Federal Aviation Administration

Memorandum

Date: August 22, 2007

From: Acting Manager, Engine and Propeller Directorate, Aircraft Certification Service

To: SEE DISTRIBUTION

Prepared by: Jay Turnberg, ANE-110, (781) 238-7116 or jay.turnberg@faa.gov

Subject: **INFORMATION:** Policy for Electronic Propeller Control Systems, §§ 35.21 and 35.23 [Policy Number ANE-2007-35.23-1]

1. PURPOSE. The FAA has developed this policy to provide guidance for certifying a propeller with an Electronic Propeller Control System (EPCS). This guidance may also be used for the development of special conditions that the Administrator may find necessary to establish a level of safety for propellers with an EPCS equivalent to that established by the existing airworthiness standards for propellers with conventional control systems.

2. RELATED REGULATIONS.

   a. Section 21.16, Special conditions.

   b. Section 35.21, Reversible propellers.

   c. Section 35.23, Pitch control and indication.

3. RELATED DOCUMENTS.

   a. Policy Number ANE-2001-35.13-R0, Policy for Propeller-Level Failure Effects; March 12, 2003.

   b. Policy Number ANE-2002-35.15-R0, Policy for Propeller Safety Analysis; October 30, 2003.

   c. Policy Number 1999-33/35-R0, Policy for Rule and Advisory Material Development under Title 14 of the Code of Federal Regulations (14 CFR) Parts 33 and 35; May 24, 1999.

d. Advisory Circular (AC) 20-115B, RTCA, Inc. Document DO-178B, Software Considerations in Airborne Systems and Equipment Certification; January 11, 1993.

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

f. AC 20-152, RTCA, Inc. Document RTCA/DO-254. Design Assurance Guidance for Airborne Electronic Hardware; July 5, 2005.

g. AC 21-16E, RTCA, Inc. Document RTCA/DO-160E, Environmental Conditions and Test Procedures for Airborne Equipment; December 20, 2005.

h. AC 23.1309-1C, Equipment, Systems, and Installations in Part 23 Airplanes; March 12, 1999.

i. AC 33.4-3, Instructions for Continued Airworthiness; Aircraft Engine High Intensity Radio Frequency (HIRF) Lightning Protection Features; September 16, 2005

j. AC 33.28-1, Compliance Criteria for 14 CFR § 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems; June 29, 2001.

k. AC 33.28-2, Guidance Material for 14 CFR § 33.28, Reciprocating Engine, Electrical and Electronic Engine Control Systems; August 13, 2003.

l. FAA Order 8110.49, Software Approval Guidelines; June 2, 2003.

m. Special Conditions No. 35-001-SC, Hamilton Sundstrand Model NP2000 Propeller; June 27, 2000.

4. DEFINITIONS. The following definitions apply to this policy:

Airplane-supplied data. All data that is supplied by or via airplane systems and used by the EPCS.

Airplane-supplied electrical power. Any electrical power supplied by or via airplane systems and used by the EPCS.

Alternate mode. Any control mode, including back-up mode(s), that is not the primary mode used for controlling the propeller.

Back-up mode. A control mode of the back-up system.

Back-up system. A part of the EPCS in which the operating characteristics or capabilities of the propeller control differ sufficiently from the primary system that the operating characteristics or capabilities of the airplane, crew workload, or what constitutes appropriate crew procedures, may be significantly impacted or changed.

Control mode. Each defined operational state of the EPCS where the crew can exercise satisfactory propeller control.

Covered failure. A failure that is detected and/or accommodated.

Electronic propeller control system. A propeller 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 rotational speed and blade angle of the propeller within the flight envelope and operating limitations.

Engine-supplied data. All data supplied by or via engine systems and used by the EPCS. Engine-supplied data is a subset of airplane-supplied data.

Failure. An occurrence that affects the operation of a component, part, or element such that it can no longer function as intended—it includes both loss of function as well as malfunction. Errors that may cause failures, for example, software errors, are not considered failures.

Failure accommodation. The capability to mitigate, either wholly or in part, a failure condition.

Failure condition. A condition with a direct or consequential effect on the airplane or its occupants caused or contributed to by one or more failures.

Full-up configuration. An EPCS that has no known failures present.

Hazardous propeller effects. The following are considered hazardous propeller effects:

(1) Significant overspeed of the propeller.
(2) Development of excessive drag.
(3) Significant thrust in the direction opposite to that commanded by the pilot.
(4) Release of the propeller or any major portion of the propeller.
(5) Failure that results in excessive unbalance.
(6) Unintended movement of the propeller blades below the established minimum in-flight low-pitch position.

Major propeller effects. The following are considered major propeller effects for variable pitch propellers:

(1) Inability to feather the propeller (for feathering propellers).
(2) Inability to change propeller pitch when commanded.
(3) Significant uncommanded change in pitch.
(4) Significant uncontrollable torque or speed fluctuation.

Primary system. The part of the EPCS used for controlling the propeller under normal operation.

Primary mode. The mode that is intended to control the propeller under normal operation—often referred to as ‘normal mode.’

Propeller. Defined by the components listed in the type design.

Propeller control system. Any system or device within the propeller system that controls, limits, or monitors propeller operation and is necessary for the continued airworthiness of the propeller.

Propeller system. The propeller plus all the components necessary for its functioning, but not necessarily included in the propeller type design.

5. BACKGROUND.

a. The development of electronic technology and, in particular, digital electronic technology, for controlling constant speed propellers is relatively recent in commercial aviation history. In the past, an EPCS typically consisted of a mechanical governor that used electronic motors, instead of hydraulic or mechanical means, to drive pitch change actuation. Today, an EPCS normally consists of digital electronic control components that use software, electronic circuitry, and electro-hydraulic actuators to control the propeller. Today’s EPCS often incorporate additional functions such as failure monitoring, synchrophasing and beta scheduling. This addition of electronics to the control system may introduce new failure modes that can result in hazardous propeller effects. Propellers that use this electronic technology rely on the incorporation of special conditions as prescribed under § 21.16 and shown in the referenced Special Conditions No. 35-001-SC.

b. Certification issues for propellers that use an EPCS include:

- system safety
- possible loss of airplane-supplied electrical power
- possible loss of or incorrect airplane-supplied data
- environmental effects including lightning strikes and high intensity radiated fields (HIRF); and
- software and complex hardware validation, and system isolation.

Unless specifically noted, airplane-supplied power or data to the propeller includes engine-supplied power or data to the propeller.

6. CERTIFICATION OBJECTIVES FOR AN EPCS. The certification objectives apply to any system or component that controls, limits or monitors propeller functions.

a. Design and Validation. The propeller control system should be designed, constructed and validated to show that:

(1) The propeller control system, operating in normal and alternative operating modes and in transition between operating modes, performs the functions defined by the applicant throughout the declared operating conditions and flight envelope.

(2) The propeller control system functionality is not adversely affected by the declared environmental conditions, including temperature, electromagnetic interference (EMI), HIRF, and lightning. The environmental limits to which the system has been satisfactorily validated should be documented in a propeller installation and operation manual.

(3) A method is provided to indicate that an operating mode change has occurred if flight crew action is required. In such an event, operating instructions should be provided in a propeller installation and operation manuals.

b. System Safety Assessment. The propeller control system should be designed and constructed so that in addition to meeting the safety objectives of policy memorandum ANE-2002-35.15-R0:

(1) No single failure or malfunction of electrical or electronic components in the control system results in a hazardous propeller effect.

(2) Failures or malfunctions directly affecting the propeller control system in a typical airplane, such as structural failures of attachments to the control, fire, or overheat, do not lead to a hazardous propeller effect.

(3) The loss of normal propeller pitch control does not cause a hazardous propeller effect under the intended operating conditions.

(4) The failure or corruption of data or signals shared across propellers does not cause a hazardous propeller effect.

c. Software Design and Implementation. EPCS imbedded software should be designed and implemented by a method approved by the Administrator that is consistent with the criticality of the performed functions and that minimizes the existence of software errors. AC 20-115B, RTCA, Inc. Document DO-178B, “Software Considerations in Airborne Systems and Equipment Certification” provides an approved method.

d. Airplane-Supplied Data. The propeller control system should be designed and constructed so that the failure or corruption of airplane-supplied data does not result in hazardous propeller effects.

e. Airplane-Supplied Electrical Power. The propeller control system should be designed and constructed so that the loss, interruption or abnormal characteristic of airplane-supplied electrical power does not result in hazardous propeller effects. The power quality requirements should be described in the propeller operation and installation manual.

f. EPCS Installation and Operation Manual. The applicant should provide the installation and operation manual for the EPCS. The manual should contain an overall description, limitations, characteristics and authority in both normal operation and failure conditions; the range of control of other controlled functions; and the interface with the airplane and engine.

7. GUIDANCE FOR CERTIFICATION OBJECTIVES OF AN EPCS. This policy applies to all types of EPCS. For instance, these might be:

- hydro-mechanical with a limited authority electronic supervisor;
- single channel full authority propeller control with hydro-mechanical back-up;
- dual channel full authority electronic propeller control system with no back-up; or
- any other combination.

The electronic technology may be analog or digital. The EPCS includes any system or device that controls, limits or monitors propeller operation and is necessary for controlling the propeller and ensuring safe operation of the propeller within the limits declared by the applicant. The referenced advisory circulars AC 33.4-3, AC 33.28-1, and AC 33.28-2 provide additional guidance applicable to meeting the objectives for the certification of an EPCS.

a. Design and Validation.

(1) Control Modes and Transitions. The applicant should perform all necessary testing and analysis to ensure that all control modes function as intended.

(a) The primary or normal mode includes all control functions designed for the control of the propeller. These control functions may include governing, beta control, feathering, and the transitions between the various primary mode control functions. Operation in an alternate mode occurs for failure accommodation when EPCS moves from the primary mode to a backup mode.

(b) The applicant should describe the functioning of the EPCS system in its primary and any alternate modes in the propeller installation and operation manual. The applicant should also clearly state any limitations on operations in alternate modes in this manual.

(c) Analyses, testing, or both are necessary to substantiate that transferring operation to alternate modes has no unacceptable effect on propeller durability or endurance. The applicant may demonstrate the durability and reliability of the control system in all modes by component testing. Performing some portion of the propeller testing in the alternate mode(s) and during transition between modes can be used as part of the system validation.

(d) The applicant may use the propeller endurance test and functional tests defined in §§ 35.39 and 35.41 using the primary full-up configuration control system. The applicant, however, should demonstrate by test, or analysis based on test, that the propeller can meet the defined criteria when operating in any alternative or back-up control mode. Adding some portion to the propeller endurance test and functional test in the alternate or back-up mode(s), including transition between modes, can be used as part of system validation, if desired. The component testing of § 35.42 addresses the durability of the control system.

(2) Environmental Considerations. The use of general conditions, such as those of RTCA DO-160/EUROCAE ED-14, allows certification of the EPCS in a consistent manner

independent from any installation considerations. However, installation on some airplanes may require additional considerations. Therefore, the applicant and airplane manufacturer should coordinate with each other, as well as with the appropriate FAA certification offices, to ensure that the propeller installation is acceptable. Additional guidance is found in the referenced advisory circulars AC 20-136A and AC 20-152.

(3) Flight Crew Action. In general, the EPCS should transition to alternate modes automatically. However, systems in which pilot action is required to engage the back-up mode may also be acceptable. When pilot action is required, care should be taken to ensure that any reliance on manual transition does not pose an unacceptable operating characteristic, unacceptable crew workload, or require exceptional skill. If annunciation to the pilot is necessary, the type of annunciation should be appropriate with the nature of the transition. For example, when transition to an alternate mode of control is automatic and the only observable changes in operation of the propeller are different rotational speed settings, the annunciation is very different from when the pilot is required to take timely action to maintain control of the airplane.

b. System Safety Assessment. As specified in ANE-2002-35.15-R0, “Policy for Propeller Safety Analysis,” airplane-level failure classifications do not directly apply to propeller safety assessments because the airplane may have features that could decrease or increase the consequences of a propeller failure effect. Additionally, the same type-certificated propeller may be used in a variety of installations, each with different airplane-level failure classifications. The applicant should declare the type of airplane, such as a part 25 airplane or a part 23 single reciprocating engine airplane, on which the EPCS will be installed. The applicant should also establish that the propeller failure modes and rates for certification and testing are at or above the airplane-level failure classifications. Otherwise, the EPCS may not be of sufficient integrity for installation on the intended airplane. AC 23.1309 provides additional guidance for airplane-level failure classifications for part 23 airplanes.

(1) Hazardous Propeller Effect Failure Rates. The propeller safety analysis in policy ANE-2002-35.15-R0 specifies that the analysis should show that hazardous propeller effects are not predicted to occur at a rate in excess of that defined as extremely remote (probability of 10^{-7} or less per propeller flight hour). Policy ANE-2002-35.15-R0 provides additional guidance for individual failures and probabilities of this low order of magnitude. We note that a probability of 10^{-7} per propeller flight hour is not acceptable for some part 23 airplanes or for any part 25 airplanes. Those airplanes may require a rate of 1×10^{-9} or less per propeller flight hour. The applicant should establish the rate required per propeller flight hour based on the airplane installation early in the control development program. This will ensure that the airplane meets its certification requirements with the propeller installed.

(2) Major Propeller Effect Failure Rates. The propeller safety analysis in ANE-2002-35.15-R0 specifies that a summary should be made of all failures that could result in a major propeller effect along with the expected hourly failure rate of occurrence for those effects. ANE-2001-35.13-R0 provides further guidance on major propeller effects. The European Aviation Safety Agency (EASA) requires the rate of occurrence for each major propeller effect to be 1×10^{-5} (1 per 100,000) or less per propeller flight hour for validation to its Certification

Standards for Propellers. This policy adopts the EASA specified failure rate for major propeller effects. Therefore, the applicant should establish the rate required per propeller flight hour based on the airplane installation early in the control development program. This will ensure that airplane meets its certification requirements with the propeller installed.

(3) Single Failure Accommodation.

(a) The applicant should substantiate single failure specifications by a combination of tests and analyses. The intent is that single failures or malfunctions in the EPCS's components, in its fully operational condition and all declared dispatchable configurations, do not result in a hazardous propeller effect. In addition, in its full-up configuration the control system should be "essentially single fault tolerant" of electrical/electronic component failures. We recognize, however, that to achieve true single fault tolerance would require either a triplicated design approach or a design approach with 100% fault detection. Currently, systems are designed with dual, redundant channels or with back-up systems that provide what has been called an "essentially single fault tolerant" system. "Essentially single fault tolerant" then becomes a state of the art, or goal, for the applicant to strive for; it reflects that single fault tolerant has not been, and is not expected to be, achieved.

(b) The objective is to have all the faults addressed as covered faults. Indeed, the dual channel or back-up system configurations cover the vast majority of potential electrical and electronic faults. However, it may be appropriate for the applicant in certain cases to omit some coverage because detection or accommodation of some electrical/electronic faults is not practical. In these cases, we recognize that single, simple electrical or electronic components or circuits can be employed in a reliable manner and that requiring redundancy may not be appropriate. In these circumstances, failures in some single electrical or electronic components, elements or circuits may result in loss of control. Such systems are considered "essentially single fault tolerant" and are acceptable.

(4) Local Events. Local events normally affect only one propeller. Events that affect more than one propeller, such as HIRF, lightning and rain, are not normally considered local events. Examples of local events include:

- Overheat conditions
- Fires, and
- Fluid leaks or mechanical disruptions that could lead to damage to control system electrical harnesses, connectors, or the control unit(s).

(5) Back-up Systems. The propeller should have a back-up system, such as an overspeed governor, counter weights, pitch lock, or low pitch stop. Two categories of malfunction should be considered:

- those resulting from external causes such as engine failures and airplane flight conditions, and
- those caused by EPCS failures.

(a) The combined normal or primary propeller control and back-up system should be at least two failures removed from a potential hazardous propeller effect. For example, a single failure mode should not result in unintended movement below the in-flight low pitch position. In this case, a potential overspeed or high drag condition will only be possible as a result of the initial failure causing a low pitch command and an independent failure preventing the protection system from operating.

(b) The applicant should show by analysis that the hourly failure rate per occurrence of a control system failure condition from any cause in combination with failures of the appropriate back-up system that would result in a hazardous condition is 10^{-9} or less for part 25 airplanes. The failure rates for part 23 airplanes range from 10^{-7} to 10^{-9} or less. AC 23.1309-1C provides additional guidance for part 23 airplanes. The applicant should establish an overall hourly failure rate per occurrence for the intended installation to ensure that the propeller is installable.

(c) The probability of the protection system failing to operate when required should be approximately 10^{-4} or less per flight hour.

(6) Shared Data or Signals. In the exchange of data with the airplane, consideration in the design of the EPCS should be given to elimination of unacceptable common mode failures affecting the operation of more than one engine or propeller. Common failures that affect the EPCS that could hazard the airplane are generally unacceptable. In particular, the applicant should consider the following:

(a) Erroneous data received from the airplane or engine by the EPCS, if the data source is common to more than one propeller (for example, air data sources or synchronizing controls).

(b) EPCS system operating failures propagating via data links between propellers (for example, maintenance recording, common bus, cross-talk, auto-feathering, and Automatic Takeoff Power Control System (ATPCS) implementation).

(c) Loss or interruption of airplane data or electrical power used by the propeller control when caused by the failure of another propeller system.

(d) Exchange of data between propellers to implement control functions (for example, synchrophasing should be shown to incorporate authority limits to prevent unacceptable common mode loss of control).

c. Software Design and Implementation. For EPCSs that use software, the objective is to prevent software errors that would result in unacceptable effects on pitch, speed and torque, or any other unsafe condition. Approved methods for developing software comply with the guidelines of AC 20-115B, RTCA, Inc. Document DO-178B, Software Considerations in Airborne Systems and Equipment Certification. FAA Order 8110.49 establishes guidelines for approving software in compliance with RTCA/DO-178B. The applicant may propose alternative methods for developing software, such as legacy systems using RTCA documents

DO-178A/EUROCAE ED-12A with established guidelines in Order 8110.49. These methods are subject to approval by the FAA.

d. Airplane-Supplied Data. Airplane-supplied data includes all analog, discrete and digital data provided by the airplane systems to the EPCS. Engine-supplied data is a subset of airplane-supplied data. When airplane-supplied data can affect EPCS operation, the applicant should address the following items, as applicable, in the SSA or other appropriate documents:

(1) Software and complex electronic hardware in the data path to the EPCS should be at a level consistent with the criticality of the EPCS function that uses that data. The data path may include other airplane avionics.

(2) The installation and operation manual should state that the airplane applicant is responsible for ensuring that changes to airplane avionics units, including software, in the data path to the EPCS do not affect the integrity of the data provided to the propeller as defined by the EPCS installation and operation manual.

(3) The installation and operation manual should state that the installer should ensure that those sensors and equipment that deliver information to the EPCS are capable of operating in "severe" HIRF and lightning environments, as defined in the certification basis for the airplane, without affecting their proper and continued operation.

e. Airplane-Supplied Electrical Power. The objective of airplane-supplied electrical power is to provide an electrical power source to the EPCS that is at a minimum single failure tolerant. The most common method of achieving this objective has been to provide an independent alternator as the electrical power source for the EPCS. However, with the increased integration of propeller-airplane systems and with the application of EPCS to small propellers, both on reciprocating and turbine engines, use of an independent alternator may not necessarily be the only design approach to meet this objective. If airplane power failures can contribute to major or hazardous propeller effects, these events should be included in the SSA. The installation and operation manual should contain the assumed quality and reliability levels of airplane power. Engine-supplied power is a subset of airplane-supplied power.

f. EPCS Installation and Operation Manual**.**

(1) Control System Description. The applicant should include a brief control system description and may reference a more detailed system description document.

(2) Interface Description. The description should specify all the physical, electrical, and functional interface requirements of the control system. The following types of information should be included for EPCSs:

(a) EPCS power requirements and quality, including interrupt limitations;

(b) Impedance and buffering limitations for the signals provided by the EPCS for display and instrumentation;

(c) Signals used by the EPCS, such as air data information. This is to ensure that the EPCS is adequately isolated and unaffected by other systems using these signals;

(d) Subtle interface requirements, such as power interrupt tolerance of the EPCS; and

(e) Control system output information for maintenance and failure information;

(3) Operational Description. The applicant should include instructions for installing and operating the propeller that contain a description of the control system operating characteristics in both the normal and alternate control and operating modes.

(a) Restrictions in the flight envelope or unusual operating characteristics in these alternate modes should be clearly defined.

(b) Abnormal control characteristics that could have an impact on crew procedures, training, workload, or any other aspects of airplane performance and/or operating characteristics should be identified for evaluation during airplane certification.

(4) Substantiation Data. The applicant should include or reference data from safety analyses, environmental testing, and software level determinations that will assist the installer to safely install the propeller in the instructions for installing and operating the propeller.

(5) System Safety Analysis. The applicant should include the applicable assumptions, requirements and limitations from the SSA along with the estimated reliability of, or the failure rates for, significant failure conditions and the other control system associated events as determined from the SSA.

(6) Environmental Testing. The types and levels of environmental exposure for which the control system has been successfully qualified (for example, vibration, temperature, HIRF, or lightning) should be stated by the applicant. For the HIRF, lightning, and EMI qualification tests, the interfacing airplane cables used for the tests should be stated by the applicant.

(7) Software and Electronic Complex Hardware Validation and Verification. The documentation submitted in support of the software and complex electronic hardware aspects of certification should be stated by the applicant.

8. EFFECT OF POLICY. The general policy stated in this document does not constitute a new regulation or create a “binding norm.” Whenever an applicant’s proposed method of compliance differs from this policy, the proposal must be coordinated with the Engine & Propeller Directorate Standards Staff, ANE-110. In addition, if an office believes that an applicant’s proposal that meets this policy should not be approved, that office must coordinate its response with the Engine & Propeller Directorate Standards Staff, ANE-110.

//signed by Mark A. Rumizen//
Mark A. Rumizen
Acting Manager, Engine & Propeller Directorate
Aircraft Certification Service

DISTRIBUTION:
Manager, Aircraft Engineering Division, AIR-100
Manager, Aircraft Manufacturing Division, AIR-200
Manager, Certification Procedures Branch, AIR-110
Manager, Brussels Aircraft Certification Staff, AEU-100
Manager, Engine Certification Office, ANE-140
Manager, Engine Certification Branch, ANE-141
Manager, Engine Certification Branch, ANE-142
Manager, Boston Aircraft Certification Office, ANE-150
Manager, New York Aircraft Certification Office, ANE-170
Manager, Airframe and Propulsion Branch, ANE-171
Manager, Rotorcraft Directorate, ASW-100
Manager, Rotorcraft Standards Staff, ASW-110
Manager, Airplane Certification Office, ASW-150
Manager, Rotorcraft Certification Office, ASW-170
Manager, Special Certification Office, ASW-190
Manager, Small Airplane Directorate, ACE-100
Manager, Small Airplane Standards Office, ACE-110
Manager, Atlanta Aircraft Certification Office, ACE-115A
Manager, Airframe and Propulsion Branch, ACE-117A
Manager, Chicago Aircraft Certification Office, ACE-115C
Manager, Propulsion Branch, ACE-118C
Manager, Wichita Aircraft Certification Office, ACE-115W
Manager, Systems and Propulsion Branch, ACE-116W
Manager, Anchorage Aircraft Certification Office, ACE-115N
Manager, Transport Airplane Directorate, ANM-100
Manager, Transport Standards Staff, ANM-110
Manager, Airframe and Propulsion Branch, ANM-112
Manager, Seattle Aircraft Certification Office, ANM-100S
Manager, Propulsion Branch, ANM-140S
Manager, Denver Aircraft Certification Office, ANM-100D
Manager, Los Angeles Aircraft Certification Office, ANM-100L
Manager, Propulsion Branch, ANM-140L