U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: Guidance Material For 14 CFR § 33.28, Engine Control Systems

Date: 5/23/14 **AC No:** 33.28-3

Initiated by: ANE-111

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) at amendment level 33-26.

Colleen M. D'Alessandro

Colleen M. D'Alessandro
Assistant Manager, Engine and Propeller Directorate,
Aircraft Certification Service

Contents

Appendices

CHAPTER 1. SECTION 33.28 - GENERAL.

1-1. Purpose. Section 33.28 regulates the general design and functioning of the ECS. It does not replace or supersede other regulations governing individual ECS components. Those components, such as alternators, sensors, and actuators, are also regulated under other part 33 sections, such as § 33.67 or 33.35 for the fuel system and § 33.91 or 33.53 for individual component tests.

1-2. Applicability. The guidance provided in this document is directed to engine manufacturers, modifiers, or Federal Aviation Administration (FAA) designated engineering representatives. This guidance should also assist the engine installer in understanding the differences between certification of the engine and the aircraft, and the assumptions made by the engine manufacturer concerning the engine-to-aircraft interface.

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,” “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.

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

This AC does not apply to conventional magnetos or electrically-powered actuators whose actuation depends on pilot action through a dedicated electric circuit or electrical relays not controlled by the EECS.

The material in this AC does not change, create any additional, authorize changes in, or permit deviations from existing regulatory requirements.

1-3. Related Reading Material. Refer to Appendix 4 for reading material that is related to this AC.

1-4. Definitions. Refer to Appendix 5 for definitions that are used in this AC.

1-5. Overview of this AC. 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.

a. 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 added to the EECS that are not required for compliance with part 33 but are required for installation compliance are documented in the engine installation manual.

b. 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 that may be integrated into the system for control of engine operations, such as bleed air valve control, are also addressed in this AC. The principles outlined in this AC apply to the whole ECS.

c. 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, take special design precautions to minimize any adverse effects from any of the following:

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

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

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

(4) Hidden design faults or discrepancies within the design of the propulsion system (which are typically the result of incomplete or inaccurate requirements), or

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

1-6. 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. Subpart E of parts 23, 25, 27, and 29 provides requirements for the installation of a certificated engine into an aircraft. The installed engine becomes a part of the powerplant system. These regulations require that the powerplant system design meet all the requirements, procedures, limitations, and assumptions specified in the engine installation or operating instructions, the engine type certificate data sheet (TCDS), or the supplemental type certificate (STC).

1-7. Determining if an engine control system (ECS) complies with applicable aircraft certification regulations is done during aircraft certification. As part of the aircraft certification program, the FAA may also require flight-testing to fully evaluate engine performance and operability characteristics for all operating modes (refer to § 939 of 14 CFR parts 23, 25, 27, and

29). However, when the aircraft application is unknown at the time of engine certification, the engine manufacturer should make reasonable installation and operational assumptions for a target application. The engine manufacturer details any installation limitations or operational issues in the engine installation or operating instructions or both, or the TCDS.

1-8. When the applicant knows that aircraft components may contribute to or cause a failure condition that is evaluated in a part 33 safety analysis, the applicant should include the maximum allowable contribution from those aircraft components in both the safety analysis and the installation limitations and instructions. Accounting for these components ensures the engine will be installable.

1-9. Appendix 1 provides applicants with references to the installation or operating instructions or both as an aid in preparing complete installation and operating instructions. The installation or operating instructions or both should include descriptive, interface, and operating data in enough detail to support aircraft certification.

1-10. Limitations specified in the engine installation or operating manuals should be consistent with those stated on the TCDS, amended TCDS, or STC, as applicable. This information is intended to ensure that part 33 certification is not invalidated when the engine is installed on the aircraft. The applicant may also document these limitations in other manuals as long as they are referenced in the installation instructions or operating instructions or both. If the applicant uses reference documents, then the applicant must make them available to the FAA and any potential installer. We recommend that the engine and aircraft manufacturers coordinate implementation of limitations or operational issues or both with the appropriate FAA certification offices.

CHAPTER 2. SECTION 33.28(a) - APPLICABILITY.

2-1. Rule Text. Section 33.28(a) reads:

"(a) *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."

2-2. Guidance: Applicability.

a. Section 33.28 applies to all types of engine control systems, including any of the following ECS types:

(1) Hydromechanical (except for those systems on reciprocating engines that are adequately covered through § 33.35 and § 33.37),

(2) Hydromechanical with a limited authority electronic supervisor,

(3) Single-channel full-authority electronic engine control with hydromechanical backup,

(4) Dual-channel full-authority EEC without backup,

(5) Three-channel full authority EEC (or 2 channels plus a voter), or

(6) Any other ECS combination.

b. 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. Many components, including electronic control units, variable-geometry actuators, cables, wires, sensors, overspeed, over-torque, and over-temperature protection systems, fuel racks, and fuel metering units, are part of the ECS. Some engine monitoring systems are physically or functionally integrated with the ECS. These systems are considered part of the ECS if they:

(1) Perform functions that affect engine safety,

(2) Are used in the context of continued-operation, or

(3) Are used in return-to-service decisions.

For example, low-cycle fatigue counters for engine critical parts, as well as some trend monitors and devices that provide information for maintenance are part of the ECS.

Some components, such as a throttle position transducer, might be mounted in the aircraft and are not part of the engine type design, but they are dedicated to the ECS and powered by it. Such elements are integral components of the ECS.

2-3. **Excluded elements**. Some elements are excluded from the ECS. For example, fuel pumps, even though often engine-mounted and integrated with the fuel metering unit, are not part of the ECS. They are part of the fuel delivery system. Demand-control pumps, however, are, or can be, a fuel controlling or limiting element of the system and are considered part of the ECS. Any other engine overspeed design features that are purely mechanical, such as rotor interference, or fuel cutoff methods through rotor axial movement, are not part of the ECS. For example, overspeed protection via blade shedding is purely mechanical protection, so blade shedding is not part of the ECS.

CHAPTER 3. SECTION 33.28(b)(1) - VALIDATION.

3-1. Rule Text. Section 33.28(b)(1) reads:

"(b) *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;

(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."

3-2. Guidance: Validation.

a. The EECS can only perform its intended function if its software is successfully integrated with the control. Accordingly, the applicant should conduct testing to demonstrate successful integration of the EEC system software and the ECS. The applicant should perform this testing either on a complete engine or on a test rig that simulates the ECS.

b. The applicant may use Aerospace Recommended Practice (ARP) 4754A, *Guidelines/or Development of Civil Aircraft and Systems,* as an acceptable method for establishing a development assurance process. SAE ARP 4754A discusses the development of aircraft and systems taking into account the overall aircraft operating environment and functions. This includes validation of requirements and verification of the design implementation for certification and process assurance. Refer to AC20-174 for further understanding of the applicability of the ARP.

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

d. 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 increasing the power lever settings in the

cockpit, results in the engine thrust or power output increases. The applicant should show that it has a continuous (no discontinuities) positive relationship (no inversions, such that increasing forward throttle movement results in decreasing thrust or power), unless it shows that in special applications, safety is enhanced by deviating from this relationship. Any deviation approved under Part 33 will also have to be approved at the aircraft installation (Part 23/25/27/29) level and therefore close coordination with the engine installer will be required to ensure the acceptability of any deviation granted.

e. For ECSs that have a governing mode for power turbine speed, § 33.28(b)(1)(iii) refers to the ability to manage engine power to maintain power turbine speed within specified limits.

f. Chapter 6 further discusses power and thrust oscillations.

CHAPTER 4. SECTION 33.28(b)(2) – ENVIRONMENTAL LIMITS.

4-1. Rule Text. Section 33.28(b)(2) reads:

"(2) *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."

4-2. Guidance: Environmental conditions include temperature, vibration, humidity, EMI, HIRF and lightning. The environmental condition requirements are addressed under §§ 33.53 and 33.91. Although we do not specify the test limits**,** the conditions the applicant declares should represent environments that engine installers and operators would encounter

a. Environmental test procedures and test limits. AC 21-16G and SAE ARP5757 provide further guidance on showing compliance with §§ 33.53, 33.91, and 33.28. This AC recommends SAE ARP5757 in combination with RTCA/DO-160G for testing, but you may use MIL-STD-810 when the tests are equal to, or more rigorous than, those defined in RTCA/DO-160G. As RTCA/DO-160 is very likely to be revised beyond revision G during the life of this AC, we encourage applicants to coordinate with the certification office before using a more recent revision of RTCA/DO-160. Unlike RTCA/DO-160G, however, we recommend performing a minimum of 10 temperature cycles for temperature variation tests. We also recommend applicants recognize that installers will use AC 20-136B and AC20-158 to show lightning and HIRF compliance, respectively, for the engine installation in the aircraft.

b. Radio frequency (RF) emission test procedures and test limits. The procedures and limits in MIL-STD-461 or RTCA/DO-160G Section 21 are acceptable.

c. HIRF and lightning tests. Aircraft HIRF compliance regulations are found in §§ 23.1308, 25.1317, 27.1317, and 29.1317. FAA guidance on HIRF compliance is found in AC 20-158. Aircraft lightning compliance regulations are found in §§ 23.1306, 25.1316, 27.1316, and 29.1316. FAA guidance on system lightning compliance is found in AC 20-136B.

(1) **Test levels**. Engine and aircraft applicants should select the HIRF and lightning test levels for the ECS. Applicants should select these test levels so that the EECS, when installed, meets aircraft certification regulations. If the applicant wants to claim any credit for HIRF and lightning testing, and if the applicant wants this claim shown on the TCDS or the IOI, the applicant must have successfully completed the ECS HIRF and lightning tests. The engine applicant should use the DO-160 section 20 and 22 categories and waveform sets defined in 4-2d(1)(c) of this AC if HIRF and lightning test levels have not been determined for a specific aircraft engine installation. Hardware or software design changes implemented after initial environmental testing should be evaluated for their effects with respect to electromagnetic compatibility (EMC), HIRF and lightning.

(a) Engine and aircraft manufacturers typically determine HIRF and lightning test levels through lightning transient and HIRF attenuation characterization tests. These tests are typically conducted on the aircraft with engines installed. If the HIRF and lightning test levels for the engine installation on a particular aircraft are not known at engine certification, the engine applicant may use the test levels in paragraphs 4-2d(1)(c) through 4-2d(1)(e) below. The aircraft applicant should confirm the compatibility of the engine test levels and the lightning transient characterization and HIRF attenuation tests with engines installed prior to aircraft certification. If these assumed test levels used for engine certification are not adequate for a particular aircraft installation, the engine applicant may need to conduct additional ECS HIRF and lightning tests or analysis.

(b) The engine installation or operating instructions should specify any wire shields, connectors, or terminations, and any electrical bonding, for HIRF and lightning protection that are required when the engine is installed. The applicant should perform the HIRF and lightning tests with the same shielding and electrical bonding configuration specified in the engine installation or operating instructions.

(c) HIRF minimum levels. The following table identifies the minimum system laboratory HIRF RF susceptibility test standards for EECS:

	RTCA/DO-160G Categories		
	Conducted	Radiated CW & SW Modulation	Radiated Pulse Modulation
Fixed-Wing Airplanes with Turbine Engines	Cat W (150 mA)	Cat W (100 V/m)	Cat D (up to 750 V/m)
Rotorcraft (all engine types)	Cat W (150 mA)	Cat Y (200 V/m)	Cat F (up to 1500 V/m)
Reciprocating Engine Intended for use with Propellers (Note 1)	Cat W (150 mA)	Cat W (100 V/m)	Cat D (up to 750 V/m)
Fuselage-Mounted Turbofan Engine Intended for use on Part23 Airplanes (Note 2)	Cat Y (300 mA)	100 MHz to 400 MHz – Cat G (100 V/m) 400MHz to 18GHz – Cat F (up to 150V/m)	Cat F (up to 1500 V/m)

Note 1: Using these HIRF test levels and the design requirements in paragraph (e) below, reciprocating engines with EECSs intended for use on propeller-driven Part 23 airplanes should be acceptable without further airplane HIRF testing.

Note **2:** Using these HIRF test levels and the design requirements in paragraph (e) below, turbofan engines with EECSs intended to be fuselage-mounted on part 23 airplanes should be acceptable without further HIRF testing.

(d) Lightning levels. The applicant should test the EECS using the minimum levels for system laboratory lightning tests specified in RTCA/DO-160G 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 Category A3J3L3 in RTCA/DO-160G Section 22. The applicant should not use series impedance during the pin injection tests (RTCA/DO-160G Section 22.5.1.h) unless the remote load impedance is in a component included as part of the engine or the remote load impedance is specified in the engine installation instructions.

(e) Alternate lightning levels for reciprocating engines with EECS and intended for use with propellers, or fuselage-mounted turbofan engine intended for use on Part 23 airplanes. Electronic engine control systems for these types of engine installations are normally subject to very high lightning transients when lightning attaches to the propeller or engine inlet. Using the lightning design and test requirements below, reciprocating engines with EECS intended for use on small propeller-driven airplanes or fuselage-mounted turbofan engines intended for use on Part 23 airplanes, should be acceptable for airplane installation without further airplane lightning tests. The reciprocating engine minimum system lightning test levels should be RTCA/DO-160G, Section 22 and Category A3H3L3 for unshielded wire bundles. Lightning commonly strikes the propeller on airplanes with propellers. This results in all lightning current directly conducted on the engine, and a large portion of the current on ECS wiring. Lightning strikes to turbofan engines result in current conducted on the engine cowls and fairings, so typically a smaller portion of the lightning current is conducted on the ECS wiring. The fuselage-mounted turbofan engine minimum system lightning test levels should be RTCA/DO-160G Section 22 and Category B3H3L3 for unshielded wire bundles. These waveform sets includes single-stroke, multiple-stroke, and multiple-burst waveforms in RTCA/DO-160G Section 22. Engine applicants should ensure that the ECS tests, design, and the engine installation or operating instructions required by § 33.28 and § 33.5 meet the following requirements:

1 Lightning test setup. Use the test setup found in RTCA/DO-160G section 22.3. Perform the cable bundle injection test with the all EECS wire bundle shields disconnected. This will ensure that the transients are injected directly onto the wires. Do not use series impedance during the pin injection tests (RTCA/DO-160G Section 22.5.1.h), unless the remote load impedance is in a component included as part of the certified engine or the remote load impedance is specified in the engine installation instructions.

2 Wire bundle shields. Install overbraid shields on all wire bundles between EECS components and from EECS components to the airplane. The shields should cover power and signal wires and their returns, and have low resistance and high-optical coverage. An overbraid shield may enclose an entire wire bundle, or multiple overbraid shields may be used over groups of wires within a bundle. For fuselage-mounted turbofan engines, install additional overbraid shields on each wire bundle where the bundle is routed outside the airplane fuselage to the engine. Each shield must be terminated to each connector. Shield terminations must be very short, preferably using backshells with zero length shield terminations. The connector shells and backshells must provide a very low resistance to the engine components, EECS, and airplane firewall or structure. Features required for electrically bonding the connectors to the airplane

firewall or structure, such as surface preparation, must be specified in the engine installation or operating instructions.

3 Engine bonding jumpers. Include at least three electrical bonding jumpers between the engine and the engine mounting frame. The bonding jumpers must be flat braided wire or flat solid conductors, with at least 16 mm^2 conducting cross section, and less than 30 cm long. Specify the maximum bonding jumper length and minimum conducting cross section in the engine installation manual. Define the maximum allowed resistance between the engine, engine mounting frame, and airframe in the engine installation or operating instructions. Provide a low-resistance conducting path from the engine to the airframe.

4 Electronic engine control systems electrical bonding. Specify the maximum allowed electrical bonding resistance between EECS components and the surface they are mounted on in the engine installation or operating instructions. For example, specify the maximum allowed resistance between the component and the airframe or firewall to which it is attached. Also, include any special features required for this electrical bonding in the engine installation or operating instructions, such as surface preparation and or bonding jumpers.

5 Power and signal returns. You should not use the engine or engine mounting frame for power returns or low-power signal returns.

(2) **Test procedures**. The EECS used for the lightning and HIRF tests should include sensors, actuators, and engine and engine-aircraft interface wire bundles. Use the HIRF and lightning test procedures provided in RTCA/DO-160G/EUROCAE ED-14G Sections 20 and 22. However, the test procedures defined in RTCA/DO-160G/EUROCAE ED-14G Sections 20 and 22 are oriented to equipment tests. Therefore, adapt those test procedures to develop the system level HIRF test, the test the applicant will use to show compliance with §§ 33.53 and 33.91.

(a) Additional guidance on system level HIRF tests may be found in SAE ARP5583A.

(b) SAE ARP5415A and ARP5416A provide guidance on system level lightning tests.

(3) **Open loop and closed loop testing**. Conduct HIRF and lightning tests on the ECS operating in closed loop or open loop control. The closed loop set-up is usually powered to move actuators to close the inner actuating loops. The applicant may use a simplified engine simulation to close the outer engine loop. The applicant should conduct the HIRF and lightning tests with the ECS controlling at the most sensitive operating point, as selected and detailed in the applicant's test plans. The reference to 'the most sensitive operating point' is in relationship to schedule sensitivity. We are suggesting that the set point not be where controlling schedules are on flat portions of the schedules. 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.

(4) **Test considerations**.

(a) If special ECS test software is embedded in the target for EMC, HIRF or

lightning testing, the applicant must ensure that the software was developed and implemented by guidelines defined for software levels of at least Level 2 in DO-178A, Level C in DO-178B, Level C in DO-178C, or equivalent. In some cases, the applicants modify the application code to include the required test code features.

(b) The test must be capable of monitoring both the output drive signals and the input signals.

(c) The applicant must duplicate all anomalies observed on inputs or outputs during open loop testing to enable the test to show compliance with the following pass/fail criteria. The applicant must perform this duplication on the engine simulation to determine whether the resulting power or thrust perturbations comply with the §§ 33.53 and 33.91 test pass/fail criteria.

(5) **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 ECS. The following are adverse effects:

(a) For turbine engines: a change greater than 3% of most sensitive operating point or 1% of take-off power or thrust, whichever is greater, for a period of more than 2 seconds.

(b) For reciprocating engines: a change greater than 10% of power at the operating point for a period of more than 2 seconds.

(c) Transfers to alternate channels, backup systems, or alternate modes.

(d) Component damage. Certain protection components, such as transient suppression diodes, may experience failures that are not detected by post-test automatic test plan (ATP), and must be checked with specific test procedures.

(e) False annunciation to the crew that could cause unnecessary or inappropriate crew action.

(f) Erroneous operation of protection systems, such as over-speed or thrust reverser circuits.

(6) Engine applicants should ensure that the ECS design and the engine installation or operating instructions required by § 33.28 and § 33.5, specify the following protection features:

(a) The engine and EECS are installed in an airplane with engine cowls and a firewall that incorporate electrically conducting materials. The conducting materials may be aluminum, copper, steel or carbon fiber composites, and may include thin metal foil or mesh incorporated into nonconducting composites. The EECS should be installed either under the conducting cowl or on an airframe that uses structure with similar conducting materials.

(b) Required wire shielding and connectors for wire bundles that connect the EECS to airplane systems are specified in the engine installation or operating instructions. The required wire shielding and connectors should be used during the HIRF tests.

(c) Electrical bonding requirements for the engine and EECS are specified in the engine installation or operating instructions.

e. **Maintenance actions**.

(1) Section 33.4 requires that the applicant prepare Instructions for Continued Airworthiness (ICA). Instructions for Continuing Airworthiness generally include a maintenance plan. The applicant should provide a maintenance plan for any protection system that is part of the type design of the ECS, and that is required to meet the qualified levels of EMC, HIRF and lightning. The plan is used to ensure the continued airworthiness for the parts of the installed system supplied by the engine type certificate holder. AC 33.4-3 provides information related to the ICA, aircraft engine HIRF, and lightning protection.

(2) Consider including periodic inspections or tests for required structural shielding, wire shields, connectors, and equipment protection components, in the ICAs. Also consider inspections or tests when the part is exposed. The applicant should also show that the maintenance actions introduced by its plan are effective in maintaining the engine's continued airworthiness.

f. **Time-limited dispatch environmental tests**. Time-Limited Dispatch (TLD) is an optional requirement. If the applicant conducts EMC, HIRF and lightning tests for TLD, we recommend that the testing be done with other tests at certification. Refer to paragraph 7.c. of the Policy Memorandum, PS-ANE100-2001-1993-33.28TLD-R1, for the TLD requirements related to environmental compliance.

CHAPTER 5 - SECTION 33.28(c) – CONTROL TRANSITIONS.

5-1. Rule Text. Section 33.28(c) reads:

"c. *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 backup system, the change occurs so that:

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

(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;

(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."

5-2. Guidance: Control Transitions.

a. General.

(1) In the showing of compliance to § 33.28(c)(1), the applicant should 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.

(2) The applicant should show that all declared dispatchable control modes are capable of performing their intended functions in the environmental conditions, including but not limited to EMI, HIRF and lightning, declared in the engine installation instructions.

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

(4) The above applies to the ECS operating in any dispatchable configuration.

(5) The applicant must show that any limitations on operations in alternate modes are clearly stated in the engine installation and operating instructions.

(6) The applicant should provide in the engine installation and operating instructions a description of the ECS operating in its primary and alternate modes.

(7) The applicant should use analyses, or testing, or both, to show that changing to, and operating in, alternate modes has no unacceptable effect on engine durability or endurance. This should not be interpreted as the need to run multiple §33.87 endurance tests. Short segments of testing in combination with analysis may be sufficient for showing of compliance.

(8) The applicant should demonstrate the durability and reliability of the control system in all modes, primarily through 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 during transition between modes can be used as part of the system validation required under § 33.28(b)(1).

(9) **Engine test considerations**.

(a) The engine certification tests defined in part 33, Subparts D and F, are often performed using only the ECS's primary mode. If the applicant requests approval for dispatch in an alternate mode under TLD, then the applicant must demonstrate that the engine can meet the defined test-success criteria in any alternate mode that is proposed as a dispatchable configuration. If a configuration is to be dispatchable, then that mode should be demonstrated to operate in all foreseeable environmental conditions. This demonstration may use analysis or test and should include capabilities such as operability in rain or hail or bird ingestion.

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

(10) **Availability**. Applicants should demonstrate through testing or monitoring, that any backup mode will be available when needed. The applicant should document in the ICA the minimum frequency of inspection or testing needed to ensure its availability.

b. **Crew training modes**. As part of the System Safety Assessment of 33.28(e), applicants should assess crew training modes. These modes are usually installation, and possibly operator specific and need to be negotiated on a case-by-case basis. For example, one common application of crew training modes is simulation of the 'fail-fixed' mode on a twin-engine rotorcraft. The applicant must describe training modes in the engine installation and operating instructions as appropriate. Also, the applicant must take precautions in the design of the ECS and its crew interfaces to prevent inadvertent entry into any training modes. The applicant must assess crew-training modes, including lockout systems.

c. **Non-dispatchable configurations and modes**.

(1) For control configurations that are not dispatchable, but for which the applicant seeks to take credit in the system LOTC/LOPC analysis (this analysis and the LOTC/LOPC concept are covered in full in Chapter 6 below), specific operating limitations may be acceptable. This means that the system will not be charged with an LOTC/LOPC event when the fault is covered by a backup means that allows the system to continue to function safely. The system,

however, would not be dispatchable in this configuration. Compliance with § 33.28(b)(1) in non-dispatchable configurations does not imply strict compliance with the operability requirements of § 33.65 and § 33.89, if applicants demonstrate that in the intended installation no likely pilot control system inputs will result in engine surge, stall, flameout, or unmanageable delay in power recovery or engine controllability issues. For example, in a twin-engine rotorcraft, a rudimentary backup system may be adequate since frequent and rapid changes in power setting when operating in the backup system may not be necessary. In this example, it is very unlikely that dispatch would be allowed with the engine controlled by this rudimentary backup system.

(2) In addition to these operability considerations, the applicant should consider the following factors in assessing the acceptability of a reduced-capability backup mode:

(a) The installed operating characteristics of the backup mode and the differences from the primary mode.

(b) The likely impact of the backup mode operations on pilot workload, if the aircraft installation is known.

(c) The frequency of transfer from the primary mode to the backup mode (i.e. the reliability of the primary mode). Frequencies of transfer of less than 1 per 20,000 engine flight hours are acceptable.

d. **Control transitions**.

(1) Section 33.28(c) requires that any control transitions that occur as a result of fault accommodation occur in an acceptable manner.

(2) In general, the ECS should transition to alternate modes automatically. However, systems in which pilot action is required to engage the backup mode are also acceptable. For instance, a fault in the primary system may result in a “fail-fixed” fuel flow that requires some action by the pilot to engage the backup system to modulate engine power. When pilot action is required, applicants should ensure that any reliance on a pilot executing a manual transition does not pose an unacceptable operating characteristic, unacceptable crew workload, or require exceptional skill.

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

(4) Applicants should consider at the minimum, the following items when reviewing control mode transitions:

(a) The frequency of occurrence of transfers to any alternate mode and the capability of the alternate mode. Applicants should support computed frequency-of-transfer rates with data from endurance or reliability testing, in-service experience on similar equipment, or other appropriate data.

(b) The magnitude of the power, thrust, rotor or propeller speed transients may affect the dynamics of the aircraft. Therefore these transients should be carefully assessed to assure acceptability for installation. The applicant should coordinate these characteristics with the intended installer.

(c) Successful demonstration, by simulation or other means, that the ECS controls the engine during the transition. In some cases, particularly those involving rotorcraft, applicants may be unable, analytically or through simulation, to show that the ECS can control the engine during mode transition. Therefore, applicants should propose a flight test program to demonstrate that the ECS controls the engine acceptably during in-flight control mode transitions.

(d) An analysis to identify those faults that cause either automatic or pilot initiated control mode transitions.

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

(f) Including in the engine installation instructions, a declaration of the power or thrust change associated with a transition. If the change is negligible, declare it as such.

(5) **Time delays**. Applicants should include in the engine installation and operating instructions a description of 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. The acceptability of these delays may need to be assessed during aircraft certification.

(6) **Annunciation to the flight crew**.

(a) 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 engine operation are different thrust control schedules would be very different than if timely action by the pilot is required to maintain control of the aircraft.

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

CHAPTER 6. SECTION 33.28(d) – ENGINE CONTROL SYSTEM FAILURES.

6-1. Rule Text. Section 33.28(d) reads:

"d. *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;

(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;

(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 components do not result in a hazardous engine effect due to engine control system failures or malfunctions."

6-2 Guidance: Engine Control System Failures.

a. Objective. Section 33.28(d) establishes ECS integrity requirements that are consistent with the operational requirements of the various installations. The introduction of EECSs should provide at least an equivalent level of safety and reliability for the engine as achieved by engines equipped with hydro-mechanical control and protection systems and magneto systems (refer to SAE ARP5107B and FAA Policy Memorandums on TLD in paragraph 3.b.). In chapters 9 and 15 of this AC, the concept of development errors being introduced within the software, or AEH designs ,or both, and the development assurance processes are addressed. This chapter and chapter 7 discuss the development error concept at the system level for an ECS.

b. Criteria for an LOTC/LOPC event. Industry practice over the past 30 years has resulted in the following generally accepted criteria for defining an LOTC/LOPC event. The applicant may propose another set of criteria if it defines an LOTC/LOPC event.

(1) For turbine engines not intended for rotorcraft, we consider an LOTC/LOPC event occurs when the ECS:

(a) Has lost the capability to modulate thrust or power between idle and 90% of maximum rated power or thrust,

(b) Suffers a fault that results in a thrust or power oscillation greater than the levels given in Paragraph 6-2c of this AC, or

(c) Has lost the capability to govern the engine in a manner that allows compliance with the operability regulations given in §§ 33.65 and 33.89.

(2) For turbine engines intended for helicopters, an LOTC/LOPC event occurs when the ECS:

(a) Has lost the capability to modulate power between idle and 90% of maximum rated power at flight condition and, if appropriate, at rotorcraft operating condition, or

(b) Suffers a fault that results in a power oscillation greater than the levels given in Paragraph 6-2 c of this AC, or

(c) Has lost the capability to govern the engine in a manner that allows compliance with the operability regulations given in §§ 33.65 and 33.89. The inability, however, 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 modes. Engine operability in alternate modes is a necessity if the control transitions to the alternate mode occur more frequently than the acceptable LOPC rate, or normal flight crew activity requires rapid changes in power to safely fly the aircraft.

2 The LOPC definition typically includes the ability to meet the operability regulations in the alternate mode(s). For multiengine rotorcraft, it may be acceptable if one engine control transitions to an alternate mode that may not have robust operability. That engine can be left at reasonably fixed power condition so that the operability. Engines with normally operating controls can change power as necessary to complete aircraft maneuvers and safely land the aircraft. Where this potential exists, i.e., differing operability levels, applicants may be required to demonstrate the ECS continues to meet regulatory standards under all conditions at aircraft certification.

(3) For reciprocating engines intended for part 23 Class I., II., and III. Aircraft, an LOPC event occurs when the ECS:

(a) Has lost the capability to modulate power between idle and 85% of maximum rated power at all operating conditions, or

(b) Suffers a fault that results in a power oscillation greater than the levels given in Paragraph 6-2 c. of this AC, or

(c) Has lost the capability to govern the engine in a manner that allows compliance with the operability regulations in § 33.51.

(4) For engines incorporating functions for propeller control integrated in the EECS, the applicant should consider the following faults or failures, either individually or in combination with another, as LOPC events:

(a) Inability to command a change in pitch,

(b) Uncommanded change in pitch,

(c) Uncontrollable propeller torque or speed fluctuation.

c. **Uncommanded thrust or power oscillations**. Any uncommanded thrust or power oscillations should not be of such a magnitude as to affect aircraft controllability. For example, thrust or power oscillations less than 10% peak-to-peak of take-off power, or thrust, or both, are acceptable where oscillation affects one engine only, unless the installer defines more or less restrictive requirements. Regardless of the levels discussed here, if the flight crew has to shut down an engine because of unacceptable thrust or power oscillations caused by the control system, we would deem such an event as an in-service LOTC/LOPC event.

d. **Acceptable LOTC/LOPC rate**. The applicant may propose an LOTC/LOPC rate other than those below. The applicant should substantiate such a proposal in relation to the criticality of 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. Refer to SAE ARP5107B and FAA Policy Memorandum, PS-ANE100-2001-1993-33.28TLD-R1 for additional information.

(1) For turbine engines, the EECS should not cause more than one LOTC/LOPC event per 100,000 engine flight hours.

(2) For reciprocating engines intended for part 23 Class I., II., and III. aircraft, an LOPC rate of 45 per million engine flight hours (or 1 per 22,222 engine flight hours) represents the upper limit of 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 subsystems can be fuel control, ignition control, or others. For systems with only one element, such as a fuel control, we recommend applicants use a maximum system LOPC rate of 15 LOPC events per million engine flight hours (PMEFH). For systems that contain more than one element, we recommend applicants use a LOPC rate of 15 events PMEFH for each, but only up to 45 events PMEFH. So, if two elements are present, for example a fuel control and an ignition control, the appropriate rate is 30 events PMEFH. If three or more, then the LOPC rate would be 45 events PMEFH.

e. **LOTC/LOPC analysis**.

(1) Since the LOTC/LOPC analysis is part of the required System Safety Assessment of §33.28(e), applicants must perform and submit an LOTC/LOPC analysis for the ECS. An ECS LOTC/LOPC analysis may take the form of a system reliability analysis (refer to SAE ARP5107B). We recommend a numerical analysis such as a Markov model analysis, fault tree analysis, or equivalent analytical approach.

(2) The LOTC/LOPC analysis should address all components in the system that can contribute to LOTC/LOPC events. This includes all electrical (including wiring), mechanical, hydromechanical, and pneumatic elements of the ECS.

(3) The engine fuel pump is usually considered part of the fuel delivery system and, therefore, not included in an LOTC/LOPC analysis.

(4) An LOTC/LOPC analysis should include those sensors or elements that may not be part of the engine type design, but that 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 should include the effects of loss, corruption, or failure of aircraft-supplied data. The engine installation instructions should include the assumed reliability and interface requirements for these nonengine type design elements. Within the aircraft system safety analyses, we recommend that installers ensure no double counting of the rate of failure of nonengine parts occurs.

(5) The LOTC/LOPC analysis should also consider all faults, both detected and undetected. The applicant should include any periodic maintenance actions needed to find and repair both covered and uncovered faults to meet the LOTC/LOPC rate in the engine instructions for continued airworthiness.

(6) See chapter 7 of this AC for additional guidance on how to perform the System Safety Assessment required under § 33.28(e).

f. **Reliability assessment plan (RAP)**. We recommend the applicant prepare, and be ready to show us, a RAP (refer to SAE ARP5890A for a framework). A RAP documents the applicant's controlled, repeatable processes for assessing the reliability of systems and equipment. It also helps assess the reliability of systems and equipment during design and operational life. The results of the RAP are important inputs to many safety assessment and analysis tasks. The results of a RAP can be used as a part of:

(1) Reliability program planning and monitoring,

(2) Safety assessments and analyses,

(3) Certification analyses,

(4) Equipment design decisions,

(5) System architecture selection, and

(6) Continued airworthiness assessments.

g. **Commercial or industrial grade electronic parts**.

(1) 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:

(a) IEC/TS 62239-1, Process Management for Avionics – Preparation of an Electronic Components Management Plan, and

(b) IEC/TR 62240-1, Process Management for Avionics – Use of Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges.

(2) The applicant should prepare, and be ready to show us, their Electronic Component Management Plan (ECMP).

(3) When applicants specify as part of the engine type design commercial or industrial-grade electronic components, which are not manufactured to military standards, we recommend considering data similar to the following, as applicable:

(a) Reliability data for each commercial and industrial grade electrical component specified in the design.

(b) 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.

(c) 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.

(4) Temperature ranges for commercial or industrial grade parts are typically a narrower range than those for military grade parts.

(a) If the applicant's declared temperature environment for the ECS will result in the detail parts exceeding the stated capability of the commercial or industrial grade electronic components, the applicant should ensure through test and analysis, that the proposed range of the specified components is suitable for the intended ECS environment. The applicant should also show that the failure rates used for those components in the System Safety Asssessment (SSA) and LOTC/LOPC analyses are appropriately adjusted for the extended temperature environment.

(b) Sometimes 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 should specify these provisions in the engine installation instructions, if action by the installer is required to provide cooling. This provision ensures that the cooling is not compromised. The cooling provisions included in the EECS design may have failure modes. If

the failure modes could result in exceeding temperature limits, then applicants should account for the probability of these failures in their SSA and LOTC/LOPC analyses.

(5) When any electrical or electronic components are changed, the applicant should review their 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 evaluate 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).

h. **Single fault accommodation**.

(1) The following guidance clarifies the meaning of "single fault tolerant."

(a) The applicant may show compliance with the single fault regulations of § 33.28(d)(2) and (3) by test and analysis. According to § 33.28(d), single failures or malfunctions in the ECS's components, in its fully operational condition and all declared dispatchable configurations, must not result in a hazardous engine effect (refer to § 33.75(g)(2) for a definition of "hazardous engine effects"). In addition, § 33.28(d) requires that 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.

(b) We recognize that achieving true single fault tolerance could require a triplicated design approach or one with 100% fault detection. Currently, systems have been designed with dual, redundant channels, or with backup 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) that lead to LOTC/LOPC events, they have demonstrated excellent in-service safety and reliability and have proven to be acceptable. Therefore, configurations such as these may be found to be compliant.

(2) Dual-channel or backup system configurations cover the vast majority of potential electrical and electronic faults. However, omitting some coverage because detection or accommodation of some electrical or electronic faults may not be practical, may be acceptable. Single, simple electrical or electronic components or circuits can be employed in a reliable manner. In those cases, requiring redundancy may be unnecessary. In those cases, 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.

(3) Single failures that result in a high thrust failure condition, with no throttle response, may be catastrophic for some aircraft operating conditions. As a cautionary note, engine certification applicants should be aware that in this case, either a modification of the engine control or an independent aircraft system will be needed for aircraft certification.

i. **Local events**.

(1) Under § 33.28(d)(4), foreseeable failures or malfunctions leading to local events, such as engine or installation-related failures that could lead to damage to control system electrical harnesses or connectors or to the control units, must not result in a hazardous engine event. We recommend that applicants analyze local events to ensure a hazardous engine event will not occur. These events include:

(a) Overheat conditions, for example, those resulting from hot air duct bursts,

(b) Fires,

(c) Maintenance and foreseeable maintenance errors such as using a wire bundle as a hand hold,

(d) Fluid leaks, and

(e) Mechanical disruptions that could lead to damage to control system electrical harnesses, connectors, or control unit(s).

(2) These local events are normally limited to one engine. 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 multiengine applications and the use of identical software in multiengine, dual-channel systems. In these and similar cases, the applicant should take extra design, testing or maintenance precautions to ensure safety.

(3) Although they are limited to one engine, local events affecting the ECS should not generate hazards to the aircraft. Local events, in particular fire and overheat, are dependent on installations and may also be addressed as a part of aircraft certification. Coordination with the installer is highly advised.

(4) Invalid assumptions of independence between failures, as well as failure to recognize common cause failure modes, are leading reasons for invalid conclusions within safety analyses. In the assessment of local events, emphasis should be placed on identifying and ensuring critical functional or physical isolation is maintained. The applicant should ensure no common cause event is present that would violate any assumptions of independence between failures. For example, fuel control components whose failure could result in overspeed are not affected by the same events that could cause loss of overspeed protection.

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

(6) When demonstrating that no hazardous engine effect exists based on the assumption that another function exists to provide the necessary protection, the applicant should show that the other function is not rendered inoperative by the same event (including destruction of wires, ducts, or power supplies).

(7) An overheat condition exists when the temperature of the system components is greater than the maximum safe design operating temperature declared by the engine applicant in the engine installation instructions. The ECS 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. Applicants may use specific design features or analysis methods to show 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. Refer to SAE ARP5757 for an example of this type of testing.

(8) The ECS, including the electrical, electronic, and mechanical parts of the system, must comply with the fire regulations of § 33.17. This rule applies to the elements of the ECS that are installed in designated fire zones. Refer to SAE ARP5757 and AC 33.17-1 for additional guidance.

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

(10) Applicants should consider all foreseeable local events when complying with § 33.28(d)(4). 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 ECS. Well documented local events and their analysis will aid in engine installation certification.

(11) The following guidance applies to ECS wiring.

(a) Test or analyze each wire or combination of wires interfacing with the EECS that could be affected by a local event. 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. Any EEC system component connector that becomes disconnected while the engine is operating must not result in a hazardous engine effect. Nor should it endanger the continued safe flight and landing of the aircraft.

(b) 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 should inform the installer of the potential effects of shorts in the interface wiring. The installer should ensure that no wiring faults exist that are not detectable and not accommodated. Also, these wiring faults must not result in a hazardous engine effect.

(c) 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.

(d) 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 is minimized between channels on one engine and eliminated between ECSs.

(e) The applicant should test and analyze the effects of fluid leaks impinging on EECS components. Impingement must not result in a hazardous engine effect, and the fluids should not impinge on circuitry or printed circuit boards, nor result in a potential latent failure condition.

(f) If the installation of the engine could be subject to part 25 rules, refer to the applicable sections of 14 CFR 25, Subpart H, Electrical Wiring Interconnection Systems (EWIS).

CHAPTER 7. SECTION 33.28(e) – SYSTEM SAFETY ASSESSMENT.

7-1. Rule Text. Section 33.28(e) reads: "(e) *System safety assessment.* When complying with this section 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 producing a surge or stall together with the predicted frequency of occurrence of these faults or failures."

7-2 Guidance: System Safety Assessment. Refer to Appendix 3 "Guidance for System Safety Assessment for EECS Applied to Reciprocating Engines."

a. Scope of the assessment. The methods presented in ARP4761 for conducting safety assessment are recognized for ECS assessments.

(1) The SSA required under § 33.28 (e) must address all operating modes.

(2) 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. For clarity, the remainder of the discussion mentions only the SSA, but it is equally applicable to an LOTC/LOPC analysis or combined SSA/LOTC/LOPC analysis.

(3) The SSA must consider all faults, both detected and undetected, and their effects on the ECS and engine operation. The SSA must also include faults or malfunctions in aircraft signals, including electrical opens, shorts, data validation, signal input errors and any other malfunction defined by the installer. These malfunctions should include those in a multiengine aircraft installation that could affect more than one engine. These types of faults are addressed under § 33.28(h).

(4) The ECS SSA should identify the applicable assumptions and installation requirements. It should also establish any limitations relating to ECS operation. These assumptions, requirements, and limitations should be stated in the engine installation and operating instructions, as appropriate.

(5) As necessary, the airworthiness limitations section of the instructions for continued airworthiness should include the limitations related to the ECS operation. For example, the LOTC/LOPC analysis may classify faults into various categories that may require repair within an approved time frame. Refer to SAE ARP5107B for additional information.

(6) The SSA must address all failure effects identified under § 33.75, as appropriate. The applicant may reference the § 33.75 analysis in this SSA when appropriate.

(7) The applicant must provide a summary listing the malfunctions or failures and their effects caused by the ECS, such as:

(a) Failures affecting power or thrust resulting in LOTC/LOPC events.

(b) Failures that result in the engine's inability to meet the operability regulations. If these failure cases are not considered LOTC/LOPC events according to the criteria of Chapter 6, then document the expected frequency of occurrence for these events.

(c) Transmission of erroneous parameters, for example; false high indication of the thrust or power setting that could lead to thrust or power changes greater than 3% of take-off power, or thrust, or both, (10% for reciprocating engines installations), or high exhaust gas temperature or turbine temperatures, or low-oil pressure that could lead to engine shutdown. These levels have typically been considered unacceptable, however, applicants may propose different levels for a specific engine.

(d) Failures affecting aircraft functions included in the ECS, for example, propeller control, thrust reverser control, control of cooling air, or control of fuel recirculation.

(e) Failures resulting in major engine effects and hazardous engine effects. In addition, reciprocating engine applicants must address failures resulting in destructive events.

(8) The SSA should also consider all signals used by the ECS, particularly any cross-engine control signals and air pressure signals as described in § 33.28(j).

(9) The SSA should include functions implemented in the ECS that involve aircraft level functions. The aircraft applicant needs to define the criticality of aircraft level functions.

b. **Criteria**. The SSA should demonstrate or provide the following:

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

(2) For failures leading to LOTC/LOPC events, Chapter 6, paragraph 6-2.d., provides guidance on compliance with the agreed LOTC/LOPC rate for the intended installation.

(3) For failures affecting engine operability but not necessarily leading to LOTC/LOPC events, only the rate of occurrence of the faults that could lead to an operability limitation should be documented. Any aircraft flight deck indications deemed necessary to inform the flight crew of such a failure will be determined at aircraft certification.

(4) The applicant must identify the consequences of the transmission by the ECS of a faulty parameter that is not indicated or identified as failed or faulty. If the consequence can result in loss of the ability to set power, then that fault should be included in the LOTC/LOPC analysis. The engine operating instructions should include any information necessary to mitigate the consequences of a detected faulty parameter transmission. For example, the engine operating instructions may indicate that a display of zero oil pressure 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.

(5) Flight crew initiated shutdowns have occurred in-service as the result of failure conditions, such as the ECS transmitting a faulty parameter. If the engine operating instructions provide information to mitigate this failure condition, then control system faults or malfunctions leading to the failure condition would not have to be included in the LOTC/LOPC analysis. In the case of the ECS transmitting faulty parameters, the loss of multiple functions should be included in the LOTC/LOPC analysis. For example, if the display of zero oil pressure and zero oil quantity (or high oil temperature) would result in a crew-initiated shutdown, then the applicant should include those failures in the systems LOTC/LOPC analysis.

c. **Malfunctions or faults affecting thrust or power**.

(1) In multiengine aircraft, faults that result in thrust or power changes of less than approximately 10% of take-off power 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 engine operating differences when the difference is greater than 10% in asymmetric thrust or power. A thrust change larger than 10% of take-off power or thrust, may be acceptable if authorized by the installer.

(2) Engine applicants and the installer should agree on the detectable difference level for engines for other installations. This is important as the installation can significantly affect the pilot's ability to detect the operating difference between engines. If the pilot cannot detect this difference and take appropriate action, the result may be hazardous to the aircraft.

(3) When operating in the take-off envelope, uncovered faults in the ECS that 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.

(4) 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, 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. We recommend on the order of 10^{-5} events per engine flight hour or less. Documentation of these faults may be required in the aircraft certification analysis.

(5) Signals sent from one ECS to another, such as signals used for an ATTCS, APR or synchrophasing, are addressed under § 33.28(h). These cross-engine signals should be limited in authority by the receiving ECS, 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. The ATTCS or APR, when activated, may command a thrust or power increase of 10% or more on the remaining engine(s). These thrust and power losses do not have to be considered LOTC/LOPC events. In addition, in a rotorcraft installation, signals sent

from one engine control to another, such as load sharing and OEI, can have a much greater impact on engine power when those signals fail. However, data on these failure modes should be in the SSA.

(6) When operating in the take-off envelope, detected faults in the ECS, that 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 low. A thrust change larger than 10% (15% for reciprocating engines) of take-off power, or thrust, may be acceptable if authorized by the installer. The predicted frequency of occurrence for this category of faults should 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 of less than of 10^{-5} events per engine flight hour would normally be acceptable, as the occurrence of this on multiple engines would be an extremely remote event.

(7) Detected faults in signals exchanged between ECSs 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.

CHAPTER 8. SECTION 33.28(f) – PROTECTION SYSTEMS.

8-1 Rule Text. Section 33.28(f) reads: "Protection Systems.

"(f) *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 instructions for operation.

(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."

8-2. Guidance: Protection Systems.

a. Rotor overspeed protection.

(1) In engines of recent design, the applicant usually provides overspeed protection, or circuits, or both, utilizing the engine control devices, systems and instruments referred to in § 33.28(f). Although they may be independent devices, the overspeed protection and circuits are generally part of the EECS

(2) Rotor overspeed protection is usually achieved by providing an independent over-speed protection system that requires two independent faults or malfunctions (as described below) to result in an uncontrolled overspeed. Examples of engine provided, as opposed to ECS provided, overspeed protection include blade shedding, rotor interference, or fuel cutoff methods through rotor axial movement. Engine-provided overspeed protection methods are addressed by § 33.27.

(3) The following guidance applies if the rotor overspeed protection is provided solely by an ECS protective function.

(a) In all dispatchable configurations, the combined engine control and overspeed protection system should be at least two independent faults removed from an uncontrolled overspeed event. Hence, a potential rotor burst due to overspeed should only be possible as a result of an independent fault preventing the overspeed protection system from operating properly in combination with a control system fault causing an overspeed.

(b) The SSA should show that the probability per engine flight hour of an uncontrolled overspeed condition from any cause in combination with a failure of the overspeed

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 should consider all the failure cases associated with the protection systems. Do not overlook the following cases:

- When the fuel metering valve and the fuel shut-off valve (SOV) have a common failure mode.

- When the metering valve is proposed to be used as the shut-off valve. These single valve systems have been problematic at installation.

(c) The overspeed protection system should have a failure rate of less than 10^{-4} failures per engine flight hour to ensure the integrity of the protected function.

(d) A self-test of the over-speed protection system to ensure its functionality prior to each subsequent flight is acceptable. Verifying the functionality of the overspeed protection system at engine shutdown and/or start-up is also acceptable to show compliance with this regulation's once-per start-stop cycle requirement. Some engines may routinely not be shut down between landings. If the engine is not shutdown between two flights, test of the over-speed protection system is not required but should be accounted for in the SSA.

(e) Because some overspeed protection systems provide multiple protection paths, uncertainty that all paths are functional at any given time always exists. Where multiple paths can trigger the overspeed protection system, the applicant should perform a test of a different path for each engine start/stop cycle. Doing so will achieve a complete test of the overspeed system, including electro-mechanical parts, in the minimum number of engine cycles. We recommend that the number of cycles it takes to verify the overspeed protection system be consistent with the system achieving a 10^{-4} failure rate—or the probability of failure (per hour) over the length of time that it takes to complete the number of cycles. If the system meets a 10^{-4} failure rate, it will generally be found compliant.

(f) If an applicant chooses to implement overspeed protection with a mechanical or hydro-mechanical system, the regulation does not require that the system be tested at each start/stop cycle. However, the regulation does require that the overspeed protection system's mechanical parts (not including the electro-mechanical parts) can operate without failure between inspection and maintenance periods. Therefore, we recommend that where a mechanical or hydro mechanical system is used, that applicants provide a rational maintenance interval/inspection plan to ensure that mechanical elements still perform their intended function and protect from a destructive overspeed.

b. **Other protective functions**.

(1) The ECS may perform other protective functions, only some of which may be engine functions (others may be aircraft or propeller functions). The integrity of other protective functions provided by the ECS should be consistent with a safety analysis associated with those functions. If those functions are not engine functions, they might not be part of engine certification.

(2) As ECSs become increasingly integrated into aircraft and propeller systems, they are implementing within the ECS, 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.

(3) The reliability and availability of these other protective functions should be consistent with the top-level hazard assessment of conditions involving these other protective functions. This assessment is usually 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 ECS—the applicant should show for part 23 or 25 installations, that an engine failure with loss of the auto-feather function cannot result from a single control system failure. Also, aircraft regulations may require that combinations of control system failures, or engine and control system failures, that lead to a significant engine loss of thrust or power with an associated loss of the auto-feather function have an extremely improbable event rate (10^{-9} events per engine flight hour).

(4) Although these other protective functions can be evaluated as a part of the aircraft level SSA, we recommend that applicants evaluate them during the engine certification process and present that as a part of engine certification. If the aircraft level hazard assessment involving these functions is available during engine certification, then coordination between the engine and aircraft certification teams will be smoother. If this coordination does not occur, then although the engine may be certified, it may not be installable at the aircraft level.

(5) The ECS safety assessment should include all failure modes of all functions incorporated in the system, including those functions that are added to support aircraft certification. Information on those failure modes will therefore, 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 is also needed.

CHAPTER 9. SECTION 33.28(g) - SOFTWARE.

9-1. Rule Text. Section 33.28(g) reads:

"(g) *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."

9-2. Guidance: Software.

a. Objective.

(1) Applicants should design their software to prevent logic errors that would result in an unacceptable effect on power or thrust or in other unsafe conditions. Because of the nature and complexity of systems containing digital logic, the applicant should develop software using a structured development approach, commensurate with the hazard associated with failure or malfunction of the system in which the digital logic is contained.

(2) Applicants may not be able to establish with certainty that their software design is without error. However, if applicants use the software design appropriate for the criticality of the performed functions, and an approved development method, the software satisfies the requirement to minimize errors. In some installations, the possibility of digital logic errors common to more than one ECS may determine the software level appropriate for the software design. However, we have not required channel-to-channel dissimilar designs when the software is designed as specified in Level A (DO-178B or C).

b. Approved methods. The primary FAA guidance on software methods is found in AC 20-115C. In addition, the FAA must also follow FAA order 8110.49. Acceptable methods for developing software comply with the guidelines of RTCA/DO-178C/EUROCAE ED-12C, hereafter referred to as DO-178B. The applicant may also propose alternative methods for developing software. However, any such alternate method is subject to approval by the Administrator. Reference AC 20-171 regarding alternative methods.

c. Use of supplements. DO-331, DO-332 and DO-333 are supplements that address certain software development techniques. Supplements add, delete, or modify objectives, activities, and life cycle data in DO-178C. You should apply the guidance within a particular supplement when you use the addressed technique. Your Plan for Software Aspects of Certification (PSAC) should identify which supplements apply and describe how you intend to use each applicable supplement. You cannot use supplements as stand-alone documents. Refer to AC20-115C paragraph 8 when using the supplements in conjunction with DO-178C.

d. Software levels.

(1) The level of software required for certification depends on the criticality of the functions it performs. For example, failures resulting in significant thrust or power increases or

oscillations may be more severe than an engine shutdown. Therefore, consider these failures when selecting a given software level.

(a) Design, implementation, and verification of software as specified in Level A (DO-178C) is normally needed for turbine engines.

(b) For a reciprocating engine EECS, software implemented as specified in Level C is the minimum acceptable requirement.

(c) The applicant may choose to evaluate the failure condition criticality of EECS functions to determine if Level B or C software would be adequate. The applicant must coordinate this evaluation with the aircraft designer and the cognizant aircraft ACO during the EECS development program.

(2) Applicants may protect or partition noncritical software from critical software and design and implement the noncritical software to a lower level. 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.

e. **Legacy software**. Software developed using DO-178, DO-178A, or DO-178B is referred to as legacy software. Refer to AC20-115C paragraph 9 when modifying and re-using software approved using DO-178, DO-178A, or DO-178B.

f. **Onboard or field-loadable software and part number marking**.

(1) When Field-Loadable Software (FLS) is used in EECS, and the applicant wants to use electronic part marking for the FLS, the FLS must meet the part marking requirements of § 45.15 (c). The information required, like that for a hardware part number, must be verifiable in the aircraft at any geographic location on the ground. Use the following guidelines and, for additional information, refer to FAA order 8110.49, Chapter 5, “Approval of Field-Loadable Software (FTS),” when onboard or field loading of EEC software and associated Electronic Part Marking is implemented. While the order is directed at the FAA certification engineer, the applicant is advised to much of the following material in 9-2 e. and its subparagraphs based on the Order’s requirements.

(2) For software changes, document the software to be loaded through an approved design change and a released service bulletin or other appropriate documentation.

(3) For an EECS unit with separate part numbers for hardware and software, the software part numbers 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 verification by electronic means requirement applies and the proper software part number must be verified before the unit is returned to service.

(4) For an EECS unit with only one part number, the one 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. As a portion of this process the software build or version number should be verified before returning the unit to service.

(5) For an EECS that will be onboard or field loaded, you cannot use the configuration control system and electronic part marking unless it was approved at the time of engine certification. 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 the applicant must update it for each change that affects the hardware and software combination. The applicable service bulletin must define the hardware configurations with which the new software version is compatible.

(6) The loading system must be in compliance with the guidelines of DO-178C, Section 2.5.5. If the applicant proposes more than one source for loading, (such as disk, CD or mass storage), all sources must comply with these guidelines.

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

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

(1) The determination of a major versus minor type-design change is established in § 21.93. A change to the software in an ECS may affect the reliability, operational characteristics, or other characteristics affecting the airworthiness of the product. Therefore, a change to the software is normally classified as major.

(2) The failure effect of EEC software is always assumed to be at least a major effect because an error could result in the total loss of thrust or power to all engines on an aircraft.

(3) Refer to FAA order 8110.49, particularly Chapter 11, “Oversight of Software Change Impact Analysis Used to Classify Software Changes as Major or Minor” for additional information.

h. **Software Changes by Others than the Type Certificate (TC) Holder**.

(1) 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.

(2) Two types of software changes that are feasible and can be implemented by someone other than the original TC holder are:

- Changes to option-selectable software, or

- Changes to user-modifiable software (UMS).

(a) Option-selectable software changes are implemented via precertified logic that uses a method of selection shown not to cause a control malfunction.

(b) User-modifiable software is software intended for modification by the aircraft operator without review by the certifying authority, the aircraft applicant, the engine manufacturer, or the equipment vendor. For ECSs, UMS has generally not been applicable. However, if approval of UMS is required, it will be reviewed on a case-by-case basis.

1 The necessary guidance for UMS is contained in DO-178C, paragraph 2.5.2. The guidance allows non-TC holders to modify the software within the constraints defined by the TC holder if the system has been certified with the provision for software user modifications. Refer to FAA order 8110.49, particularly Chapter 7, "Approval of Airborne Systems and Equipment Containing User-Modifiable Software (UMS)" for additional information.

2 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.

3 When software is changed in a manner not allowed by the TC holder as "user modifiable," the non-TC holder applicant must comply with all applicable requirements of part 33, particularly § 33.28, as well as the requirements in part 21, subpart E. Refer to FAA order 8110.49, particularly Chapter 7, "Approval of Airborne Systems and Equipment Containing User-Modifiable Software (UMS)" for additional information.

CHAPTER 10. SECTION 33.28(h) – AIRCRAFT-SUPPLIED DATA.

10-1. Rule Text. Section 33.28(h) reads:

"(h) *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 in the engine installation instructions the effects of these failures on engine power or thrust, engine operability, and starting characteristics throughout the flight envelope."

10-2. Guidance: Aircraft-Supplied Data.

a. Objective. The EECS should be self-sufficient and isolated from other aircraft systems, or provide redundancy that enables it to accommodate aircraft data system failures. 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. The single failure requirement applies to all dispatchable configurations of the engine control and aircraft air data systems.

b. Background.

(1) Reciprocating engines with EECS are not considered "conventional reciprocating engines." For conventional reciprocating engines, magneto ignition and mechanical fuel systems can accommodate single failures leading to loss, interruption or corruption of aircraft-supplied data or data shared between engines. Therefore, further guidance is not necessary concerning conventional reciprocating engines.

(2) For reciprocating engines with EECS, any LOPC event is an unacceptable change in power. Therefore, as required by § 33.28 (h)(2), the applicant should show that the failure of aircraft-supplied data does not cause a LOPC.

(3) Aircraft-supplied data failures that result in engine effects less severe than a LOPC, such as a minor power loss, are typically considered to be acceptable changes in power. The analyses and the engine installation and operating instructions should identify these types of events along with their effects on engine operation if the effect of the event can be observed by the flight crew. This data can also be used in the powerplant installation safety analysis required during airplane certification to evaluate the impact of these failures on airplane operations.

(4) Previous regulatory practice preserved the independence of the engine from the aircraft. Hence, even with very reliable architectures, such as triplex air data computer (ADC) systems, the ECS provided an independent control that crews could use to safely fly the aircraft should all the ADC signals be lost. 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 the ECS provide fault accommodation against single failures of aircraft-supplied data for which such accommodation is possible.

c. **Design Assessment**.

(1) As part of their compliance plan, applicants should provide an analysis, based on component, system, or engine testing, that shows they adequately evaluated the impact of a failure of aircraft data on the engine's performance and operability throughout the aircraft flight envelope. This failure analysis should address all allowable engine control and aircraft dispatch configurations in which failure of aircraft data in that dispatch configuration would impact ECS response. "Failure of aircraft data," includes airplane system failure events that either prevent data from being transmitted or result in the transmission of incorrect data. This analysis should include:

(a) Their evaluation of the engine control responses to aircraft data inputs, including an evaluation of the effect on the EECS of faulty and corrupted aircraft-supplied data.

(b) An evaluation of the potential for common mode faults affecting operation of more than one engine in EEC systems intended for installation on multiengine airplanes. The installation and/or the operating instructions should identify data transfers and exchanges between engines, and between the airplane and engines, that could produce common mode faults. Examples of potential common mode faults that the analysis should address include:

1 A single erroneous data source transmitted from the aircraft to multiple engines and their associated EEC systems (for example, air data sources or auto throttle systems),

2 Control system operating faults spread through data links between engines (for example, maintenance recording, common bus, cross-talk, or automatic power reserve system), and

3 Loss or interruption of aircraft data used by the engine control when that loss or interruption is caused by the failure of another engine.

(c) An evaluation of the EECS fault accommodation logic for coverage of aircraft-supplied data failures. Applicants should conduct testing or analysis on the fault accommodated control mode to establish that the engine operating characteristics comply with all operability requirements of part 33. The applicant may incorporate precautions for addressing common effects in the aircraft system architecture or in the EECS itself.

(2) When the particular aircraft air data failure mode(s) are unknown, the engine applicant should assume typical failure modes for loss of data and erroneous data. The engine applicant should assume that erroneous data is being transmitted to the EECS and identify for the installer the impact of this data on engine operation.

(3) The applicant may use any number of tools and techniques to assess and to shape the design of the ECS and its interface with the aircraft data systems. One example is the use of a Fault Accommodation chart and Markov Modeling, wherein applicants define the fault accommodation architecture for the aircraft-supplied data.

(4) If the ECS relies entirely on aircraft air data to complete any of its critical control functions, then the aircraft air data system becomes an element of the ECS. To maintain compliance to § 33.28, the applicant must require via the installation, or the operating instructions, or both that:

(a) 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).

(b) No common mode faults exist where multiple incorrect, but valid, signals are transmitted to the EECS (for example, dedicated sensor(s) and pneumatic lines for each air data computer).

(5) The ECS's LOTC/LOPC analysis should also analyze the effects of air data system failures in all allowable ECS and air data system dispatch configurations.

(6) Elements of the ECS, such as a throttle position transducer, may be mounted in the aircraft and not part of the engine type design but dedicated to the ECS and powered by it. Such elements are an integral component of the EECS, and are not considered aircraft data. The applicant should include failures in the throttle position sensing system and thrust command system in their engine LOTC/LOPC analysis.

(7) When aircraft-supplied data can affect ECS operation, the applicant should address the effects of faulty and corrupted aircraft-supplied data on the EECS, as applicable, in the SSA or other appropriate documents.

d. **Accommodation**. Even with a redundant, multipath aircraft air data system, the EECS should incorporate appropriate accommodation features. These features should retain a thrust or power modulation capability for complete loss of all aircraft environmental (i.e., speed, altitude, temperature data) information. The following are examples of possible means of accommodation:

(1) Implementation of an alternate mode that is independent of aircraft-supplied data.

(2) Dual sources of aircraft-supplied sensor data with local engine sensors providing data as alternate sources. This local engine sensor can be used to aid in the selection of the

correct aircraft-supplied data. The local engine sensor used in this selection is often called a voter.

(3) **Use of synthesized engine parameters to control or act as voters**. When synthesized parameters are used for control or voting purposes, the SSA should consider the impact of temperature and other environmental effects on sensors whose data are used in the synthesis. Also, applicants should assess any data tolerances necessary to correlate the data from the sensors used in the synthesis and the parameters being synthesized.

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

e. **Effects on the engine**. Applicants should ensure that their ECS system is capable of ensuring that the engine provides the declared minimum rated thrust or power throughout the engine operating envelope. The effects of failures in aircraft-supplied data must be documented in the SSA as described in Chapter 7 of this AC.

f. **Validation**.

(1) Applicants should demonstrate by test, analysis, or a combination thereof, that their ECS fault accommodation logic continues to successfully manage engine performance when the aircraft air data system is not functional.

(2) Applicants should also show that for all dispatchable control modes that involve aircraft data, the next single fault in the EECS does not lead to a hazardous engine effect.

(3) When the alternate mode is intended to be a dispatchable mode, applicants should demonstrate that the ECS continues to successfully meet the engine and aircraft certification basis when operating in this alternate mode, and the aircraft air data system is not functional. The objective here is to assure that a dispatchable alternate mode does not lead to a hazardous engine effect when there is a subsequent loss of aircraft air data. The instructions for installation should include characteristics of operation in this alternate mode, even if it is a nondispatchable mode.

g. **Installation requirements**. As a result of increasing levels of integration between aircraft systems and ECSs, engine applicants should show that their installation instructions provide guidance with certain aspects of the data interface during the integration of the engine. “Certain aspects” includes ensuring that the engine continues to meet its certification basis when installed. This means that the engine applicant should state in the engine installation instructions that the installer is responsible for ensuring that:

(1) The software in the data path to the EECS is at a level consistent with how the aircraft data is used by the EECS, as described and analyzed in the EECS’s SSA, and

(2) The impact of the engine responses are included in the aircraft’s SSA as the data path may include other aircraft equipment, such as aircraft thrust management computers, or other avionics equipment, and

(3) The effects of faulty or corrupted aircraft-supplied data on the EECS are addressed in the aircraft SSA, and

(4) Those sensors and equipment involved in delivering information to the EECS continue to operate properly when exposed to EMI, HIRF and lightning, and

(5) The reliability level for the aircraft-supplied data is no worse than that used as part of the EEC's SSA and LOTC/LOPC analysis, and

(6) Any assumptions made during the ECS design assessment regarding the reliability or configuration of the aircraft systems are appropriate, and thus the results of the evaluation of erroneous aircraft data as documented in the SSA are also appropriate.

h. **Thrust and power command signals**.

(1) Thrust and power command signals sent from the aircraft are unique and are not subject to the regulations of § 33.28(h).

(2) Some aircraft thrust or power command systems are configured to move the engine thrust or power levers or transmit an electronic signal to command a thrust or power change. When so configured, the ECS merely responds to the command and changes engine thrust or power as appropriate. In these cases, other than input range or data validity checks, the ECS should not attempt to differentiate between correct or erroneous throttle or power lever commands. For EEC systems in which the throttle or power lever command system is not included in the EEC system design, do not include thrust and power command signals sent from the aircraft in the evaluation required by § 33.28(h)(2).

(3) For EEC systems in which the power lever command is included in the EEC system design to be certificated under part 33, we recommend including the thrust and power command signals in the analysis.

(4) In both moving and non-moving throttle (or power lever) configurations, the installer should ensure that a proper functional hazard analysis is performed on the aircraft system involved in generating engine thrust or power commands. The installer should also ensure that the system meets the appropriate aircraft functional hazard assessment safety related regulations. This should be shown at aircraft certification. However, failures in the throttle position sensing system and thrust command system must be included in the LOTC/LOPC analysis of the engine as defined in the LOTC/LOPC analysis system description.

CHAPTER 11. SECTION 33.28(i) – AIRCRAFT-SUPPLIED ELECTRICAL POWER

11-1. Rule Text. Section 33.28(i) reads: "(i) *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 paragraph (i)(1) of this section, 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 paragraph (i)(3) of this section must meet the requirements of paragraph (i)(1) of this section. The engine control system must be capable of resuming normal operation when aircraft-supplied power returns to within the declared limits."

11-2. Guidance: Aircraft-Supplied EECS Electrical Power.

a. The most common means of providing electrical power to an EECS has been an engine-mounted alternator. An EECS dedicated engine-mounted alternator is not subject to the typical interruptions and power transients present in the aircraft power systems. In addition, this configuration is typically single-electric fault tolerant including common cause/mode electric fault tolerant. However, other options do exist, and are discussed below.

(1) **Batteries**. Batteries are not generally an acceptable aircraft-supplied power source, particularly for turbine engine aircraft, as they are unable to satisfy the reliability needs for the EECS. For reciprocating engines, however, an ECS dedicated battery may be acceptable. If an applicant proposes a battery as an EECS dedicated power source, the applicant should in the engine installation instructions, identify battery health, status, and maintenance requirements.

(2) **Self-contained electrical power systems**. This type of system is an integral part of the engine design. The self-contained reference may be only applicable to the critical functions of the ECS. It is both functionally and physically isolated from the aircraft electrical power system. This is acknowledging that there are means other than an alternator that may be used. However, an engine driven alternator based system does fit into this type of system.

(a) A self-contained system is considered part of the EECS, and applicants should include the predicted failure event rate of the self-contained system in the EECS SSA.

(b) A self-contained system may not require backup electrical power. However, if aircraft power is a backup power source, then applicants should provide detailed electrical system interface requirements in the engine installation instructions.

(c) Applicants should also show in their compliance plan, that abnormalities in the aircraft power system cannot cause the EECS to behave abnormally. The applicant does not have to include the predicted failure event rate of this backup power system in the EECS SSA because we have not typically allowed credit toward achieving system reliability based on backup power from the aircraft.

(3) **Aircraft power bus**. If a power source supplies power to both the aircraft main power bus and the EECS, the source may be "independent" for purposes of evaluating EECS power sources, but further inquiry is needed. The determination is made by looking at what is dedicated to the EECS, and what is not. For example, if the EECS draws its power from the aircraft main power bus, the power is aircraft bus supplied power and the EECS does not have a self-contained engine power source. However, if a winding on an alternator with dual windings provides only the EECS with power, the dedicated winding is a self-contained engine power source, even if the other winding provides power to the main power bus. In this instant the EECS power source would be "independent," even though the alternator supplies both.

b. **Design architecture analysis**.

(1) **Dedicated aircraft power**.

(a) Applicants should ensure that the design of any engine dedicated power source would provide sufficient power to allow the ECS to continue functioning during any anticipated engine recovery event. For example, when autolight is an intended ECS function, the ECS should have sufficient power to continue operation during an automatic relight after unintended shutdown. ECS independence from aircraft power during restart when the engine is windmilling, is not always required. For example the ignition system is often powered by the aircraft electrical system.

(b) The applicant should also ensure that the ECS design accounts for any anticipated variations in aircraft power availability, such as those due to temperature variations, manufacturing tolerances, or idle speed variations.

(2) **Failure of aircraft-supplied power**. The applicant should show through analysis, or bench testing that the EECS continues to function properly during and after a failure or interruption of an aircraft-supplied power source at any point within the declared engine-operating envelope. The applicant's analysis of the ECS design architecture should identify all requirements for engine-dedicated and aircraft-supplied power sources. The analysis should 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 should also define the aircraft-supplied power requirements.

c. **Aircraft-supplied power system(s)**. Applicants should consider the single bus failure rate.

(1) **Failure of a single bus**. A failure of one of multiple aircraft buses is not considered a loss of aircraft power if the buses are independent and power the EECS separately. Therefore, a backup source could be an alternate bus, such as an essential bus, that is independent, isolated from the bus serving as the primary power source, and services only electrical loads required for continued safe operation.

(2) **Installation instructions**. The engine installation instructions may reference a detailed wiring diagram with the information. If it does, the wiring diagram itself should not need to be issued as a part of the engine installation and/or operating instructions.

(3) **Failure event rate**. If required to meet the declared LOTC/LOPC failure rate, the applicant should include in the installation instructions the maximum allowable failure event rate for the aircraft electrical power system, recalling that the total EECS failure event rate, including the aircraft power source, must remain within the EECS SSA criteria for full-up and degraded systems. This inclusion of failure rate data insures that, as installed, the ECS still satisfies the allowable rates.

(4) **Aircraft as primary power source**. If aircraft-supplied power, such as an aircraft bus and battery system, is used as the primary power source, then the EECS should have an isolated backup power source. This backup power source can be integral to the engine EECS or provided by the airplane.

(a) Separation of EECS power and aircraft power. Aircraft electrical power generators or battery systems certified with the engine should be physically and functionally separate from the primary EECS power system to avoid any interaction and potential for common cause or common mode failures.

(b) Backup power source monitoring. The applicant should provide ICA and provisions for system monitoring. System monitoring will ensure that the backup system is capable of powering the EECS for continued safe flight. For example, a battery system should incorporate provisions for charge level monitoring and the ICA should include maintenance procedures to ensure that the charge level is adequate to power the EECS.

(c) Backup power, such as alternate buses, essential buses, or battery systems. We recommend that the engine installation, or operating instructions, or both, specify the following to ensure that the installer does not violate any of the assumptions in the EECS SSA:

1 A requirement that the backup system be physically and functionally separate from the primary EECS power system, and

2 The interface and reliability requirements needed for the airplane system to meet overall EECS objectives, and

3 System charge level or power requirements and health monitoring requirements to ensure that power or charge level is available, and

4 For battery systems, a requirement to isolate the backup battery system from the engine starting battery system, and

5 For battery systems, a requirement that the battery capacity must allow for engine operation to be maintained in excess of the time required for the primary flight displays.

d. **Aircraft-supplied power reliability**.

(1) **Power reliability values**. The applicant should include in the engine installation instructions all aircraft-supplied power reliability values that they used in their system analyses. This is to ensure that the installer does not violate any of the assumptions in the EECS SSA.

(2) **Inclusion of aircraft power effects**. Applicants should include in the EECS SSA all events where the aircraft-supplied power is used in any architecture and aircraft power faults or failures can contribute to LOTC/LOPC or hazardous engine effects.

(3) **Credit for backup power**. Aircraft-supplied power has typically been provided to accommodate the loss of the engine dedicated power source. However, we will review 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 backup system or as a backup power source on a case-by-case basis. If the engine control can operate in the presence of aircraft power bus transfers, then the use of aircraft power as a backup may be acceptable.

(4) **Without dedicated power source**. In some system architectures, compliance with the regulations may not require an engine dedicated power source. Two examples are mixed electronic and hydro-mechanical systems, and EEC systems that could support a critical fly-by-wire flight control system. Both are discussed below.

(a) Mixed electronic and hydromechanical systems.

1 These systems consist of a primary electronic single channel and a full capability hydromechanical backup system independent of electrical power. A full capability hydromechanical control system meets all part 33 regulations and does not depend on aircraft power. In this architecture, a loss or interruption of aircraft-supplied power is accommodated by transferring control to the hydromechanical system.

2 Transition from the electronic to the hydromechanical control system is addressed under § 33.28 (c). For these systems, the applicant should show that the transition from the electronic-powered mode to the mechanical control mode can be performed without the aircraft-supplied power and without the occurrence of an LOTC/LOPC.

(b) EECS powered by an aircraft power system that could support a critical fly-by-wire flight control system.

1 These systems may be acceptable as the sole source of power for an EECS. In this example, the engine installation instructions should 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 should also state that any emergency power sources must be known to be operational at the beginning of the flight.

2 Any emergency power sources should 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 should show that the flight crew can determine battery condition prior to flight, and that battery capacity is sufficient to ensure exhaustion will not occur before the airplane lands. This will ensure that appropriate reliability assumptions are provided to the installer.

e. **Aircraft-supplied power quality**.

(1) **Requirements**. When aircraft electrical power is necessary for operation of the ECS, the engine installation instructions must contain the ECS's electrical power supply quality requirements. This applies to any of the configurations listed above or to any new or novel configurations that use aircraft-supplied power. These quality requirements should include steady state and transient under-voltage and over-voltage limits for the equipment. RTCA/DO-160/EUROCAE ED-14 provides additional information on setting power input standards. If used, the applicant should identify any exceptions to the power quality standards cited for the category of equipment specified.

(2) **Low voltage transients**. 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. When the ECS is operating on aircraft-supplied power, if low voltage aircraft power supply conditions are below those required to sustain normal operation, the electrical or electronic components of the ECS may not function as intended. However, during these transients, EECS operation must not per regulation, result in a hazardous engine effect. Further, low voltage transients outside the control system's declared capability should not:

(a) Cause permanent ECS loss of function, or

(b) Result in inappropriate system operation, or

(c) Cause the engine to exceed any operational limits, or

(d) Cause the transmission of unacceptable erroneous data.

f. **Power recovery**.

(1) Power recovery from voltage transients does not usually apply to systems powered by ECS dedicated PMA/PMG systems. However, aircraft supplied power does have the potential to have low voltage transient. Impact from these type of transients has been shown to affect ECS using aircraft power for backup power even when they are being powered by a PMA/PMG. The applicant should demonstrate the ECS reaction to aircraft power low voltage transients. The following cases should also be tested if the system could be operating on aircraft power:

(a) Recovery from low voltage. When aircraft power recovers from a low-voltage condition, the ECS must resume normal operation. Applicants should include in the engine installation or operating instructions the time interval associated with this recovery.

(b) Aircraft low power supply condition. These 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, applicants should include in the operating instructions any special flight crew procedures for executing an engine restart during such conditions.

(c) Low voltage transients effects. These transients can be 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. Therefore, the applicant should consider the effects of any aircraft electrical bus-switching transients or power transients in the engine installation or operating instructions.

(2) **All engine out restart**. During certain aircraft operations, such as low engine speed and in-flight engine restarts, aircraft electrical power is generally used to operate the ECS. However, operationally, battery power may have to suffice. If battery power is required to meet a low engine speed or “all engine out” restart requirement, the engine applicant should define the battery power requirements and verify them via test. Those power requirements will thereafter, be available to the installer in the engine installation instructions and will ensure that the EECS will generally have sufficient power during any in-flight engine restart(s).

g. **Effects on the engine**.

(1) **Change of control mode**. 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).

(2) **Acceptable loss of aircraft electrical power**. 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.

(a) Engine operating characteristics. These are acceptable if the engine is still capable of complying with all of the rules and does not operate in a manner unexpected by the pilot.

(b) Similar designs. Examples include the ignition systems and some performance enhancing systems (see (3) below) that are typically powered by aircraft.

(c) Accommodation. This refers to whether the loss of the function is accommodated by automatic control features that result in an unnoticeable operational change.

(3) **Aircraft powered functions**. Examples of engine control functions that have traditionally relied on aircraft power include

(a) Engine start and ignition,

(b) Thrust reverser deployment,

(c) Anti-icing (engine probe heat),

(d) Fuel shut-off,

(e) Over-speed protection systems, and

(f) Noncritical functions that are primarily performance enhancement functions that, if inoperative, do not affect the safe operation of the engine.

h. **Validation**. The applicant should demonstrate the effects of loss of aircraft-supplied electrical power by engine test, system validation test, bench test, or combination thereof.

i. **New and novel design concepts**. Technological advances in electrical power-generating components and in the associated systems may allow for new and novel design concepts to meet the requirements of § 33.28(i). For example, dual use alternators or use of an essential battery, are concepts that until recently were not considered successful. Therefore, if an applicant has a new or novel design concept, we recommend contacting the responsible certification office early to develop an appropriate compliance plan.

CHAPTER 12. SECTION 33.28(j) – AIR PRESSURE SIGNAL.

12-1. Rule Text. Section 33.28(j) reads:

"(j) *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 paragraph (e) of this section and must adopt the appropriate design precautions."

12-2. Guidance: Section 33.28(j) covers ingress of foreign matter (for example, sand, dust, water, or insects) that could result in blockage of the lines and adversely affect engine operation. Lines used for measuring the static pressure in the compressor of turbine engines can suffer from two predominate failure modes: signal lines are either blocked by frozen water (leading to a loss of power or to failures to detect changes in the engine static pressure) or they fail to open or develop a leak, thereby leading to a loss of power. Each are discussed separately.

a. Signal lines can be blocked by frozen water. We recommend applicants take precautions, such as:

(1) Use of protected openings,

(2) Filters,

(3) Drains for water,

(4) Effective geometry of plumbing to aid in draining,

(5) Appropriate plumbing line inside diameter to aid in draining,

(6) Appropriate bleed hole and drain hole sizing,

(7) Heating the lines to prevent freezing of condensed water, and

(8) Corrosion resistant features.

b. Signal lines can also fail to open or develop a leak. Precautions might in this case, include:

(1) Enhanced support of the plumbing lines to prevent loosening or fracture due to vibration or handling damage during maintenance,

(2) Special design precautions to prevent loosening of the fittings, and

(3) Appropriate plumbing line size for durability.

c. In addressing system failure modes, the applicant should consider both pressure line failure modes in paragraphs a. and b. above independently and in combination.

CHAPTER 13. SECTION 33.28(k) – AUTOMATIC AVAILABILITY AND CONTROL OF ENGINE POWER FOR A 30-SECOND OEI RATING.

13-1. Rule Text. Section 33.28(k) reads:

"(k) *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."

13-2. Guidance: Using a 30-second OEI rating during flight may create high pilot workload. Therefore, the rating should be applied and controlled automatically by the ECS, other than to terminate it. Until terminated, the software should 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.

a. 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. This should free the pilot to focus on flying the aircraft. Such means for automatic control within the operating limitations must be effective during normal and abnormal operations.

b. When selected, the means required by § 33.28(k) must automatically govern the engine to its 30-second OEI power rating. The applicant should provide information in it's installation instructions, on methods to ensure that engine limiter settings do not prevent the engine from reaching the 30-second OEI power. These limiter settings may include engine speed, measured gas temperature and fuel flow. Pay particular attention to take-off conditions with a cold-soaked engine.

CHAPTER 14. SECTION 33.28(L) – ENGINE SHUT DOWN MEANS.

14-1. Rule Text. Section 33.28(l) reads:

"(l) *Engine Shut Down Means.* Means must be provided for shutting down the engine rapidly."

14-2. Guidance: Engine shut down means. This requirement is usually met through a fuel shut-off valve in the fuel metering system of the engine control. The pilot usually activates the valve via a switch or lever. In some applications, however, the valve is not part of the engine control. In these cases, the applicant should indicate in the installation manual that a pilot initiated means for rapid shutdown of the engine must be provided by the installer. The engine manufacturer and the installer should coordinate a mutually acceptable means. The issues to be addressed include the acceptability of the valve's location and response time, its compatibility with the ECS, and the pilot's capability to rapidly select this function. In addition, the valve may have reliability, environmental, fire, or other requirements.

CHAPTER 15. SECTION 33.28(M) - PROGRAMMABLE LOGIC DEVICES (PLDS).

15-1. Rule Text. Section 33.28(m) reads:

"(m) *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."

15-2. Guidance: Previously, PLDs were the devices of greatest concern in the family of devices complex enough to require additional certification scrutiny. Further, the FAA had not yet recognized RTCA/DO-254 as a method for showing compliance. So, the FAA issued AC 20-152, RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware, which limits the scope of the application of DO-254. AC 20-152 remains "current guidance." However, AC 33.28-1A supplements and reinforces the guidance in AC 20-152, and provides guidance specific to engine controls. Applicants should be aware that the broader scope of AEH, covered by AC 20-152, is verified at the installation level.

a. **Objective**. Applicants should design their logic to minimize logic errors that would result in an unacceptable effect on power or thrust or in other unsafe conditions. Because of the nature and complexity of systems containing digital logic, the applicant should develop PLDs using a structured development approach. The applicant's approach must be commensurate with the hazard associated with failure or malfunction of the system in which the digital logic is contained. Applicants may not be able to establish with certainty that their PLD design is without error. However, if the applicant uses the hardware design assurance level appropriate for the criticality of the performed functions and an approved development method, the logic satisfies the requirement to minimize errors.

b. **Approved methods**. The primary FAA guidance on PLDs is found in AC 20-152. Addition information can be found in FAA order 8110.105 CHG 1, Simple and Complex Electronic Hardware Approval Guidance. Methods for developing PLDs, compliant with the guidelines of document AC 20-152, are generally acceptable. The applicant may, however, also propose alternative methods for developing PLDs.

c. **Level of hardware design assurance**.

(1) 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.

(2) In multiple engine installations, the possibility of digital logic errors common to more than one ECS may determine the criticality of the hardware design assurance level.

However, the FAA has not required dissimilar designs when the PLD is designed as specified in Level A (DO-254).

(3) The criticality of control 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.

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

CHAPTER 16. OTHER CONSIDERATIONS: ENGINE, PROPELLER, AND AIRCRAFT SYSTEMS INTEGRATION AND RELATIONSHIPS BETWEEN ENGINE, PROPELLER, AND AIRCRAFT CERTIFICATION ACTIVITIES

16-1. Systems Integration.

a. Two forms of systems integration are discussed. First, aircraft or propeller functions integrated into EECS hardware and software, and second, integrating engine functions into aircraft systems. One version of systems integration involves the integration of aircraft or propeller functions (i.e. those that have traditionally not been considered engine control functions) into the EECS hardware and software. The other version involves aircraft systems performing functions traditionally considered part of the ECS. These are addressed in paragraphs (2)(a) and (2)(b), respectively, below.

b. We encourage applicants with highly integrated systems to develop an EEC System Integration Certification Plan (SICP). A SICP should identify the tasks unique to integration. You should include in it's SICP a clear definition of the respective certification tasks of the engine, propeller, and aircraft manufacturers. The applicant should also develop it's plan during close coordination with the associated engine, propeller, and aircraft certification authorities. The SICP may provide valuable information to the installer and should be provided to the installer for their use. It may address the following types of integration:

(1) **Aircraft or propeller functions integrated into the ECS or EECS**.

(a) Examples of aircraft or propeller functions integrated into the ECS include thrust reverser control systems, propeller speed governors, ATTCS, and APR System. When integrating aircraft or propeller functions into the ECS, the EECS failure cases related to the integration need to be included in the Aircraft Level SSA by the installer. Although aircraft functions incorporated into the ECS may be reviewed at engine certification, the acceptability of the safety analysis involving these functions will be determined at aircraft certification.

(b) The EECS may be configured to contain parts 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.

(c) One example of configuring the ECS to contain all functionality of an aircraft system: an ECS designed to fully govern propeller speed in turboprop aircraft. Here, the engine applicant may need to configure the ECS logic to feather a propeller when an engine fails. Failure of the prop to feather may result in catastrophic aircraft failure as the result of excessive drag. Another example is an ATTCS or APR in turbofan aircraft. If an engine fails during takeoff, the engine applicant may need to configure the logic to increase the thrust of the remaining engine(s). Both examples indicate that criticality is not limited, since ECS failure

could result in loss of aircraft. Both examples also involve aircraft functionality that would receive significant review during aircraft certification.

(d) When functions like these are integrated into the ECS so that they render an ECS critical, the applicant should 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.

(2) **Integration of engine control functions into aircraft systems**.

(a) Applicants may use aircraft systems to implement a significant number of ECS functions. For example, integrated flight and ECSs, such as those integrated into avionics, may be used to govern engine speed, and in helicopters, rotor speed, rotor pitch angle, and rotor tilt angle. A special case of this type of implementation is via an Integrated Modular Avionics system as defined in RTCA/DO-297. Implementation of a FADEC in an Integrated Modular Avionics system will require special considerations. The engine applicant needs to coordinate this with the Engine and Propeller Directorate. In these examples, we may require aircraft systems be used during engine certification. If so, then the engine applicant should specify the EECS requirements in the engine installation instructions and show that those EECS requirements are adequate to protect the engine from any hazardous engine effects.

(b) An example of limited integration is an engine control that receives a torque output demand signal from the aircraft and responds by changing the engine's fuel flow and other variables to meet that demand. Then the EECS, which is part of the type design, provides all the functionality required to safely operate the engine as required by part 33 or other applicable specifications.

16-2. Certification Activities.

a. **Engine certification**. All hardware and software that reside on the engine, including those that provide aircraft or propeller functions, must meet the requirements of §§ 33.28(b), (f), (g) and (m). This should include environmental testing of all components and software, and quality assurance of the software that performs both the engine and aircraft functions. The EECS SSA and other analyses (aircraft power, fault accommodation, etc.) that the engine applicant submits for engine certification, should address only engine functions performed by the EECS. The aircraft and propeller functions do not need to be evaluated in the EECS SSA unless the functions affect engine operation or reliability.

b. **Aircraft or propeller certification**.

(1) The aircraft or propeller certification program should include all hardware and software substantiation requirements for the hardware and software that reside on the aircraft or propeller, including those that perform engine control functions. The applicant should also include environmental testing of all components and software, and quality assurance of the software that performs both engine and airplane functions.

(2) To satisfy aircraft requirements, such as §§ XX.901, XX.903 and XX.1309, the applicant should analyze the consequences to the aircraft of ECS failures. Together with the aircraft applicant, the engine applicant should ensure that the ECS software and AEH levels and safety and reliability objectives are consistent with aircraft certification requirements.

c. **Interface Definition and System Responsibilities**.

(1) The applicant should identify in the appropriate documents, e.g., EEC SICP or an Interface Control Document (ICD), the system responsibilities as well as interface definitions for the functions, the hardware and the software. These interfaces are typically between the engine, propeller, and aircraft systems.

(2) The engine, propeller, and aircraft documents should include:

(a) Requirements and categorization of the severity of the effects of a failure condition (that may be based on engine, propeller, and aircraft considerations),

(b) Fault accommodation strategies,

(c) Maintenance strategies,

(d) The software and airborne electronic hardware levels (per function if necessary), and

(e) The reliability objectives for:

1 LOTC/LOPC and MPL events, and

2 Transmission of faulty parameters.

(f) 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),

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

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

d. **Distribution of compliance tasks**. Engine, propeller, and aircraft applicants often share aircraft propulsion system certification tasks. This is particularly true for aircraft propulsion systems equipped with electronic controls. Therefore, applicants sharing aircraft propulsion system certification tasks should identify how these tasks are distributed between themselves. They should also include this distribution in their compliance plan(s). For example, the EEC SICP should list each task related to the EECS certification, identifying what each applicant should accomplish. The plan should likewise, address all analyses and tests required for EECS certification, also identifying what each applicant should accomplish. The appropriate engine,

propeller, and aircraft authorities will reach an agreement with the manufacturers on this distribution. This will ensure that all certification responsibilities are fully understood by each applicant, thereby avoiding certification delays.

(1) An EECS controlling the engine and propeller is a good example.

(a) 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. The engine certification would also address the safety 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.

(b) Similarly, propeller certification would address the propeller functions. The functions and characteristics that the propeller applicant defines that are to be provided by the ECS would normally need to be refined by flight test. The propeller applicant would 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.

(2) An aircraft computer performing the functions for the control of the engine is also a good example.

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

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

e. **Design change control**. The EEC SICP should describe the design change control system the applicant established to support post-certification activity. This design change system should ensure that changes to any control element integrated into the EECS are evaluated by all design approval holders of that integrated system.

APPENDIX 1. REFERENCES TO INSTALLATION (AND/OR OPERATING) INSTRUCTIONS

The following is a list of all paragraph references in this AC to information that must be documented, if applicable, in the installation or operating instructions required by § 33.5. This list is provided as an aide to applicants.

Table A1-1. Paragraph References.

AC Chapter/Paragraph number	Brief Description
1-2a.	Functions that are added to the EECS that are not required for compliance with part 33, but are required for installation compliance.
1-4	Installation and operational assumptions for the target application and any installation limitations or operational issues must be noted.
4-1	*Rule:* Environmental limits to which the system has been qualified must be documented.
4-2d.(1)	HIRF and lightning test levels must be declared for engine type certification and documented in the engine installation instructions.
4-2d.(1)(b)	Wire shields, connectors, etc. required for HIRF and lightning protection when the engine is installed on the aircraft.
4-2d.(1)(e)	Same requirements for Reciprocating engines when using alternate levels. These are listed in the subsequent paragraphs.
5-1	*Rule:* 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.
5-2a.(2)	Show that all declared dispatchable control modes are capable of performing their intended functions in the environmental conditions
5-2a.(5)	Any limitations on operations in alternate modes must be clearly stated.
5-2a.(6)	Descriptions of the functioning of the ECS operating in its primary and any alternate modes must be provided.
5-2a.(9)(b)	The loss of capability in some non-dispatchable modes such as operability in rain, hail, or bird ingestion should be documented or demonstrated.
5-2b.	Training modes must be described.
5-2d.(4)(f)	The power or thrust change associated with mode transition should be declared.
5-2d.(5)	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.
5-2d.(6)(b)	The intent and purpose of the cockpit annunciation must be clearly stated.
6-2e.(4)	The assumed reliability and interface requirements for non-engine type design elements must be documented.
6-2g.(4)(b)	If cooling provisions are required in the design of the EECS, the applicant must specify these provisions.
6-2i.(7)	The maximum safe design operating temperature for the components must be declared.
6-2i.(11)(b)	Where aircraft interface wiring is involved, applicant must inform the installer of the potential effects of shorts in the interface wiring.
7-2a.(4)	Identify the applicable assumptions and installation requirements and establish any limitations relating to ECS operation.

AC Chapter/Paragraph number	Brief Description
10-2c.(1)(b)	The installation and/or the operating instructions should identify data transfers and exchanges between engines, and between the airplane and engines, that could produce common mode faults.
10-2c.(4)	If the ECS relies entirely on aircraft air data to complete any of its critical control functions, then the engine applicant must require: • that the aircraft air data system is unaffected by a complete loss of aircraft generated power, and • that there be no common mode faults where multiple incorrect, but valid, signals are transmitted to the engine control.
10-2f.(3)	If an alternate mode, independent of aircraft-supplied data, has been provided, the applicant should document the characteristics of operation in this mode.
10-2g.	The engine applicant must document data or issues to allow the installer to ensure engine compliance as installed. These are listed in the subsequent paragraphs.
11-1	Rule: Identify all characteristics for any required aircraft power.
11-2a.(1)	Engine installation instructions should identify battery health, status, and maintenance requirements.
11-2a.(2)(b)	If aircraft power is a back-up power source, then applicants should provide detailed electrical system interface requirements in the engine installation instructions.
11-2c.(2)	As a part of the consideration regarding an aircraft single bus failure, The installation instructions may reference a wiring diagram.
11-2c.(3)	The maximum allowable failure event rate values should be declared
11-2c(4)(c)	Back up power used as a primary power source has specific requirements to assure that the EECS SSA assumptions are not violated
11-2d.(1)	Any aircraft-supplied power reliability values used in system analyses, whether supplied by the aircraft manufacturer or assumed must be included.
11-2d(4)(b)1	Design review and safety analysis requirements if aircraft power without a dedicated power source is to be used
11-2e.(1)	The ECS's electrical power supply quality requirements.
11-2f.(1)(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 and the time interval associated with this recovery must be documented.
11-2f.(1)(c)	The applicant should consider the effects of any aircraft electrical bus-switching transients or power transients in the engine installation or operating instructions.
11-2f.(2)	The power requirements necessary for in-flight engine restarts are defined.
14-2.	If the installer is to supply the fuel SOV, the applicant must state that a pilot initiated means for rapid shutdown of the engine must be provided by the installer.

In some instances these items may be documented in an Interface Control Document (ICD), also referenced in Section 16-2 c.(1). If an applicant wants to use the ICD as the means to document these facts, that may be possible. However, if that is the chosen method then the installation or operating instructions must reference the ICD and the ICD will need to be available to the Airworthiness Authorities and the installer.

APPENDIX 2. CERTIFICATION AIDS

The following are some document subjects commonly submitted with certification packages. Engine control system certification programs may vary. Not all documents in this list will apply to all programs, and this list is by no means, all inclusive.

Table A2-1.
Certification Aids.

Submitted Document	Major Sections	AC Chapter Reference	Part 33 Section Number
Installation and/or Operating Instructions	• Requirements • Procedures • Limitations • Assumptions Also refer to Appendix 1	1	33.28
Declared Component/System Environmental Limits	• Electrical • Physical	4	33.28(b)(2)
Component/System Environmental Test Plans and Test Reports (Electrical)	• HIRF • Lightning • EMI • TLD Environmental Tests	4	33.53 33.91 33.28(b)(2)
ICA's (as specified in AC 33.4-3)	• Maintenance Actions	4	33.28(b)(2)
Component/System Environmental Test Plans and Test Reports (Physical)	• Thermal • Vib • Shock • etc	4	33.53 33.91 33.28(b)(2)
Control Modes	• Documentation • Tests • Analysis • Backup availability	5	33.28(c)
Reliability Assessment Plan		6	33.28(d)
LOTC/LOPC Analysis	(May be a sub-set of the SSA)	6	33.28(d)
Commercial or Industrial Grade Electronic Parts Assessment		6	33.28(d)
Single Fault Accommodation Analysis		6	33.28(d)
Local Events Analysis		6	33.28(d)
System Safety Analysis	• Full-up System • Degraded System • Protective Functions/Systems	7	33.28(e)

Submitted Document	Major Sections	AC Chapter Reference	Part 33 Section Number
Plan for Software Aspects of Certification (ref. RTCA/DO-178C)	NOTE**:** Applicants should prepare all remaining Software Design Assurance documents as specified in RTCA/DO-178B and have them on file and available for FAA audit.	9	33.28(g)
Software Configuration Index (ref. RTCA/DO-178C)		9	33.28(g)
Software Accomplishment Summary (ref. RTCA/DO-178C)		9	33.28(g)
Aircraft-Supplied Data Analysis	• Design Assessment • Validation	10	33.28(h)
Aircraft-Supplied Power Analysis	• Design Architecture Analysis • Validation	11	33.28(i)
Air Pressure Signals Analysis	• Design Analysis	12	33.28(j)
Plan for Hardware Aspects of Certification (ref. RTCA/DO-254)	NOTE: Applicants should prepare all remaining Hardware Design Assurance documents as specified in RTCA/DO-254 and have them on file and available for FAA audit.	15	33.28(m)
Hardware Configuration Management Records (ref. RTCA/DO-254)		15	33.28(m)
Hardware Accomplishment Summary (ref. RTCA/DO-254)		15	33.28(m)
EEC System Integration Certification Plan (SICP) (if applicable)	• Distribution of Compliance Tasks • Interface Definition & Other Data • Design Change Control	16	33.28

APPENDIX 3. RECIPROCATING ENGINE EECS SSAs

A reliability and safety analysis can show that the applicant's system design meets its intended purpose. Two key terms that are used when evaluating system safety are "single-fault tolerant" and "unsafe condition." Refer to chapter 11 of this AC for a discussion of ECS failures and, in particular, the subject of single-fault tolerance.

a. Unsafe condition. Engine power loss events are not typically considered unsafe conditions when evaluating airplane safety. However, if the frequency of these events is excessive relative to the safety objectives of the intended application, then they may be considered unsafe conditions. Consequently, engine power losses and shutdowns are included in the following failure conditions and categories that are considered unsafe conditions for reciprocating engines:

(1) Destructive events (DE).

(2) Excessive number of LOPC events.

(3) Excessive number of MPL events.

b. Continued operations

(1) Section 33.28 does not specifically address continued operations when faults are present in the EECS. However, service experience indicates that to be economically feasible, EECS-equipped engines must be permitted to operate for limited time periods with faults present in the system (that is, permitted to operate in a degraded state). In addition, a thorough system safety analysis includes all the components of the control system, including the mechanical components.

(2) To address these issues as well as meet the intent of the rule, the FAA has developed a method for demonstrating compliance for reciprocating engines that allows for operation with certain faults (that is, in a degraded state). This method consists of an ECS safety analysis with both quantitative and qualitative elements. The quantitative element compares the predicted number of failure events of the electrical or electronic components, with established criteria that represents unsafe conditions. Both full-up and degraded configurations are evaluated, but those degraded system configurations that are found acceptable are limited to 20 hours of operation. Mechanical component reliability is evaluated through the test and analyses required by §§ 33.19, 33.49, and 33.53. The qualitative elements provide an evaluation of the entire ECS.

(3) Instead of addressing all forms and levels of safety analyses, the FAA has developed a method for demonstrating compliance that meets the intent of § 33.28(e) and ensures an acceptable level of safety. The applicant may use a different method of showing

compliance. Alternative methods should be presented to the FAA for review and approval as early in the project as possible.

(4) The applicant may submit an EECS SSA to comply with § 33.28. The method of showing compliance described in this appendix allows for FAA approval of time-limited flight operations with certain reciprocating engine EECS faults. We derived a time limit of 20 hours from the unsafe condition criteria established for a degraded EECS. This 20 hour limit ensures that the engine maintains an acceptable reliability level during this type of operation.

c. **EECS SSA: General**. The EECS SSA includes a quantitative element that is intended to evaluate the predicted reliability of the components of the EECS, and to compare it to the system safety criteria included in this AC. The EECS SSA also includes a qualitative element that provides an evaluation of certain aspects of the EECS.

(1) The EECS SSA quantitative analysis will determine the instantaneous failure event rates in both the full-up system and degraded system. These event rates are then compared to the unsafe condition criteria for both full-up and degraded systems. The quantitative analysis may consist of the following analyses:

(a) Numerical FTA,

(b) FMEA, and

(c) Markov or similar type of analysis to evaluate the EEC system in a degraded condition.

(2) The EECS SSA qualitative analysis consists of design appraisals of certain aspects of the EECS. The qualitative analyses may include the following reports:

(a) Alternate control mode(s) characteristics,

(b) Control mode transition (refer to Chapter 5 of this AC),

(c) EECS output data content,

(d) Existing subsystems,

(e) Local events test or analysis (refer to Chapter 6 of this AC), and

(f) Commercial, automotive, or industrial grade electronic parts analysis (refer to Chapter 6 of this AC).

d. **EECS SSA assumptions**. The applicant should include in the EECS SSA, an explanation of any assumptions it made regarding airplane installation and operating conditions. The applicant’s assumptions should be consistent with it’s data in the ICAs and the engine installation or operating instructions. The applicant’s assumptions may include the following:

(1) Maintenance actions and associated intervals,

(2) Airplane systems or equipment response,

(3) Powerplant installation design and environment, and

(4) Latent failure exposure period.

e. **EECS SSA quantitative analysis**. The quantitative analysis is intended to supplement, but not replace, qualitative methods based on engineering and operational judgment and experience. In general, the depth and scope of an acceptable safety analysis depend on the complexity and criticality of the functions performed by the system, and can vary considerably for different types of systems. Because this analysis is limited to reciprocating engine electronic control systems, the criteria provided in this appendix are more specific. The quantitative analysis should encompass all elements of the control system: electrical or electronic, and mechanical.

(1) **EECS SSA safety criteria**. This appendix provides safety criteria, expressed in terms of events per million hours, for full-up and degraded configurations. The applicant may propose different criteria. However, if the applicant does so, the applicant should show that it's different criteria provide an equally effective method of meeting the safety criteria.

(a) The safety criteria is provided for each of the two typical reciprocating engine control subsystems (fuel and ignition), and also for any other subsystem. This accommodates varying degrees of system functionality by increasing the allowable failure event rates as subsystems or functions are added to the total system definition. Once the total number of subsystems is defined and the associated maximum failure event rates are calculated, the applicant's failure rates should be allocated across the total system and not to the individual subsystems. The failure event rates of tables A3-1 and A3-2 are consistent with FAA safety objectives for reciprocating engines.

(2) **Full-up system analysis methods**. The applicant may use this analysis to confirm that the full-up system meets the system safety criteria specified in table A3-1. We recommend that the applicant performs a numerical FTA and an FMEA, and that the applicant includes all engine parts in each.

(a) Each of the system elements in table A3-1 is additive. "Other" applies to each subsystem. For example, an EECS comprised of fuel, ignition, and wastegate control functions should meet a total system reliability of 15+15+15= 45 LOPC events per million hours (and 450 MPL events per million hours). This criteria is then applied to the entire system and not allocated to each of the subsystems.

(b) The applicant should limit the maximums to 45 LOPC and 450 MPL events per million hours, regardless of the number of subsystems. For example, if the EECS includes more than three subsystems, the sum of the LOPC rates for the total system should not exceed 45

LOPC or 450 MPL events per million hours for all of the electrical and electronic elements. Finally, the applicant should apply the event rates in table A3-1 to the highest appropriate system or subsystem level and not to individual components of the same system.

(3) **Degraded system analysis methods and criteria**. The applicant may use this analysis to confirm that the degraded system meets the system safety criteria of table A3-2 with existing fault(s), or with time limited operations. If the existing fault(s) does not affect engine operability and the criteria of table A3-2 are met, then Time-Limited Operations (TLO) may be approved for these fault conditions. The analysis determines the instantaneous failure rate with one or more failures in the system. A Markov analysis, or channel failure analysis for simple systems, may be used.

f. **Time-limited operations (TLO) implementation requirements**. The EEC SSA should include the following:

(1) The applicant should group all EECS faults into one of the following three operating limitations categories:

(a) No take-off (NTO). Faults in this category preclude departure. These faults are total system faults that result in calculated event rates that exceed the degraded system limits, or when the total system has insufficient resources to properly operate the engine. These system faults are defined as NTO faults.

(b) TLO. TLO faults permit operations up to 20 hours, and preclude them thereafter. These faults are also system faults that result in calculated event rates that exceed the full-up system limits but which are less than the degraded system limits. Also, the system LOPC and MPL rates are not generally greater than 450 and 4500 events per million flight hours, respectively. These system faults are defined as TLO faults.

(c) Unlimited operation (ULO). ULO faults are system faults where the calculated event rates are less than the full-up system limits (this may also apply to degraded system with certain minor faults).

(2) The applicant should ensure that its EECS design provides separate cockpit indications for TLO faults and NTO faults, such as:

(a) Indicator lights, codes, etc., and

(b) Confirmation of indicator function during the pre-flight check.

(3) The applicant should also specify engine airworthiness and operating limitations for TLO faults, NTO faults, and ULO faults, in the TCDS and STC limitations sections, the Instructions for Continued Airworthiness Limitations Section, and the Engine installation and/or operating instructions. The applicant should also include maintenance actions information associated with EECS faults in the troubleshooting procedures of the engine maintenance manual.

(4) The installer should publish limitations in the Airplane Flight Manual or Pilot Operating Handbook.

TABLE A3-1. Full-Up System Safety Criteria. Electrical or Electronic Components (Events per Million Hours)

	Subsystem Maximum			**Total System Maximum**
Failure Condition	**Ignition**	**Fuel**	**Other**	**System**
Destructive Event	<0.001	<0.001	<0.001	<0.003
LOPC	15	15	15	45
MPL	150	150	150	450
No Effect (i.e., the fault does not affect the LOPC or MPL rate)			-	-

TABLE A3-2. Degraded System Safety Criteria. Electrical or Electronic Components (Events per Million Hours)

	Subsystem Maximum			**Total System Maximum**
Failure Condition	**Ignition**	**Fuel**	**Other**	**System**
Destructive Event	<0.001	<0.001	<0.001	<0.003
LOPC	150	150	150	450
MPL	1500	1500	1500	4500
No Effect			-	-

g. **EECS SSA qualitative analysis**. Your Qualitative analysis should include the mechanical, electrical, and electronic components. It should also include the following sections:

(1) **Alternate control mode analysis**. Refer to Chapter 5 of this AC for guidance on alternate mode analysis.

(3) **EECS output data analysis**. The applicant's reciprocating engine EECS SSA should include information about faults or failures that could cause the transmission of faulty or drifting engine parameters to aircraft systems. It should also include a prediction of the rates of occurrence of those faults or failures. The following engine output parameters are examples of parameters that this analysis could address:

(a) Oil pressure,

(b) Engine speed,

(c) Manifold pressure,

(d) Cylinder head temperature,

(e) Turbine inlet temperature,

(f) Exhaust gas temperature,

(g) Calculated engine power parameters (horsepower or torque, etc.),

(h) Combustion pressure, and

(i) Engine detonation (sometimes called knock).

(4) **Existing subsystems analysis**. The applicant's reciprocating engine EECS SSA should include an evaluation of the functional interaction of any existing mechanical control system elements that remain on the engine after incorporation of the EECS or subsystem. The existing subsystems analysis should:

(a) Analyze existing mechanical subsystems such as carburetors, magneto ignition, turbo mechanical wastegates, and mechanical fuel injection,

(b) Identify interface and installation requirements related to existing mechanical systems or components, and

(c) Analyze the effects on the EECS of failures of these mechanical systems.

(5) **Local events analysis**. Refer to Chapter 6 of this AC for guidance on Local Event Analysis.

(6) **Guidance for use of commercial or industrial grade electronic parts**. Refer to Chapter 6 of this AC for guidance on Commercial and Industrial Grade Electronic Parts analysis.

APPENDIX 4. RELATED REFERENCES

The following references are related to this AC:

A4-1. **Related Regulations in 14 CFR**. Sections 23.901, 23.903, 23.909, 23.1309, 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, 33.35, 33.49, 33.53, 33.65, 33.66, 33.67, 33.69, 33.73, 33.75, 33.91, and Appendix A of part 33.

A4-2. **FAA ACs, Orders, & Policy**. Use latest revision available.

AC 20-115C, RTCA, Inc. Document RTCA/DO-178C, July 19, 2013.

AC 20-136B, Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning, September 7, 2011.

AC 20-152, RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware, June 30, 2005.

AC 20-158, The Certification of Aircraft Electrical and Electronic Systems for Operation in the High-Intensity Radiated Fields (HIRF) Environment, July 30, 2007.

AC 20-174, Development of Civil Aircraft and Systems, September 30, 2011.

AC 21-16G, RTCA, Inc. Document RTCA/DO-160 versions D, E, F, and G, Environmental Conditions and Test Procedures for Airborne Equipment, June 22, 2011.

AC 33-2B Aircraft Engine Type Certification Handbook, June 30, 1993.

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

AC 33.17-1A, Engine Fire Protection § 33.17, August 3, 2009.

AC 33.91-1, Engine System and Component Tests, December 9, 2010.

AC 20-171, Alternatives to RTCA/DO-178B for Software in Airborne Systems and Equipment, January 19. 2011.

A4-3. The following Orders and Policy are referenced for completeness and are not requirements for the applicants showing of compliance.

a. **FAA Orders and Policy**

Order 8110.49 CHG 1, Software Approval Guidelines, September 28, 2011.

Order 8110.105 CHG 1, Simple and Complex Electronic Hardware Approval Guidance, September 23, 2008.

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.

Policy Letter PL-45, Time Limited Dispatch (TLD) Authorization for Full Authority Digital Electronic Control (FADEC) Engines, Rev 2, March 4, 2004 (available at http://www.opspecs.com/).

Policy Memorandum, PS-ACE100-2004-10024, Installation of Electronic Engine Control for Reciprocating Engine, November 18, 2004.

b. European Aviation Safety Agency (EASA) Orders and Policy.

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.

A4-4 Industry Documents.

a. International Electrotechnical Commission (IEC) Documents.

IEC/TS 62239-1, Process Management for Avionics – Preparation of an Electronic Components Management Plan, 2012-07.

IEC/TR 62240-1, Process Management for Avionics – Use of Semiconductor Devices Outside Manufacturers' Specified Temperature Ranges, First edition 2005-06.

b. RTCA Documents.

RTCA/DO-178A, Software Considerations in Airborne Systems and Equipment Certification, March 22, 1985.

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

RTCA/DO-178C/EUROCAE ED-12C, Software Considerations in Airborne Systems and Equipment Certification, December 13, 2011.

RTCA DO-330, Software Tool Qualification Considerations, December 13, 2011.

RTCA DO-331, Model-Based Development and Verification Supplement to DO-178C and DO-278A, December 13, 2011.

RTCA DO-332, Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A, December 13, 2011.

RTCA DO-333, Formal Methods Supplement to DO-178C and DO-278A, December 13, 2011.

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

RTCA/DO-160G/EUROCAE ED-14G, Environmental Conditions and Test Procedures for Airborne Equipment, December 8, 2010/May 2011.

c. **SAE International Documents**.

SAE ARP4754A, Guidelines for Development of Civil Aircraft and Systems, December 21, 2010.

SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, December 1996.

SAE ARP5107B, Guidelines for Time Limited Dispatch (TLD) Analysis for Electronic Engine Control Systems, November 15, 2006.

SAE ARP5415A, Users Manual for Certification of Aircraft Electrical/Electronic Systems for the Indirect Effects of Lightning, February 16, 2008.

SAE ARP5416A, Aircraft Lightning Test Methods, January 7, 2013.

SAE ARP5583, Guide to Certification of Aircraft in a High Intensity Radiated Field (HIRF) Environment, June 4, 2010.

SAE ARP5757, Guidelines for Engine Component Tests, March 2008.

SAE ARP5890A, Guidelines for Preparing Reliability Assessment Plans for Electronic Engine Controls, February 3, 2011.

A4-5 Military Specifications.

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

MIL-STD-810G, Test Method Standard for Environmental Engineering Considerations and Laboratory Tests, October 31, 2008.

MIL-E-5007D, Engines, Aircraft, Turbojet and Turbofan, General Specification For, December 27, 1995.

A4-6. **Reference Addresses**. The following addresses are provided to aid in accessing some of the reference documents.

EASA: www.easa.eu.int.

FAA: www.faa.gov.

IEC: IEC, Central Office, 3, rue de Varembé, P.O. Box 131, CH - 1211 GENEVA 20, Switzerland. They are also available online at www.iec.org.

RTCA: RTCA, Inc. 1150 18th Street, NW, Suite 910, Washington, DC 20036. Also available online at www.rtca.org.

SAE: SAE World Headquarters, 400 Commonwealth Drive, Warrendale, PA 15096-0001 USA. Also available online at www.rtca.org .

EUROCAE: EUROCAE, 102, rue Etienne Dolet, 92240 Malakoff, France. Also available online at www.eurocae.net.

Military Specifications: Available online at http://dodssp.daps.dla.mil

APPENDIX 5. DEFINITIONS

For the purposes of this AC, the following definitions apply:

Airborne Electronic Hardware (AEH). Examples include line replaceable units, circuit board assemblies, application specific integrated circuits, and programmable logic devices.

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 or propeller control system.

Alternate Mode. Any control mode that is not the primary mode.

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), Markov analysis, similarity analysis and loss of thrust control or loss of power control analysis.

Automatic Power Reserve (APR) System. The entire automatic system used only during takeoff, including all devices both mechanical and electrical that sense engine failure, transmit signals, actuate fuel controls or power levers on operating engines, including power sources, to achieve the scheduled power increase and furnish cockpit information on system operation.

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.

Backup Mode. The backup 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 backup modes under the definition.

Backup System. A part of the engine or 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 that may involve evaluation in the aircraft.

Covered Fault. A fault that is detected or accommodated or both.

Demand Control Pump. A fuel pump whose output is variable and not directly proportional to engine rotor speed.

Destructive Event. Any malfunction or failure of the EEC system that may result in a condition in which the engine, or any of its components, causes physical damage to the airplane structure or its occupants that may affect continued safe operation of the airplane. Examples include engine separation from its mounts, uncontrolled fire, inability to shutdown the engine, generation of toxic products, or uncontained high-energy debris.

Dispatchable Configuration. All control system configurations approved for flight 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 active 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.

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.

Erroneous data. Data that appears to be valid, but is incorrect.

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. An occurrence that affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of function and malfunction). Note: errors may cause failures, but are not considered to be failures.

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. A manifestation of an error in a component, part, element, or system that may lead to a failure.

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 loss of thrust (or power) control rate.

Local Events. Failures of aircraft systems and components, other than the EECS, that may affect the installed environment of the EEC unit.

Loss of Power Control (LOPC). A ECS failure event resulting in the inability to attain at least 85% of rated power or to modulate power under normal operating conditions.

Loss of Thrust Control (LOTC). An ECS failure event on a turbine engine that results in the inability to attain at least 90% of rated thrust or to modulate thrust under normal operating conditions.

Minor Power Loss (MPL). A reciprocating engine ECS failure event resulting in the ability to attain less than 95%, but still greater than 85%, of rated power.

Primary Mode. The mode for controlling the engine under normal operation; often referred to as the ‘normal mode.

Primary System. The part of the ECS/PCS 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). These devices are a subset of AEH.

Propeller Control System (PCS). Any system or device that is part of the propeller type design that controls, limits, or monitors propeller operation.

Redundancy. Multiple independent methods incorporated within a system to accomplish a given function.

Time-Limited Operations (TLO). The duration of reciprocating engine flight operations permitted with the EEC system in a degraded condition.

Uncovered Fault. A fault or failure for which either no detection mechanism exists or, if detected, no accommodation exists.

Unsafe Condition. For the purposes of this AC, any malfunction or failure of a reciprocating engine EECS that could result in a destructive event or EECS LOPC and MPL rate in excess of

those specified in Tables A3-1 and A3-2 of this AC. This definition is intended to apply to reciprocating engine EECS.

APPENDIX A-6. ADVISORY CIRCULAR FEEDBACK INFORMATION

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) complete the form online at https://ksn2.faa.gov/avs/dfs/Pages/Home.aspx or (2) emailing this form to 9-AWA-AVS-AIR-DMO@faa.gov

Subject: AC 33.28-6 Date: _____

Please check all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph _____ on page _____.

☐ Recommend paragraph _____ on page _____ be changed as follows:

☐ In a future change to this AC, please cover the following subject:
(Briefly describe what you want added.)

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by: _____ Date: _____

Telephone Number: _____ Routing Symbol: _____

FAA Form 1320-19 (10-98)