode and the differences from the primary mode.
- The likely impact of the back-up mode operations on pilot workload, if the aircraft installation is known.
- The frequency of transfer from the primary mode to the back-up mode (i.e. the reliability of the primary mode). Frequencies of transfer of less than 1 per 20,000 engine flight hours have been considered acceptable.

#### (4) Control Transitions.

(a) The intent of § 33.28(c) is to ensure that any control transitions, which occur as a result of fault accommodation, occur in an acceptable manner.

(b) In general, the engine control system should transition to alternate modes automatically. However, systems in which pilot action is required to engage the back-up mode may also be acceptable. For instance, a fault in the primary system may result in a “failed-fixed” fuel flow which requires some action by the pilot to engage the back-up system to modulate engine power. The applicant should ensure that any reliance on manual transition is not expected to pose an unacceptable operating characteristic, unacceptable crew workload, or require exceptional skill.

(c) The transient change in power or thrust associated with transfer to alternate modes must be reviewed for compliance with § 33.28(c). If available, the applicant should consider input from the installer.

(d) Although not a complete list, some of the items that should be considered when reviewing the acceptability of control mode transitions are:

1 The frequency of occurrence of transfers to any alternate mode and the capability of the alternate mode. Computed frequency-of-transfer rates should be supported with data from endurance or reliability testing, in-service experience on similar equipment, or other appropriate data.

2 The magnitude of the power, thrust, rotor or propeller speed transients. The magnitude of the changes in these parameters impacts the installation and therefore should be reasonably assured to be acceptable for installation.

3 Successful demonstration, by simulation or other means, of the ability of the engine control system to control the engine safely during the transition. In some cases, particularly those involving rotorcraft, it may not be possible to determine that the mode

DRAFT

transition provides a safe system based solely on analytical or simulation data. Therefore, the FAA normally expects a flight test program to support this data during aircraft certification.

4 An analysis should be provided to identify those faults that cause control mode transitions either automatically or through pilot action.

5 For turboprop or turboshaft engines, the control mode transition should not result in excessive over-speed or under-speed of the rotor or propeller that could cause emergency shutdown, loss of electrical generator power, or the setting-off of warning devices.

6 The power or thrust change associated with the transition should be declared in the engine installation instructions.

(e) Time Delays. Any observable time delays associated with control mode, channel or system transitions, or in re-establishing the pilot's ability to modulate engine thrust or power must be identified in the engine installation and operating instructions. The acceptability of these delays should be assessed during aircraft certification.

(f) Annunciation to the Flight Crew.

1 If annunciation is necessary to comply with § 33.28(c)(1)(iii), the type of annunciation to the flight crew must be commensurate with the nature of the transition. For example, the form of annunciation for a reversion to an alternate mode of control when the transition is automatic and the only observable changes in operation of the engine are different thrust control schedules would be very different than if timely action by the pilot is required to maintain control of the aircraft.

2 The intent and purpose of the cockpit annunciation must be clearly stated in the engine installation and operating instructions, as appropriate.

#### 11. Section 33.28(d) – Engine Control System Failures.

a. Rule Text. Section 33.28(d) reads: “Engine control system failures. The applicant must design and construct the engine control system so that:

(1) the rate for Loss of Thrust (or Power) Control (LOTC/LOPC) events, consistent with the safety objective associated with the intended application can be achieved, and

(2) in the full-up configuration, the system is single fault tolerant, as determined by the Administrator, for electrical or electronic failures with respect to LOTC/LOPC events, and

(3) single failures of engine control system components shall not result in a hazardous engine effect, and

(4) foreseeable failures or malfunctions leading to local events in the intended aircraft installation such as fire, overheat, or failures leading to damage to engine control system

DRAFT

components must not result in a hazardous engine effect due to engine control system failures or malfunctions.”

b. Guidance: Engine Control System Failures.

(1) Objective. The intent of § 33.28(d) is to establish engine control system integrity requirements consistent with the operational requirements of the various installations. In particular, the introduction of EECSSs should provide at least an equivalent level of safety and reliability for the engine, as achieved by engines equipped with hydromechanical control and protection systems and magneto systems.

(2) Criteria for an LOTC/LOPC Event.

(a) For turbine engines intended for part 25 installations. A LOTC/LOPC event occurs when the ECS:

- has lost the capability of modulating thrust or power between idle and 90% of maximum rated power or thrust;
- suffers a fault which results in a thrust or power oscillation greater than the levels given in paragraph 11.b.(3) of this AC; or
- has lost the capability to govern the engine in a manner which allows compliance with the operability regulations given in §§ 33.65 and 33.89.

(b) For turbine engines intended for rotorcraft. A LOTC/LOPC event occurs when the ECS:

- has lost the capability of modulating power between idle and 90% of maximum rated power at the flight condition, except One-Engine-Inoperative (OEI) power ratings;
- suffers a fault which results in a power oscillation greater than the levels given in paragraph 11.b.(3) of this AC; or
- has lost the capability to govern the engine in a manner which allows compliance with the operability regulations given in §§ 33.65 and 33.89, with the exception that the inability to meet the operability regulations in the alternate modes may not need to be included as LOPC events.

1 Single engine rotorcraft will normally be required to meet the operability regulations in the alternate mode(s). Engine operability in the alternate mode(s) is a necessity if:

- the control transitions to the alternate mode occurs more frequently than the acceptable LOPC rate; or
- normal flight crew activity requires rapid changes in power to safely fly the aircraft.

DRAFT

2 For multi-engine rotorcraft, the LOPC definition may not need to include the inability to meet the operability regulations in the alternate mode(s). This may be acceptable because when one engine control transitions to an alternate mode that may not have robust operability, that engine can be left at reasonably fixed power conditions. The engine(s) with the normally operating control(s) can change power as necessary to complete aircraft maneuvers and safely land the aircraft. Demonstration of the acceptability of this type of operation may be required at aircraft certification.

(c) For turbine engines intended for other installations. A LOTC/LOPC event occurs when the ECS :

- has lost the capability of modulating thrust or power between idle and 90% of maximum rated power or thrust,
- suffers a fault which results in a thrust or power oscillation that would impact controllability in the intended installation, or
- has lost the capability to govern the engine in a manner which allows compliance with the operability regulations in §§ 33.65 and 33.89, as appropriate.

(d) For reciprocating engines. A LOPC event occurs when the ECS:

- has lost the capability of modulating power between idle and 85% of maximum rated power at all operating conditions,
- suffers a fault which results in a power oscillation greater than the levels given in paragraph 11.b.(3) of this AC, or
- has lost the capability to govern the engine in a manner which allows compliance with the operability regulations in § 33.89.

(e) For engines incorporating functions for propeller control integrated in the EECS. The following faults or failures should also be considered as LOPC events:

- inability to command a change in pitch
- uncommanded change in pitch, or
- uncontrollable propeller torque or speed fluctuation.

(3) Uncommanded thrust or power oscillations. Any uncommanded thrust or power oscillations must not be of such a magnitude as to impact aircraft controllability in the intended installation. Thrust or power oscillations less than 10% peak to peak of take-off power and/or thrust have been considered acceptable in some installations where the failure affects one engine only. Regardless of the levels discussed herein, if the flight crew has to shut down an engine because of unacceptable thrust or power oscillations caused by the control system, such an event would be deemed an in-service LOTC/LOPC event.

(4) Acceptable LOTC/LOPC rate. The applicant may propose an LOTC/LOPC rate other than those below. Such a proposal should be substantiated in relation to the criticality of

## DRAFT

the engine and control system relative to the intended installation. The intent is to show equivalence of the LOTC/LOPC rate to existing systems in comparable installations.

(a) For turbine engines. The EECS must not cause more than one LOTC/LOPC event per 100,000 engine flight hours.

(b) For reciprocating engines. An LOPC rate of 45 per million engine flight hours (or 1 per 22,222 engine flight hours) represents an acceptable level for the most complex EECS. As a result of the architectures used in many of the EECS for these engines, the functions are implemented as independent system elements. These system elements or sub-systems can be fuel control, ignition control, or others. If a system were to contain only one element, such as fuel control, then the appropriate total system level would be 15 LOPC events per million engine flight hours. The system elements are then additive up to a maximum of 45 LOPC events per million hours. For example, an EEC system comprised of fuel, ignition, and wastegate control functions must meet a total system reliability of  $15+15+15 = 45$  LOPC events per million engine flight hours. This criteria is then applied to the entire system and not allocated to each of the subsystems. Note that a maximum of 45 LOPC events per million engine flight hours are allowed, regardless of the number of subsystems. For example, if the EEC system includes more than three subsystems, the sum of the LOPC rates for the total system must not exceed 45 LOPC events per million engine flight hours for all of the control system elements.

(5) Reliability Assessment Plan. The applicant must prepare a reliability assessment plan (see SAE ARP5890 for a framework). This plan documents the controlled, repeatable processes for assessing the reliability of systems and equipment. It also can help assess the reliability of systems and equipment during their design and operational life. Reliability assessment results are important inputs to many safety assessment and analysis tasks. The results of a plan can be used as a part of:

- Reliability program planning and monitoring
- Safety assessments and analyses
- Certification analyses
- Equipment design decisions
- System architecture selection, and
- Continued airworthiness assessments.

(6) LOTC/LOPC Analysis.

(a) The applicant must submit a system reliability analysis (see SAE ARP5107) to substantiate the agreed LOTC/LOPC rate for the engine control system. A numerical analysis such as a Markov model analysis, fault tree analysis, or equivalent analytical approach is recommended.

(b) The analysis must address all components in the system that can contribute to LOTC/LOPC events. This includes all electrical, mechanical, hydromechanical, and pneumatic elements of the engine control system.

DRAFT

(c) The engine fuel pump is generally not included in the definition of the engine control system, since it is usually considered part of the fuel delivery system.

(d) The LOTC/LOPC analysis must include those sensors or elements which may not be part of the engine type design but which may contribute to LOTC/LOPC events. An example is the throttle or power lever transducer, which is usually supplied by the installer. The LOTC/LOPC analysis must include the effects of loss, corruption, or failure of aircraft-supplied data. The engine installation instructions must include the assumed reliability and interface requirements for these non-engine type design elements. Within the aircraft system safety analyses, the installer should ensure that there is no double counting of the rate of failure of non-engine parts.

(e) The LOTC/LOPC analysis must consider all faults, both detected and undetected. Any periodic maintenance actions needed to find and repair both covered and uncovered faults to meet the LOTC/LOPC rate must be contained in the engine instructions for continued airworthiness.

(f) This LOTC/LOPC analysis should be done in conjunction with the System Safety Assessment required under § 33.28(e). Paragraph 12 of this AC provides additional guidance.

(7) Commercial or Industrial Grade Electronic Parts.

(a) The grade and handling of electronic parts is an important contributor to the reliability of the EEC. Two examples of industry documents that provide guidance on the application of commercial or industrial grade components are:

- IEC/TS 62239, Process Management for Avionics – Preparation of an Electronic Components Management Plan
- IEC/TR 62240, Process Management for Avionics - Use of Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges

(b) When the engine type design specifies commercial or industrial-grade electronic components, which are not manufactured to military standards, the applicant should have the following data available for review, as applicable:

1 Reliability data for each commercial and industrial grade electrical component specified in the design.

2 The applicant's procurement, quality assurance, and process control plans for the vendor-supplied commercial and industrial grade parts. These plans should ensure that the parts will be able to maintain the reliability level specified in the approved engine type design.

3 Unique databases for similar components obtained from different vendors, because commercial and industrial grade parts may not all be manufactured to the same accepted industry standard.

DRAFT

## DRAFT

(c) Commercial and industrial grade parts have typical operating ranges of 0 to +70 degrees Celsius and -40 to +85 degrees Celsius, respectively. Military grade parts are typically rated at -54 d to 125 degrees Celsius. Commercial and industrial grade parts are typically defined in these temperature ranges in vendor parts catalogues. If the declared temperature environment for the engine control system exceeds the stated capability of the commercial or industrial grade electronic components, the applicant must substantiate that the proposed extended range of the specified components is suitable for the installation and that the failure rates used for those components in the SSA and LOTC/LOPC analyses is appropriately adjusted for the extended temperature environment. Additionally, if commercial or industrial parts are used in an environment beyond their specified rating and cooling provisions are required in the design of the EECS, the applicant must specify these provisions in the engine installation instructions to ensure that the provisions for cooling are not compromised. The cooling provisions included in the EECS design may have failure modes. If failures such as these could result in exceeding the temperature limits, the applicant must account for the probability of these failures in the SSA and LOTC/LOPC analyses.

(d) When any electrical or electronic components are changed, the applicant should review SSA and LOTC/LOPC analyses with regard to the impact of any changes in component reliability. Component, subassembly or assembly level testing may be needed to substantiate a change that introduces commercial or industrial part(s). However, such a change would not be classified as “significant” with respect to § 21.101(b)(1).

### (8) Single Fault Accommodation.

(a) The FAA considered using the phrase “essentially single fault tolerant” in proposed paragraph § 33.28(d)(2) as the standard for measuring the compliance of an applicant’s engine control system. After extensive discussions with the industry about the meaning of “essentially single fault tolerant,” the FAA determined that the term “essentially” introduces sufficient ambiguity into a regulation so that the phrase could not serve as the basis for an enforceable standard. Therefore, we removed “essentially” and reserved the right to determine what is meant by “single fault tolerant” to the Administrator. The following guidance clarifies the meaning of “single fault tolerant.”

(b) Compliance with the single fault regulations of § 33.28(d)(2) and (3) may be substantiated by a combination of tests and analyses. Single failures or malfunctions in the engine control system’s components, in its fully operational condition and all declared dispatchable configurations, must not result in a hazardous engine effect. In addition, in its full-up configuration the control system must be essentially single fault tolerant of electrical/electronic component failures with respect to LOTC/LOPC events. We recognize that to achieve true single fault tolerance for LOTC/LOPC events could require a triplicated design approach or one with 100% fault detection. Currently, systems have been designed with dual, redundant channels or with back-up systems that provide what has been called an “essentially single fault tolerant” system. Although these systems may have some single faults (that are not covered faults) which lead to LOTC/LOPC events, they have demonstrated excellent in-service safety and reliability and have proven to be acceptable.

DRAFT

## DRAFT

(c) The objective is to address all the faults as covered faults. Indeed, the dual channel or back-up system configurations cover the vast majority of potential electrical and electronic faults. However, on a case-by-case basis, we may approve the applicant omitting some coverage because detection or accommodation of some electrical/electronic faults may not be practical. In these cases, we recognize that single, simple electrical or electronic components or circuits can be employed in a reliable manner and that requiring redundancy in some situations may not be appropriate. In these circumstances, failures in certain single electrical or electronic components, elements, or circuits may result in an LOTC/LOPC event. These systems, which are referred to as “essentially single fault tolerant,” are acceptable.

### (9) Local Events.

(a) Local events to be considered under § 33.28(d)(4) include:

- Overheat conditions, for example, those resulting from hot air duct bursts,
- Fires, and
- Fluid leaks or mechanical disruptions that could lead to damage to control system electrical harnesses or connectors or to the control unit(s).

(b) These local events are normally limited to one engine. Therefore, a local event is not usually considered a common mode event, and common mode threats, such as HIRF, lightning and rain, are not considered local events. Examples of a single, common mode fault in systems are single source batteries in multi-engine applications and the use of identical software in multi-engine, dual-channel systems. In these and similar cases, extra design, testing or maintenance precautions are taken to ensure safety.

(c) Whatever the local event, the behavior of the EECS must not cause a hazardous engine effect in any declared dispatchable mode.

(d) When a demonstration that there is no hazardous engine effect is based on the assumption that another function exists to afford the necessary protection, the applicant must show that this function is not rendered inoperative by the same local event on the engine (including destruction of wires, ducts, or power supplies).

(e) An overheat condition exists when the temperature of the system components is greater than the maximum safe design operating temperature for the components, as declared by the engine applicant in the engine installation instructions. The engine control system must not cause a hazardous engine effect when the components or units of the system are exposed to an overheat or over-temperature condition or when it cools down. Specific design features or analysis methods may be used to show compliance with respect to the prevention of hazardous engine effects. We may require testing when this is not possible; for example, due to the variability or the complexity of the failure sequence.

(f) The engine control system, including the electrical, electronic, and mechanical parts of the system, must comply with the fire regulations of § 33.17 and follow the guidance of

DRAFT

AC 33.17-1. This rule applies to the elements of the engine control system that are installed in designated fire zones.

(g) If an ECS component is located so that it could present an ignition source for flammable fluids or vapors, an explosion proof demonstration is required to verify that the component cannot be the source of ignition for an explosion. See SAE ARP5757 for this type of demonstration.

(h) Since no probability is associated with § 33.28(d)(4), applicants should consider all foreseeable local events. We recognize, however, that it is difficult to address all possible local events in the intended aircraft installation at the time of engine certification. Therefore, the applicant should use sound engineering judgment to identify reasonably foreseeable local events. Compliance with this regulation may be shown by considering the end result of the local event on the engine control system. The local events analyzed should be well documented to aid in certification of the engine installation.

(i) The following guidance applies to engine control system wiring.

1 Each wire or combination of wires interfacing with the EECS that could be affected by a local event should be tested or analyzed with respect to local events. The assessment should include opens, shorts to ground, and shorts to power (when appropriate). The results should show that faults result in specific responses and do not result in hazardous engine effects.

2 The applicant should test or analyze engine control unit aircraft interface wiring for shorts to aircraft power; these “hot” shorts should result in a specific and non-hazardous engine effect. Where aircraft interface wiring is involved, the engine installation instructions must inform the installer of the potential effects of shorts in the interface wiring. The installer must ensure that no wiring faults exist which could affect more than one engine.

3 Where practical, wiring faults should not affect more than one channel. The engine applicant should include any assumptions regarding channel separation in the LOTC/LOPC analysis.

4 Where physical separation of conductors is not practical, the engine applicant and the installer should coordinate to ensure that the potential for common mode faults between engine control systems is eliminated and between channels on one engine is minimized.

5 The applicant should assess, by analysis or test, the effects of fluid leaks impinging on components of the EECS. Such conditions must not result in a hazardous engine effect, and the fluids may not be allowed to impinge on circuitry or printed circuit boards or result in a potential latent failure condition.

12. Section 33.28(e) – System Safety Assessment.

DRAFT

a. Rule Text. Section 33.28(e) reads: “System safety assessment. When complying with §§ 33.28 and 33.75, the applicant must complete a System Safety Assessment for the engine control system. This assessment must identify faults or failures that result in a change in thrust or power, transmission of erroneous data, or an effect on engine operability together with the predicted frequency of occurrence of these faults or failures.”

b. Guidance: System Safety Assessment.

(1) Scope of the assessment.

(a) The SSA required under § 33.28 (e) must address all operating modes, and the data used in the SSA must be substantiated.

(b) The LOTC/LOPC analysis described in § 33.28(d) is a subset of the SSA. The LOTC/LOPC analysis and SSA may be separate or combined as a single analysis.

(c) The SSA must consider all faults, both detected and undetected, and their effects on the engine control system and engine operation. Primarily, the SSA must address the faults or malfunctions that only affect one engine control system and therefore only one engine. However, the SSA must also include faults or malfunctions in aircraft signals, including those in a multi-engine aircraft installation that could affect more than one engine; these types of faults are addressed under § 33.28(h).

(d) The engine control system SSA and LOTC/LOPC analysis, or combined analyses, must identify the applicable assumptions and installation requirements and establish any limitations relating to engine control system operation. These assumptions, requirements, and limitations must be stated in the engine installation and operating instructions, as appropriate.

(e) As necessary, the airworthiness limitations section of the instructions for continued airworthiness should include the limitations related to the engine control system operation. For example, the LOTC/LOPC analysis classifies faults into various categories which may require repair within an approved time frame for these fault categories for the particular system being analyzed.

(f) The SSA must address all failure effects identified under § 33.75, as appropriate.

(g) The applicant must provide a summary listing the malfunctions or failures and their effects caused by the engine control system, such as:

1 Failures affecting power or thrust resulting in LOTC/LOPC events.

2 Failures which result in the engine’s inability to meet the operability regulations. If these failure cases are not considered LOPC events according to paragraph

DRAFT

11.b.(2)(b) of this AC, the expected frequency of occurrence for these events must be documented.

3 Transmission of erroneous parameters, for example, false high indication of the thrust or power setting, which could lead to thrust or power changes greater than 3% of take-off power and/or thrust (10% for reciprocating engines installations), or, for example, of high EGT or turbine temperatures or low oil pressure, which could lead to engine shutdown.

4 Failures affecting aircraft functions included in the engine control system, for example, propeller control, thrust reverser control, control of cooling air, control of fuel recirculation.

5 Failures resulting in major engine effects and hazardous engine effects.

(h) The SSA must also consider all signals used by the engine control system, particularly any cross-engine control signals and air signals as described in § 33.28(j).

(i) The aircraft applicant needs to define the criticality of functions included in the engine control system that involve aircraft level functions.

(2) Criteria. The SSA must demonstrate or provide the following:

(a) Compliance with §§ 33.75, as appropriate.

(b) For failures leading to LOTC/LOPC events, compliance with the agreed LOTC/LOPC rate for the intended installation—see paragraph 11.b.(4) of this AC.

(c) For failures affecting engine operability but not leading to LOPC events, compliance with the expected total frequency of occurrence of failures that result in engine response that is non-compliant with §§ 33.65 and 33.89 regulations (as appropriate). The acceptability of the frequency of occurrence for these events—along with any aircraft flight deck indications deemed necessary to inform the flight crew of such a condition—will be determined at aircraft certification.

(d) The consequences of the transmission of a faulty parameter by the engine control system must be identified and included, as appropriate, in the LOTC/LOPC analysis. The engine operating instructions must include any information necessary to mitigate the consequences of a faulty parameter transmission. For example, the engine operating instructions may indicate that a display of zero oil pressure should or may be ignored in-flight if the oil quantity and temperature displays appear normal. In this situation, failure to transmit oil pressure or transmitting a zero oil pressure signal should not lead to an engine shutdown or LOTC/LOPC event.

(e) Admittedly, flight crew initiated shutdowns have occurred in-service during such conditions. If the engine operating instructions provide information to mitigate the condition, then control system faults or malfunctions leading to the condition

## DRAFT

do not have to be included in the LOTC/LOPC analysis. In this situation, the loss of multiple functions should be included in the LOTC/LOPC analysis. If the display of zero oil pressure and zero oil quantity (or high oil temperature) would result in a crew-initiated shutdown, then those conditions should be included in the systems LOTC/LOPC analysis.

### (3) Malfunctions or Faults Affecting Thrust or Power.

(a) In multi-engine aircraft, faults that result in thrust or power changes of less than approximately 10% of take-off power and/or thrust may be undetectable by the flight crew. This level is based on pilot assessment and has been used for a number of years. Pilots have indicated that flight crews will note the engine operating differences when the difference is greater than 10% in asymmetric thrust or power.

(b) The detectable difference level for engines for other installations should be agreed upon with the installer.

(c) When operating in the take-off envelope, uncovered faults in the engine control system which result in a thrust or power change of less than 3% (10% for reciprocating engines installations) are generally considered acceptable. However, this does not diminish the applicant's obligation to ensure that the full-up system is capable of providing the declared minimum rated thrust or power. In this regard, faults that could result in small thrust changes should be random in nature and detectable and correctable during routine inspections, overhauls, or power-checks.

(d) The SSA documentation should include the frequency of occurrence of uncovered faults that result in a thrust or power change greater than 3% of take-off power and/or thrust, but less than the change defined as an LOTC/LOPC event. No specific regulations relating to this class of faults for engine certification exist. However, the rate of occurrence of these types of faults should be reasonably low, on the order of  $10^{-4}$  events per engine flight hour or less. These faults may be required in the aircraft certification analysis.

(e) Signals sent from one engine control system to another, such as signals used for an ATTCS or synchrophasing, are addressed under § 33.28(h). These cross-engine signals must be limited in authority by the receiving engine control system, so that undetected faults do not result in an unacceptable change in thrust or power for the engine using those signals. The maximum thrust or power loss on the engine using a cross-engine signal should generally be limited to 3% absolute difference of the current operating condition. We recognize that ATTCS, when activated, may command a thrust or power increase of 10% or more on the remaining engine(s). We also recognize that signals sent from one engine control to another in a rotorcraft installation, such as load sharing and OEI, can have a much greater impact on engine power when those signals fail. Data on these failure modes must be in the SSA.

(f) When operating in the take-off envelope, detected faults in the engine control system which result in a thrust or power change of up to 10% (15% for reciprocating engines) may be acceptable if the total frequency of occurrence for these types of failures is relatively

DRAFT

DRAFT

low. The predicted frequency of occurrence for this category of faults must be in the SSA documentation. Requirements for the allowable frequency of occurrence for this category of faults and any need for a flight deck indication of these conditions are reviewed during aircraft certification. A total frequency of occurrence in excess of 10<sup>-4</sup> events per engine flight hour would not normally be acceptable.

(g) Detected faults in signals exchanged between engine control systems should be accommodated so as not to result in greater than a 3% thrust or power change on the engine using the cross-engine signals.

13. Section 33.28(f) – Protection Systems.

a. Rule Text. Section 33.28(f) reads: “Protection Systems.

(1) The design and functioning of engine control devices and systems, together with engine instruments and operating and maintenance instructions, must provide reasonable assurance that those engine operating limitations that affect turbine, compressor, fan, and turbosupercharger rotor structural integrity will not be exceeded in service.

(2) When electronic overspeed protection systems are provided, the design must include a means for testing, at least once per engine start/stop cycle, to establish the availability of the protection function. The means must be such that a complete test of the system can be achieved in the minimum number of cycles. If the test is not fully automatic, the requirement for a manual test must be contained in the engine operating instructions.

(3) When overspeed protection is provided through hydromechanical or mechanical means, the applicant must demonstrate by test or other acceptable means that the overspeed function remains available between inspection and maintenance periods.”

b. Guidance: Protection Systems.

(1) Rotor Over-speed Protection.

(a) The engine control devices, systems and instruments referred to in § 33.28(f) are usually provided in engines of recent design by over-speed protection and/or circuits which, although they may be independent devices, are generally part of the EECS.

(b) Rotor over-speed protection is usually achieved by providing an independent over-speed protection system, such that it requires two independent faults or malfunctions (as described below) to result in an uncontrolled over-speed.

(c) Examples of engine provided over-speed protection include blade shedding, rotor interference, or fuel cutoff methods through rotor axial movement that are not addressed by this regulation.

## DRAFT

(d) The following guidance applies if the rotor over-speed protection is provided solely by an engine control system protective function.

1 In all dispatchable configurations, the combined engine and over-speed protection system must be at least two independent faults removed from an uncontrolled over-speed event. Hence, a potential rotor burst due to overspeed should only be possible as a result of a first fault causing an over-speed and an independent second fault preventing the over-speed protection system from operating properly.

2 The SSA must show that the probability per engine flight hour of an uncontrolled over-speed condition from any cause in combination with a failure of the over-speed protection system to function is less than one event per hundred million hours (a failure rate of  $10^{-8}$  events per engine flight hour). The SSA must consider all the failure cases associated with the protection systems. A case that should not be overlooked is when the fuel metering valve and the fuel shut-off valve (SOV) have a common failure mode.

3 The over-speed protection system must have a failure rate of less than  $10^{-4}$  failures per engine flight hour to ensure the integrity of the protected function.

4 A self-test of the over-speed protection system to ensure its functionality prior to each subsequent flight is normally necessary. Verifying the functionality of the over-speed protection system at engine shutdown and/or start-up is considered adequate for compliance with this requirement. We recognize that some engines may routinely not be shut down between flight cycles. This is acceptable and should be accounted for in the analyses.

5 Because some over-speed protection systems provide multiple protection paths, uncertainty that all paths are functional at any given time will always exist. Where multiple paths can invoke the over-speed protection system, a test of a different path may be performed for each engine cycle. The objective is to achieve a complete test of the over-speed system, including electro-mechanical parts, in the minimum number of engine cycles. If the system meets a  $10^{-4}$  failure rate, it will generally be found compliant with this requirement.

6 The applicant may provide data demonstrating that the mechanical parts (not including the electro-mechanical parts) of the over-speed protection system can operate without failure between stated periods. A periodic inspection may be established for those parts. This data is acceptable in lieu of testing the mechanical parts of the sub-system for each engine cycle.

### (2) Other Protective Functions.

(a) The engine control system may perform other protective functions; some may be engine functions, but others may be aircraft or propeller functions. Engine functions should be considered under the guidelines of this AC. The integrity of other protective functions provided by the engine control system should be consistent with a safety analysis associated with those functions, but if those functions are not engine functions, they might not be part of engine certification.

DRAFT

DRAFT

(b) As engine control systems become increasingly integrated into the aircraft and propeller systems, they are incorporating protective functions previously provided by the aircraft or propeller systems. Examples include:

- reducing the engine to idle thrust if a thrust reverser deploys, and
- providing the auto-feather function for the propeller when an engine fails.

(c) The reliability and availability associated with these functions should be consistent with the top-level hazard assessment of conditions involving these functions. This is completed during aircraft certification. For example, if an engine failure with loss of the auto-feather function is catastrophic at the aircraft level—and auto-feather is incorporated into the engine control system—the applicant must show for part 25 installations, or for part 23 installations certified to part 25, that an engine failure with loss of the auto-feather function cannot result from a single control system failure. Also, combinations of control system failures, or engine and control system failures, which lead to a significant engine loss of thrust or power with an associated loss of the autofeather function may be required to have an extremely improbable event rate ( $10^{-9}$  events per engine flight hour).

(d) Although these functions await evaluation at the aircraft level, we recommend that, if practicable, the aircraft level hazard assessment involving these functions be available at the time of the engine control system certification. This will facilitate discussion and coordination between the engine and aircraft certification teams under the conditions outlined in paragraph 21 of this AC. This coordination may not occur. Because of this, the applicant should recognize that although the engine may be certified, it may not be installable at the aircraft level.

(e) The overall requirement is that the safety assessment of the engine control system must include all failure modes of all functions incorporated in the system. This includes those functions that are added to support aircraft certification, so that the information on those failure modes will be properly addressed and passed on to the installer for inclusion in the airframe SSA. Information concerning the frequencies of occurrence of those failure modes may be needed as well.

14. Section 33.28(g) - Software.

a. Rule Text. Section 33.28(g) reads: “Software. The applicant must design, implement, and verify all associated software to minimize the existence of errors by using a method, approved by the FAA, consistent with the criticality of the performed functions.”

b. Guidance: Software.

(1) Objective.

(a) For engine control systems that use embedded software and/or complex electronic hardware in the form of programmable logic devices, the objective of §§ 33.28(g) and (m) is to prevent as far as possible logic errors that would result in an unacceptable effect on power or thrust or in other unsafe conditions. Because of the nature and

## DRAFT

complexity of systems containing digital logic, the software and the PLDs must be developed using a structured development approach, commensurate with the hazard associated with failure or malfunction of the system in which the digital logic is contained.

(b) Applicants may not be able to establish with certainty that the software and/or the PLD has been designed without errors. However, if the applicant uses the software level and/or the hardware design assurance level appropriate for the criticality of the performed functions and uses an approved development method, the software and/or the PLD satisfies the requirement to minimize errors. In multiple engine installations, the possibility of digital logic errors common to more than one engine control system may determine the criticality level of the software and the hardware design assurance level.

(2) Approved Methods. The primary FAA guidance on software methods is found in AC 20-115B and in Order Number 8110.49. Acceptable methods for developing software comply with the guidelines of documents RTCA DO-178B/EUROCAE ED-12B, hereafter referred to as DO-178B. Alternative methods for developing software may be proposed by the applicant and are subject to approval by the Administrator.

### (3) Level of Software.

(a) In multiple engine installations, the design, implementation and verification of software in accordance with Level A (DO-178B) is normally needed to achieve the certification objectives for aircraft to be type certificated under part 25, part 27-Category A, and part 29-Category A.

(b) The criticality of functions on other aircraft may be different, and, therefore, a different level of software design assurance may be acceptable. For example, in the case of a reciprocating engine in a single engine aircraft, level C (DO-178B) software has been found to be acceptable.

(c) Determination of the appropriate software level may depend on the failure modes and consequences of those failures. For example, it is possible that failures resulting in significant thrust or power increases or oscillations may be more severe than an engine shutdown, and, therefore, these failures must be considered when selecting a given software level.

(d) Applicants may protect or partition non-critical software from critical software and design and implement the non-critical software to a lower level as defined by the RTCA guidelines. The applicant must demonstrate the adequacy of the partitioning method as well as the protection and isolation features needed to prevent corruption between the two levels of software. This demonstration should consider whether the protected/partitioned lower software levels are appropriate for any anticipated installations. Should the criticality level be higher in subsequent installations, the applicant would need to meet all requirements for the higher software level.

### (4) Legacy Software.

DRAFT

DRAFT

(a) Software developed using DO 178 or DO-178A is referred to as legacy software. In general, changes made to legacy software applicable to its original installation are assured in the same manner as the original certification. When legacy software is used in a new aircraft installation that requires DO-178B, the original approval of the legacy software is still valid assuming equivalence to the required software level can be ascertained. In this manner, legacy software can be used in the new installation that requires DO-178B software.

(b) If the software level of the legacy system cannot be shown to be equivalent or better than that required by the product installation being considered, then an applicant must upgrade the software per RTCA/DO-178B, Section 12.1.4, "Upgrading a Development Baseline." This may necessitate a complete reevaluation to demonstrate assurance to the appropriate objectives of RTCA/DO-178B. Additional information on this subject can be found in FAA Order 8110.49 titled "Software Approval Guidelines." See particularly Chapter 10, "Approval Of Software Changes In Legacy Systems Using RTCA/DO-178B."

(5) On-Board or Field Software Loading and Part Number Marking. Use the following guidelines when on-board or field loading of electronic engine control software and associated Electronic Part Marking (EPM) is implemented:

(a) For software changes, document the software to be loaded by an approved design change and released with a service bulletin.

(b) For an EECS unit with separate part numbers for hardware and software, the software part number(s) need not be displayed on the unit as long as they are embedded in the loaded software and can be verified by electronic means. When new software is loaded into the unit, the same verification requirement applies and the proper software part number must be verified before the unit is returned to service.

(c) For an EECS unit with only one part number, the single part number represents a combination of a software and hardware build. Applicants should change or update the unit part number on the nameplate when the new software is loaded. The software build or version number must be verified before the unit is returned to service.

(d) The configuration control system for an EECS that will be onboard/field loaded and the use of EPM must be approved. The drawing system must provide a compatibility table that tabulates the combinations of hardware part numbers and software versions that have been approved by the Administrator. The top-level compatibility table must be under configuration control, and it must be updated for each change that affects hardware/software combinations. The applicable service bulletin must define the hardware configurations with which the new software version is compatible.

(e) The loading system must be in compliance with the guidelines of DO-178B. If the applicant proposes more than one source for loading, (for example, diskette or mass storage), all sources must comply with these guidelines.

DRAFT

DRAFT

(f) The service bulletin must require verification that the correct software version has been loaded after installation on the aircraft.

(6) Software Change Category. The processes and methods used to change software must not affect the design assurance level of that software.

(a) The determination of major versus minor is established in § 21.93. A change to the software in an engine control system may affect the reliability, operational characteristics, or other characteristics affecting the airworthiness of the product. Paragraphs (b) and (c) below provide appropriate guidance in these instances.

(b) The failure effect of FADEC software is always major because an error could result in the total loss of thrust. Therefore, software changes are almost always classified as major. Exceptions are decided on a case-by-case basis. Therefore, a change to software produced in accordance with the guidelines of RTCA DO-178B should be classified as major if any of the following applies and the failure effect is catastrophic, hazardous or major:

1 The executable code for software, determined to be Level A or B in accordance with the guidelines, is changed, unless that change involves only a variation of a parameter value within a range already verified for the previous certification standard;

2 The software is upgraded to, or downgraded from, Level A, B or C; or

3 The executable code, determined to be Level C, is deeply changed, for example, after a software reengineering process accompanying a change of processor.

(c) For software developed to guidelines other than DO-178B, the applicant should assess changes in accordance with the system principles. For systems assessed under § xx.1309, the classification process is based on the functional aspects of the change and its potential effects on safety. The following guidance applies:

1 When the failure effect at the aircraft level is “catastrophic” or “hazardous,” the change must be classified as major.

2 When the failure effect at the aircraft level is 'major', the change must be classified as major if:

- aspects of the compliance demonstration use means that have not been previously accepted for the nature of the change to the system;
- the change affects the pilot/system interface (displays, controls, approved procedures); or
- the change introduces new types of functions/systems.

(7) Software Changes by Others than the TC Holder.

DRAFT

(a) Software changes by someone other than the original TC holder are generally not feasible. The applicant must address the approval process with the certification authority to determine feasibility.

(b) Two types of software changes exist that could be implemented by someone other than the original TC holder:

- option-selectable software, or
- user-modifiable software (UMS).

1 Option-selectable changes are pre-certified logic that use a method of selection shown not to be capable of causing a control malfunction.

2 UMS is software intended for modification by the aircraft operator without review by the certification authority, the aircraft applicant, or the equipment vendor. For engine control systems, UMS has generally not been applicable. However, approval of UMS, if required, would be addressed on a case-by-case basis.

(c) The necessary guidance for UMS is contained in DO-178B, paragraph 2.4. The guidance allows non-TC holders to modify the software within the modification constraints defined by the TC holder if the system has been certified with the provision for software user modifications. To certify an EECS with the provision for software modification by a non-TC holder, the TC holder must (1) provide the necessary information for approval of the design and implementation of a software change; and (2) demonstrate that the necessary precautions have been taken to prevent the user modification, regardless of whether it is implemented correctly, from affecting engine airworthiness.

(d) When the software is changed in a manner not allowed by the TC holder as “user modifiable,” the non-TC holder applicant must comply with the requirements in part 21, subpart E. See FAA Order 8110.49, “Software Approval Guidelines,” particularly Chapter 7, “Approval of Airborne Systems and Equipment Containing User-Modifiable Software (UMS)” for additional information.

15. Section 33.28(h) – Aircraft-Supplied Data.

a. Rule Text. Section 33.28(h) reads: “Aircraft-supplied data. Single failures leading to loss, interruption or corruption of aircraft-supplied data (other than thrust or power command signals from the aircraft), or data shared between engines must:

(1) not result in a hazardous engine effect for any engine; and

(2) be detected and accommodated. The accommodation strategy must not result in an unacceptable change in thrust or power or an unacceptable change in engine operating and starting characteristics. The applicant must evaluate and document the effects of these failures on engine power or thrust, engine operability, and starting characteristics throughout the flight envelope.”

b. Guidance: Aircraft-Supplied Data.

(1) Objective. As required by § 33.28(h), in the case of loss, interruption, or corruption of aircraft-supplied data, the engine must 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 regulations of §§ 33.65 and 33.89, as appropriate.

(2) Background.

(a) Previous regulatory practice was to preserve the independence of the engine from the aircraft. Hence, even with very reliable architecture, such as triply redundant air data computer (ADC) systems, the engine control system was required to provide an independent control means that could be used to safely fly the aircraft should all the ADC signals be lost.

(b) With the increased engine-aircraft integration currently occurring in the aviation industry, and with the improvement in reliability and implementation of aircraft-supplied data, the new requirement is that fault accommodation be provided against single failures of aircraft-supplied data. This single failure requirement applies to all dispatchable configurations of the engine control aircraft air data systems.

(c) Elements of the engine control system, such as a throttle position resolver, may be mounted in the aircraft and not part of the engine type design but dedicated to the engine control system and powered by it. Such elements are an integral component of the EECS and are not considered aircraft data.

(3) Design Assessment.

(a) A number of tools and techniques, for example, a Fault Accommodation chart and Markov Modeling, are used to assess and to shape the design of the engine control system and its interface with the aircraft data systems. The FAA recommends that applicants prepare a Fault Accommodation chart that defines the fault accommodation architecture for the aircraft-supplied data.

(b) When the particular failure modes of the aircraft air data are unknown, the typical failure modes of loss of data and erroneous data should be assumed. The term “erroneous data” is used herein to describe a condition where the data appears to be valid but is incorrect. The engine applicant must provide such assumptions and the results of the evaluation of the impact of erroneous aircraft data to the installer.

(c) If the engine and/or the aircraft applicant intends to show that complete loss of the aircraft air data system itself is extremely improbable, and if the engine control system relies entirely on aircraft air data to complete any of its critical control functions, then the applicant must show that the aircraft air data system is unaffected by a complete loss of aircraft generated power (for example, the air data system is backed up by battery power). In addition, the aircraft

## DRAFT

air data system must be shown to have no common mode faults that would cause it to transmit multiple incorrect, but valid, signals.

(d) The engine control system's LOTC/LOPC analysis must contain the effects of air data system failures in all allowable engine control system and air data system dispatch configurations.

(e) Failures in the throttle position sensing system and thrust command system must be included in the engine's LOTC/LOPC analysis. Although these systems are mounted in the aircraft and are not part of the engine type design, they are dedicated to the engine control system and powered by it. They are considered to be an integral component of the EECS.

(f) When aircraft-supplied data can affect engine control system operation, the applicant must address the effects of faulty and corrupted aircraft-supplied data on the EECS, as applicable, in the SSA or other appropriate documents.

(4) Accommodation Techniques. The following are examples of possible means of accommodation:

(a) Provision of an alternate mode that is independent of aircraft-supplied data.

(b) Dual sources of aircraft-supplied sensor data with local engine sensors provided as voters and alternate data sources.

(c) Use of synthesized engine parameters to control or act as voters. When synthesized parameters are used for control or voting purposes, the analysis should consider the impact of temperature and other environmental effects on sensors whose data are used in the synthesis. The variability of any data or information necessary to correlate the data from the sensors used in the synthesis to the parameters being synthesized should also be assessed.

(d) Triple redundant ADC systems that provide the required data.

(5) Effects on the Engine.

(a) Section 33.75 defines the hazardous engine effects for turbine engines.

(b) Section 33.28(h) addresses the effects of aircraft signals, such as aircraft air data information, or other signals that could be common to all engine control systems in a multi-engine installation. The control system design must ensure that the full-up system is capable of providing the declared minimum rated thrust or power throughout the engine operating envelope.

(c) Section 33.28(h) requires the applicant to provide an analysis of the effect of loss or corruption of aircraft data on engine thrust or power. The effects of failures in aircraft-supplied data must be documented in the SSA as described in paragraph 12 (Section 32.28(e) – System Safety Assessment). When appropriate, aircraft data failures or malfunctions that contribute to LOTC/LOPC events must be included in the LOTC/LOPC analysis.

DRAFT

DRAFT

(6) Validation.

(a) Functionality of the fault accommodation logic must be demonstrated by test, analysis, or a combination thereof. When the aircraft air data system is not functional because of the loss of all aircraft generated power, the engine control system must include validated fault accommodation logic that allows the engine to operate acceptably with the loss of all aircraft-supplied air data. Engine operation in this system configuration must be demonstrated by test.

(b) For all dispatchable control modes, the next single fault in the EECS must be shown not to lead to a hazardous engine effect.

(c) If an alternate mode, independent of aircraft-supplied data, has been provided to accommodate the loss of all data, the applicant should conduct sufficient testing to demonstrate that the operability regulations have been met when operating in this mode. Characteristics of operation in this mode must be included in the engine installation and operating instructions, as appropriate. This alternate mode need not be dispatchable.

(7) Installation Requirements.

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

(b) The engine applicant must state in the engine installation instructions that the aircraft applicant is responsible for ensuring 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.

(c) The engine applicant must supply the effects of faulty and corrupted aircraft-supplied data on the EECS in the engine installation instructions.

(d) The engine installation instructions must state that the installer should ensure that those sensors and equipment involved in delivering information to the EECS are capable of operating in “severe” EMI, HIRF and lightning environments, as defined in the certification basis for the aircraft, without affecting their proper and continued operation.

(e) The applicant must state the reliability level for the aircraft-supplied data that was used as part of the SSA and LOTC/LOPC analysis as the “assumed value” in the engine installation instructions.

(f) As stated in § 33.28(h), thrust and power command signals sent from the aircraft are not subject to the regulations of § 33.28(h)(2). If the aircraft thrust or power command system is configured to move the engine thrust or power levers or transmit an electronic signal to command a thrust or power change, the engine control system merely responds to the command and changes engine thrust or power as appropriate. The engine control

DRAFT

system may have no way of knowing that the sensed throttle or power lever movement was correct or erroneous.

(g) In both the moving and non-moving throttle (or power lever) configurations, the installer must show that a proper functional hazard analysis is performed on the aircraft system involved in generating engine thrust or power commands and that the system meets the appropriate aircraft's functional hazard assessment safety related regulations. This task is an aircraft certification issue. However, failures in the throttle position sensing system and thrust command system must be included in the engine's LOTC/LOPC analysis.

(h) Any assumptions made during the design assessment regarding the reliability or configuration of the aircraft systems and the results of the evaluation of erroneous aircraft data must be documented in the engine installation instructions.

16. Section 33.28(i) – Aircraft-Supplied Electrical Power.

a. Rule Text. Section 33.28(i) reads: “Aircraft-supplied electrical power.

(1) The applicant must design the engine control system so that the loss, malfunction, or interruption of electrical power supplied from the aircraft to the engine control system will not result in any of the following:

(i) a hazardous engine effect, or

(ii) the unacceptable transmission of erroneous data.

(2) When an engine dedicated power source is required for compliance with § 33.28(i)(1), its capacity should provide sufficient margin to account for engine operation below idle where the engine control system is designed and expected to recover engine operation automatically.

(3) The applicant must identify and declare the need for, and the characteristics of, any electrical power supplied from the aircraft to the engine control system for starting and operating the engine, including transient and steady state voltage limits, in the engine installation instructions.

(4) Low voltage transients outside the power supply voltage limitations declared in § 33.28(i)(3) must meet the requirements of § 33.28(i)(1). The engine control system must be capable of resuming normal operation when aircraft-supplied power returns to within the declared limits.”

b. Guidance: Aircraft-Supplied Electrical Power.

(1) Objective. The objective is to provide an electrical power source to the EECS that is single fault tolerant (including common cause/mode). The most common means of achieving

## DRAFT

this objective has been to provide an engine-mounted alternator as the electrical power source for the EECS.

### (2) Electrical power sources.

(a) An “engine dedicated power source” is usually provided by an alternator(s), mechanically driven by the engine or the transmission system of rotorcraft. With the increased integration of engine-aircraft systems and with the application of EECS to small engines, both reciprocating and turbine, an engine-mounted alternator may not necessarily be the only design approach to meeting this objective.

(b) Batteries are not considered an aircraft-supplied power source, except in the case of reciprocating engines. For reciprocating engines, a battery source dedicated solely to the engine control system may be accepted as an engine dedicated power source. In such applications, the applicant must provide appropriate information including, for example, health status and maintenance requirements for the dedicated battery system, to the installer.

### (3) Design Architecture Analysis

(a) The applicant’s analysis of the engine ECS design architecture must identify all requirements for engine-dedicated and aircraft-supplied power sources. The analysis must also include the sources of power and the effects of losing these sources. If the engine depends on aircraft-supplied power for any operational functions, the analysis must define the aircraft-supplied power requirements. The following configurations have been used in previously certified configurations:

- EECS independent of aircraft-supplied power (engine dedicated power source)
- Aircraft-supplied power directly used for engine functions, independent from the EECS
- Use of aircraft-supplied power for functions switched by the EECS
- Use of aircraft-supplied power to back up the engine dedicated power source
- EECS dependent on aircraft-supplied power

(b) Any engine dedicated power source must provide sufficient power to the ECS to continue functioning during any anticipated engine recovery event. The autonomy of the ECS must be sufficient to ensure its functioning in the case of immediate automatic relight after unintended shutdown if autolight is an intended function of the control system. Conversely, ECS autonomy during restart when windmilling is not always required. The applicant must also ensure that the design accounts for any anticipated variations in power output, such as those due to temperature variations, manufacturing tolerances and idle speed variations. The FAA also recommends that the applicant show by test and/or analysis that the design margin accounts for any deterioration over the life of the engine.

### (4) Aircraft-Supplied Power Reliability.

## DRAFT

(a) Any aircraft-supplied power reliability values used in system analyses, whether supplied by the aircraft manufacturer or assumed, must be included in the engine installation instructions.

(b) When aircraft-supplied power is used in any architecture, if aircraft power faults or failures can contribute to LOTC/LOPC or hazardous engine effects, these events must be included in the engine SSA and LOTC/LOPC analyses.

(c) When compliance with § 33.28(i)(1) imposes an engine dedicated power source, the LOTC/LOPC analysis must address failure of this source. While it is not normally necessary to give credit in the LOTC/LOPC analysis for the use of aircraft-supplied power as a back-up power source, aircraft-supplied power has typically been provided to accommodate the loss of the engine dedicated power source. However, LOTC/LOPC allowance and any impact on the SSA for the use of aircraft-supplied power as the sole power source for an engine control back-up system or as a back-up power source would be reviewed on a case-by-case basis. If the engine control can operate in the presence of aircraft power bus transfers, then the FAA may give credit for the use of aircraft power as a backup.

(d) In some system architectures, an engine dedicated power source may not be required and aircraft-supplied power may be acceptable as the sole source of power. Two examples are:

1 A system that consists of a primary electronic single channel and a full capability hydromechanical back-up system that is independent of electrical power. A full capability hydromechanical control system meets all part 33 regulations and is not dependent on aircraft power. In this architecture, a loss or interruption of aircraft-supplied power is accommodated by transferring control to the hydromechanical system. Transition from the electronic to the hydromechanical control system is addressed under § 33.28 (c).

2 An EECS powered by an aircraft power system that could support a critical fly-by-wire flight control system. Such a power system may be acceptable as the sole source of power for an EECS. In this example, the engine installation instructions must state that a detailed design review and safety analysis must be conducted to identify latent failures and common cause failures that could result in the loss of all electrical power. The instructions must also state that any emergency power sources must be known to be operational at the beginning of the flight. Any emergency power sources must be isolated from the normal electrical power system so that the emergency power system will be available no matter what happens to the normal generated power system. If batteries are the emergency power source, the applicant must show that the flight crew has a means of determining their condition prior to flight, and that their capacity is sufficient to ensure exhaustion will not occur before getting the airplane back on the ground. This will ensure that appropriate reliability assumptions are provided to the installer.

### (5) Aircraft-Supplied Power Quality.

(a) When aircraft electrical power is necessary for operation of the engine control system, § 33.28(i)(3) specifies that the engine installation instructions contain the engine control

DRAFT

## DRAFT

system's electrical power supply quality requirements. This applies to any of the configurations listed above or to any new configurations or novel approaches not listed that use aircraft-supplied power. These quality requirements must include steady state and transient under-voltage and over-voltage limits for the equipment. The power input standards of RTCA DO-160/EUROCAE ED-14 provide an acceptable definition of such requirements. If RTCA DO-160/EUROCAE ED-14 is used, any exceptions to the power quality standards cited for the particular category of equipment specified must be stated.

(b) We recognize that the electrical or electronic components of the ECS, when operated on aircraft-supplied power, may cease to operate during some low voltage aircraft power supply conditions beyond those required to sustain normal operation. However, operation of the engine control must never result in a hazardous engine effect. Further, low voltage transients outside the control system's declared capability must not cause permanent ECS loss of function, result in inappropriate system operation, cause the engine to exceed any operational limits, or cause the transmission of unacceptable erroneous data.

### (6) Power Recovery.

(a) When aircraft power recovers from a low-voltage condition to a condition within which the ECS is expected to operate normally, the ECS must resume normal operation. The engine instructions for installation must include the time interval associated with this recovery. We recognize that aircraft power supply conditions may lead to engine shutdown or an engine condition that is not automatically recoverable. In these cases, the engine should be capable of being restarted. Also, any special flight crew procedures for executing an engine restart during such conditions must be contained in the engine operating instructions. The FAA will determine the acceptability of any non-recoverable engine operating conditions that result from these aircraft power supply conditions at aircraft certification.

(b) If battery power is required to meet an "all engine out" restart requirement, the applicant must provide a definition of those power requirements. During certain operations, such as low engine speed, in-flight re-starting conditions, the aircraft electrical power may be used to operate the ECS. The applicant must consider the effects of any aircraft electrical bus-switching transients or power transients. These transients are associated with application of electrical loads that could cause an interruption in voltage or a decay in voltage level below that required for proper control functioning.

### (7) Effects on the Engine.

(a) When loss of aircraft power results in a change in engine control mode, the control mode transition must meet the requirements of § 33.28(c).

(b) For some engine control functions that rely exclusively upon aircraft-supplied electrical power, the loss of electrical power may still be acceptable. Acceptability is based on evaluation of the change in engine operating characteristics, current experience with similar designs, or the accommodation designed into the control system.

DRAFT

DRAFT

(c) Examples of engine control functions that have traditionally relied on aircraft power include:

- Engine start and ignition
- Thrust reverser deployment
- Anti-icing (engine probe heat)
- Fuel shut-off
- Over-speed protection systems; and
- Non-critical functions that are primarily performance enhancement functions that, if inoperative, do not affect the safe operation of the engine.

(8) Validation. The applicant must demonstrate the effects of loss of aircraft-supplied electrical power by engine test, system validation test, bench test, or combination thereof.

(9) Installation Requirements. The engine installation instructions must include the assumed quality and reliability levels of aircraft power.

17. Section 33.28(j) – Air Pressure Signal.

a. Rule Text. Section 33.28(j) reads: “Air Pressure Signal. The applicant must consider the effects of blockage or leakage of the signal lines on the engine control system as part of the system safety assessment of § 33.28(e) and must adopt the appropriate design precautions.”

b. Guidance: Air Pressure Signal. Section 33.28(j) covers ingress of foreign matter (for example, sand, dust, water, or insects) which could result in blockage of the lines and adversely affect engine operation. Experience has shown that lines used for measuring the static pressure in the compressor of turbine engines can be blocked by frozen water, leading to a loss of power. The applicant should, therefore, take precautions, such as:

- use of protected openings,
- filters,
- drains for water,
- effective geometry of plumbing to aid in draining,
- appropriate bleed/drain hole sizing,
- heating the lines to prevent freezing of condensed water, and
- corrosion resistant features.

18. Section 33.28(k) – Automatic Availability and Control of Engine Power for a 30-Second OEI Rating.

a. Rule Text. Section 33.28(k) reads: “Automatic availability and control of engine power for 30-second OEI rating. Rotorcraft engines having a 30-second OEI rating must incorporate means, or a provision for a means, for automatic availability and automatic control of the 30-second OEI power within its operating limitations.”

DRAFT

b. Guidance: Automatic Availability and Control of Engine Power for 30-second OEI Rating. Using this rating during flight may create a high pilot workload. Therefore, the rating must be applied and controlled automatically, other than to terminate it. Until terminated, the software will automatically prevent the engine from exceeding its limits, specified in the engine's TCDS and associated with this rating. Because the 30-second OEI rating may use almost all the available margin in the engine design, exceeding the rating limits would likely result in engine failure.

(1) The required automatic control of the 30-second OEI power should eliminate the need to monitor engine parameters, such as output shaft torque or power, output shaft speed, gas generator speed, and gas path temperatures. The requirement for automatic control is intended to free up the pilot to focus on his primary responsibility of flying the aircraft. Such means for automatic control within the operating limitations must be effective during normal and abnormal operations.

(2) When selected, the means required by § 33.28(k) must automatically govern the engine to its 30-second OEI power rating. The applicant must provide information on methods to ensure that engine limiter settings would not prevent the engine from reaching the 30-second OEI power which must be automatically available in compliance with § 33.28 (k). These limiter settings may include engine speed, measured gas temperature and fuel flow. Particular attention should be given to take-off conditions with a cold-soaked engine.

19. Section 33.28(1) – Engine Shut Down Means.

a. Rule Text. Section 33.28(1) reads: “Engine Shut Down Means. Means must be provided for shutting down the engine rapidly.”

b. Guidance: Engine Shut Down Means. A means for shutting the engine down rapidly must be provided.

(1) Usually this is provided by a fuel shut-off valve included as part of the fuel metering system in the engine control. Normally, the SOV is activated by the pilot through a switch or lever.

(2) In some applications, we have accepted that the SOV is not provided as part of the engine control. However, in these cases, the applicant must demonstrate that the means for the pilot to activate the SOV is readily available and that the engine shut down can be accomplished in an acceptable, safe time frame.

(a) Rapid engine shut down is usually accomplished via a fuel shut-off valve, included as part of the fuel metering system in the ECS. Normally, the pilot through a switch or lever activates the valve. In some applications, we have accepted that the valve is not provided as part of the ECS. When it is not, you must show that the pilot can readily activate the fuel shut off valve and that engine shut down occurs in an acceptable, safe time frame.

DRAFT

(b) If the fuel shut-off valve is to be supplied by the installer to comply with § 33.28(l), the applicant must define the valve specifications in the engine installation instructions. For example, the valve may have reliability, response, environmental, fire or other requirements.

20. Section 33.28(m) - Programmable Logic Devices (PLDs).

a. Rule Text. Section 33.28(m) reads: “Programmable logic devices. The development of programmable logic devices using digital logic or other complex design technologies must provide a level of assurance for the encoded logic, which is commensurate with the hazard associated with the failure or malfunction of the systems in which the devices are located. The applicant must design, implement, and verify all associated logic to minimize the existence of errors by using a method, approved by the FAA, that is consistent with the criticality of the performed function.”

b. Guidance: Programmable Logic Devices.

(1) Objective.

(a) For engine control systems that use embedded software and/or complex electronic hardware in the form of programmable logic devices, the objective of §§ 33.28(g) and (m) is to prevent logic errors that would result in an unacceptable effect on power or thrust or other unsafe conditions. Because of the nature and complexity of systems containing digital logic, the applicant must develop software and PLDs using a structured development approach, commensurate with the hazard associated with failure or malfunction of the system in which the digital logic is contained.

(b) The applicant may not be able to establish that the software and/or the PLD has been designed without errors. However, if the applicant uses the software level and/or the hardware design assurance level appropriate for the criticality of the performed functions and an approved development method, the software and/or the PLD may satisfy the FAA requirement to minimize errors. In multiple engine installations, the possibility of digital logic errors common to more than one engine control system may determine the criticality of the software/hardware design assurance level.

(2) Approved Methods.

(a) The primary FAA guidance on PLD methods is found in AC 20-152. Methods for developing PLDs, compliant with the guidelines of document RTCA DO-254/EUROCAE ED-80, hereafter referred to as DO-254, are acceptable. Alternative methods for developing PLDs may be proposed by the applicant and are subject to approval by the Administrator.

(b) The applicant may use service experience to show regulatory compliance for off-the-shelf or modified equipment. In that case, we recommend the applicant show that the worst case failure or malfunction of the device in the new installation is no more severe than the failure modes of the original design. The applicant should also compare service history

## DRAFT

regarding operational environment, installation, and aircraft category with its anticipated installation.

### (3) Level of hardware design assurance.

(a) Determining the appropriate hardware design assurance level depends on failure modes and consequences of those failures. For example, failures resulting in significant thrust or power increases or oscillations may be more severe than an engine shutdown. Therefore, the applicant should consider the possibility of these types of failures when selecting a given hardware design assurance level.

(b) In multiple engine installations, the design, implementation and verification of the PLD in accordance with Level A (DO-254) is normally needed to achieve the certification objectives for aircraft to be type certificated under part 25, part 27-Category A, and part 29-Category A.

(c) The criticality of functions on other aircraft may be different, and therefore, a different level of hardware design assurance may be acceptable. For example, in the case of a reciprocating engine in a single engine aircraft, level C (DO-254) hardware design assurance has been found acceptable.

(d) If the criticality level is higher in subsequent installations, the applicant must meet all the requirements for the higher hardware design assurance level.

## 21. Other Considerations: Engine, Propeller and Aircraft Systems Integration and Relations Between Engine, Propeller and Aircraft Certification Activities.

### a. Aircraft or Propeller Functions Integrated into the Engine Control System.

(1) This involves the integration of aircraft or propeller functions (i.e., those that have traditionally not been considered engine control functions) into the Electronic Engine Control System's hardware and software.

(2) Examples include thrust reverser control systems, propeller speed governors, which govern speed by varying pitch, and ATTCS. When this type of integration is pursued, the installer should include the EECS as part of the aircraft's SSA. Although the aircraft functions incorporated into the EECS may be reviewed at engine certification, the acceptability of the safety analysis involving these functions will be determined at aircraft certification.

(3) The EECS may be configured to contain part or all of the aircraft system's functionality. Thrust reverser control systems are an example of including only part of the functionality in the EECS. In those control systems, the aircraft is configured with separate switches and logic (i.e., independent from the EECS) 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 EECS.

## DRAFT

(4) One example of configuring the ECS to contain all of an aircraft systems functionality is configuring an ECS to fully govern propeller speed in turboprop aircraft. Here, the ECS logic must be configured to feather a propeller on an engine that fails. Failure of the prop to feather may result in excessive drag, which could be critical. Another example is an ATTCS in turbofan aircraft. If an engine fails during takeoff, the system will increase the thrust of the remaining engine(s). Both examples indicate that the criticality is not limited, since ECS failure could result in loss of aircraft. Both examples involve aircraft functionality that would receive significant review during aircraft certification.

(5) This combination of control system elements and logic relies totally on the ECS to perform flawlessly. When functions like these are integrated into the ECS so that they render an ECS critical, we recommend you take special attention to ensure that no single failure (including common cause/mode) could cause the critical failure condition. For example, exposing the EECS to overheat should not cause both an engine shutdown and failure of the propeller to feather.

### b. Integration of Engine Control Functions into Aircraft Systems.

(1) The trend toward systems integration may lead to aircraft systems performing functions traditionally considered part of the engine control system. Some designs may use aircraft systems to implement a significant number of the engine control system functions. An example is the complex integrated flight and engine control systems—integrated in aircraft avionics units—which govern engine speed, rotor speed, rotor pitch angle, and rotor tilt angle in tilt-rotor aircraft.

(2) In these designs, aircraft systems may be required to be used during engine certification. In such cases, the engine applicant is responsible for specifying the requirements for the EECS in the engine installation instructions and for substantiating the adequacy of those requirements. An example of limited integration is an engine control which 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. In this case, the EECS, which is part of the type design, provides all the functionality required to safely operate the engine in accordance with part 33 or other applicable specifications.

### c. Certification Activities.

(1) Objective. To satisfy aircraft requirements, such as §§ 25.901, 25.903 and 25.1309, the applicant must analyze the consequences of engine control system failures on the aircraft. Together with the aircraft applicant, the engine applicant must ensure that the software levels and safety and reliability objectives for the engine control system are consistent with these aircraft requirements.

#### (2) Interface Definition and System Responsibilities.

(a) The FAA recommends that the applicant identify system responsibilities as well as interface definitions for the functional and hardware and software aspects between the engine, propeller, and aircraft systems in the appropriate documents.

## DRAFT

(b) The engine/propeller/aircraft documents should include:

- Functional requirements and criticality (which may be based on engine, propeller and aircraft considerations)
- Fault accommodation strategies
- Maintenance strategies
- The software level (per function if necessary)
- The reliability objectives for:
  - LOTC/LOPC events
  - Transmission of faulty parameters
- The environmental requirements including the degree of protection against lightning or other electromagnetic effects (for example, level of induced voltages that can be supported at the interfaces)
- Engine, propeller, and aircraft interface data and characteristics
- Aircraft power supply requirements and characteristics (if relevant).

(3) Distribution of Compliance Tasks.

(a) Engine, propeller, and aircraft applicants may share the tasks for the certification of the aircraft propulsion system equipped with EECSs. The distribution of these tasks between applicants should be identified and agreed upon with the appropriate engine, propeller and aircraft authorities.

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

(c) The engine certification addresses the functional aspects of the engine control system in compliance with the applicable engine requirements.

(d) Appropriate evidence provided for engine certification should also be used for aircraft certification. For example, the quality of any aircraft function software and aircraft/engine interface logic already demonstrated for engine certification would not need additional substantiation for aircraft certification.

(e) Two examples illustrate this principle.

- Case of an EECS controlling the engine and propeller:

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

2 The engine certification would address the functional aspects for the engine functions (for example, safety analysis, rate for LOTC/LOPC events, and effect of loss of

## DRAFT

aircraft-supplied data). The fault accommodation logic affecting the control of the engine will be reviewed at that time.

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

4 In this example, the propeller functions and characteristics that the propeller applicant defines that are to be provided by the engine control system would normally need to be refined by flight test. The propeller applicant should ensure that these functions and characteristics—provided for use during the engine certification program—define an airworthy propeller configuration, even if they have not yet been refined by flight test.

5 With regard to changes in design, all parties should agree so that changes to the engine control system that affect the propeller system, or vice versa, do not lead to any inadvertent effects on the other system.

- Case of an aircraft computer performing the functions for the control of the engine:

6 The aircraft certification will address all general requirements, such as software quality assurance procedures, EMI, HIRF, and lightning protection levels, and functional aspects for the aircraft functions.

7 The engine certification will address the functional aspects for the engine functions (for example, safety analysis, rate for LOTC/LOPC events, and effect of loss of aircraft-supplied data). The fault accommodation logic affecting the control of the engine will be reviewed at that time.