

Engine Electronic Unit Fire and Overheat Design Guide

RATIONALE

The design and testing of the engine electronic unit's fire and overheat protection scheme is a critical task faced by the aerospace industry. It is fundamentally difficult to argue and demonstrate the safe operation of an engine electronic unit when subjected to fire, yet the design features introduced to address this issue must not jeopardize the safe operation of the engine that they control or monitor in normal operation. The aerospace industry has tried many varied approaches to reaching the right compromise in this difficult area and this guide highlights some of that experience that should aid the industry in general.

FOREWORD

Historical engine control systems for civil aircraft have employed hydromechanical controls. Where these operated in a designated fire zone or carried flammable fluids, they were subjected to appropriate fire tests to demonstrate safe behavior in the presence of fire. The advent of modern engine control systems, based around engine-mounted electronic control and monitoring units, has introduced previously unseen levels of system complexity and novel technology, yet the test standards applied to the engine control system to cover the threat of fire remain unaltered from those applied to hydromechanical systems. This design guide has been produced to aid the aerospace industry in its approach to the design and test of electronic units that are installed in designated fire or overheat zones and which must be shown to behave in a safe manner in the presence of fire or overheat threats.

TABLE OF CONTENTS

1.	SCOPE	4
1.1	Purpose	4
1.2	Field of Application	4
1.3	Document Format	4
2.	REFERENCES	4
2.1	Applicable Documents	4
2.1.1	SAE Publications	5
2.1.2	FAA Publications	5
2.1.3	EASA Publications	5
2.1.4	RTCA Publications	6
2.1.5	ISO Publications	6
2.2	Terms and Definitions	6
2.3	Abbreviations	7
3.	REQUIREMENTS FROM GUIDANCE MATERIAL	7
3.1	Aircraft Level	8
3.1.1	FAA Regulations and Advisory Material	8
3.1.2	EASA Certification Specification and Acceptable Means of Compliance	8

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2021 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
 Tel: +1 724-776-4970 (outside USA)
 Fax: 724-776-0790
 Email: CustomerService@sae.org
 http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE AIR6108

For more information on this standard, visit
<https://www.sae.org/standards/content/AIR6108/>

Documents

Document Sharing Hub

3.2	Engine Level	8
3.2.1	FAA Regulations and Advisory Material	8
3.2.2	EASA Specifications and Advisory Material	8
3.3	Component Level Considerations	9
4.	ENGINE HAZARDS ASSOCIATED WITH FIRE AND OVERHEAT	10
4.1	Fire and Overheat Requirements for Electronic Engine Control Systems	10
5.	FIRE AND OVERHEAT CONSIDERATIONS FOR NON-ELECTRONIC COMPONENTS	11
5.1	General	11
5.2	Harnesses and Connectors	11
5.3	Permanent Magnet Alternator (PMA)	11
5.4	Fuel Metering Unit (FMU)	11
5.4.1	Compressor Geometry Control	12
5.4.2	Fuel Shutoff Function	12
5.5	Bleed Valves	12
5.6	Ignition	12
6.	EEC FIRE AND OVERHEAT CONSIDERATIONS	12
6.1	Sources of Fire and Overheat Threats to EECs	12
6.1.1	Fire Zones	12
6.1.2	Overheat Threats	13
6.2	EEC Installation Locations	13
6.2.1	Proximity to Zone Ventilation Inlet	13
6.2.2	Proximity to Hot Air Sources	13
6.3	EEC Physical Considerations	13
6.3.1	EEC Internal Interconnect Faults	14
6.3.2	EEC Internal Fire and Overheat Failures	14
6.3.3	EEC Case Burn Through	14
6.3.4	EEC Solder Melt	15
6.3.5	EEC Burn-on/Violent Events	15
6.3.6	EEC Retention and Vibration Environment	16
6.4	EEC Installation Mitigations	16
6.4.1	Fire Shields	16
6.4.2	Intumescent Paint	17
6.4.3	Enhanced Thermal Management	17
7.	DESIGN STRATEGY OPTIONS	18
7.1	System Architectural and Installation Strategies	18
7.1.1	Avoidance of Fire and Overheat Threats	18
7.1.2	Creation of a Non-Fire Zone	19
7.2	Electronic Engine Control (EEC) Strategies	19
7.2.1	Segregation of Control and Protection Functions	19
7.2.2	Graceful Shutdown	20
7.2.3	Thermal Cut-Out of the EEC	22
7.2.4	EEC Temperature Measurement, Crew Alert, and Failsafe Command	23
8.	VERIFICATION OF COMPLIANCE	26
8.1	General Fire and Overheat Test Considerations	26
8.1.1	Engine Control System Test Modes	27
8.1.2	Test Equipment Fidelity	27
8.1.3	Build Standard	28
8.1.4	Vibration	28
8.2	Verification of Fire Compliance	28
8.2.1	General	28
8.2.2	Fire Test Conditions	28
8.2.3	Fire Pass Fail Criteria	30

8.3	Verification of Overheat Compliance	31
8.3.1	General.....	31
8.3.2	Overheat Test Conditions.....	31
8.3.3	Overheat Pass Failure Criteria	32
8.4	Overheat Protection System Design Substantiation.....	33
9.	NOTES	33
9.1	Revision Indicator	33

1. SCOPE

This SAE Aerospace Information Report (AIR) provides an overview of fire and overheat protection approaches that have been utilized for engine electronic units. While the electronic engine control (EEC) is the engine electronic unit specifically addressed in this document, the approaches presented can extend to any engine electronic unit, including monitoring units and other electronic based engine components.

1.1 Purpose

The purpose of this report is to help engineers in the design and test of engine electronic control systems that are required to behave in a safe manner in the presence of fire or overheat threats.

1.2 Field of Application

This document is written to address the fire and overheat requirements for engine electronic units installed on civil certified engines. While many military requirements are similar to civil requirements, this report describes the design considerations for type design of civil aeronautical products specific to the certification standards. The fire and overheat concepts presented here could be applied to any aerospace electronic control unit in designated fire or overheat zone. The document is not intended to cover spacecraft.

1.3 Document Format

This AIR contains the following sections:

Section 1 is an introduction to the document, giving its scope, field of application, and format.

Section 2 contains a list of references to other documents, terms, and definitions.

Section 3 discusses the applicable certification requirements, advisory circulars, and acceptable means of compliance.

Section 4 identifies the engine hazards that are to be addressed by the engine control system during fire and overheat events.

Section 5 identifies the engine non-electronic unit hazards and the resulting considerations for the EEC design and test with respect to fire and overheat strategies.

Section 6 identifies the unique fire and overheat considerations for an EEC along with potential mitigations to be incorporated in the complete fire and overheat strategies identified in Section 7.

Section 7 contains various EEC fire and overheat strategies that have been used in industry, including key tradeoff considerations.

Section 8 addresses the verification of compliance.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

ARP4754	Guidelines for Development of Civil Aircraft and Systems
ARP4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
ARP5757	Guidelines for Engine Component Tests

2.1.2 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

14 CFR Part 1	Definitions
14 CFR Part 23	Normal Category Airplanes
14 CFR Part 25	Transport Category Airplanes
14 CFR Part 27	Normal Category Rotocraft
14 CFR Part 29	Transport Category Rotocraft
14 CFR Part 33	Aircraft Engines
AC 20-135	Powerplant Installation and Propulsion System Fire Protection Test Methods, Standards and Criteria, with Change 1 Dated 10/11/2018
AC 33.17-1A	Engine Fire Protection
AC 33.28-3	Engine Control Systems
AC 33.91-1	Engine System and Component Tests
FAA Report	Standard Fire Test Apparatus and Procedure (for Flexible Hose Assemblies) No. 3A

2.1.3 EASA Publications

Available from European Union Aviation Safety Agency, Konrad-Adenauer-Ufer 3, D-50668 Cologne, Germany (for visitors and for mail over 1 kg) and Postfach 10 12 53, D-50452 Cologne, Germany (for mail 1 kg or less); Tel: +49 221 8999 000, www.easa.europa.eu.

AMC E 130	Fire Protection (Part of CS-E)
AMC-20	General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances
AMC-20-3	Certification of Engines Equipped with Electronic Engine Control Systems (Part of AMC-20)
CS-23	Certification Specifications for Normal, Utility, Aerobatic, and Commuter Aeroplanes
CS-25	Certification Specifications for Large Aeroplanes
CS-27	Certification Specifications for Small Rotocraft
CS-29	Certification Specifications for Large Rotocraft

CS-Definitions	Definitions and Abbreviations Used in Certification Specifications for Products, Parts and Appliances
CS-E 50	Certification Specifications for Engines, Engine Control Systems (Part of CS-E)
CS-E	Certification Specifications Engines

2.1.4 RTCA Publications

Available from RTCA, Inc., 1150 18th Street, NW, Suite 910, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

RTCA DO-160 Environmental Conditions and Test Procedures for Airborne Equipment

2.1.5 ISO Publications

Copies of these documents are available online at <http://webstore.ansi.org/>.

ISO 2685 Aircraft - Environmental Test Procedure for Airborne Equipment - Resistance to Fire in Designated Fire Zones

2.2 Terms and Definitions

FIREPROOF (as defined in AC 33.17-1A): The capability of a part or component to withstand, as well as or better than steel, a 2000 °F average flame temperature (± 150 °F individual thermocouple tolerance) for a minimum of 15 minutes, while still performing those functions intended to be performed when exposed to a fire.

FIREPROOF (as defined in CS-Definitions): With respect to materials, components, and equipment, fireproof means the capability to withstand the application of heat by a flame, for a period of 15 minutes without any failure that would create a hazard to the aircraft. The flame will have the following characteristics:

- Temperature: 1100 °C $\pm$ 80 °C
- Heat flux density: 116 kW/m² $\pm$ 10 kW/m²

For materials, this is considered to be equivalent to the capability of withstanding a fire at least as well as steel or titanium in dimensions appropriate for the purposes for which they are used.

NOTE: The flame characteristics above are per ISO 2685. Most U.S. test plans define flame characteristics per FAA Report Number 3A, which specifies similar but different flame characteristics (temperature: 2000 °F, heat flux: 4500 Btu/h) and calculation methods. The specific applicable publications, flame characteristics, and calculation methods should be clearly established with the certification authorities.

FIRE RESISTANT (as defined in AC 33-17A): The capability of a part or component to perform those functions intended to be performed while exposed to the heat and other conditions that are likely to occur at the particular location, and to withstand a 2000 °F average flame temperature (± 150 °F individual thermocouple tolerance) for a minimum of 5 minutes.

FIRE RESISTANT (as defined in CS-Definitions): With respect to materials, components, and equipment, fire resistant means the capability to withstand the application of heat by a flame, as defined for fireproof, for a period of 5 minutes without any failure that would create a hazard to the aircraft.

For materials, this may be considered to be equivalent to the capability of withstanding a fire at least as well as aluminum alloy in dimensions appropriate for the purposes for which they are used.

NOTE: AMC E 130 provides the rationale for the 5 minute fire resistance period: "The 5 minutes exposure which is associated with a 'fire resistant' status provides a reasonable time period for flight crew to recognize a fire condition, shut down the appropriate fuel shutoff valve(s). This cuts off the source of fuel."

GRACEFUL: As used in this document to describe system or engine response, this term indicates behavior that does not create an engine hazardous effect. Graceful response may occur due to a designed-in failure state, or a system's graceful accommodation action.

2.3 Abbreviations

AC	Advisory circular (FAA nomenclature)
AMC	Acceptable means of compliance (EASA nomenclature)
ARP	Aerospace recommended practice
CAS	Crew alerting system
CFR	Code of Federal Regulations (FAA nomenclature)
CS	Certification specification (EASA nomenclature)
EASA	European Aviation Safety Agency
EEC	Electronic engine control (i.e., the physical device)
EMI	Electromagnetic interference
FAA	Federal Aviation Administration
FADEC	Full authority digital engine control
FHA	Functional hazard analysis
FMEA	Failure modes and effects analysis
FMU	Fuel metering unit
IFSD	In-flight shut down
ISO	International Organization for Standardization
LOTC	Loss of thrust control
LRU	Line replaceable unit
PMA	Permanent magnet alternator
PRA	Particular risk assessment
PSSA	Preliminary system safety assessment
RTCA	RTCA, previously Radio Technical Commission for Aeronautics
SSA	System safety assessment

3. REQUIREMENTS FROM GUIDANCE MATERIAL

In addition to the design requirements flowing from safe aircraft operation considerations, the certification authorities have published certification standards and associated compliance guidance for the type design certification of engines and aircraft.

3.1 Aircraft Level

Ultimately the aircraft being the final product that can fly, the engine installation has to demonstrate that the aircraft complies with aircraft requirements including safe and reliable operations. Engine compartments are the most common sources of fire and overheat risks inherent to their controlled combustion, i.e., fuel burning. These risks are common to both reciprocating and gas turbine engine installations without regard to aircraft type or category.

3.1.1 FAA Regulations and Advisory Material

The Federal Aviation Administration (FAA), the civil aviation type design certification authority in the U.S., publishes the aircraft design standards as Parts of Title 14 of the Code of Federal Regulations (14 CFR). 14 CFR Part 1 defines “fire-proof” and “fire resistant.” Parts 23 to 29 have the same structure with a fire protection section in their Subpart E (Powerplant) and Subpart D (Design and Construction).

Each aircraft type design is divided in zones—designated fire zones, flammable fluids leakage zones, and dry zones that are subject to high temperatures under normal or failure conditions, such as adjacent to bleed air ducts or engines. The designated fire zones are isolated from the rest of the aircraft (including fuel tanks) by firewalls.

The FAA also publishes Advisory Circulars (AC) to provide interpretation and guidance as a means, but not the only means, to demonstrate compliance to the regulations contained in the 14 CFR Parts. Of interest is AC 20-135, which defines a standard flame to be used for component testing. Note that Change 1 to AC 20-135 contains revised guidance regarding the type of burner to be used for testing.

3.1.2 EASA Certification Specification and Acceptable Means of Compliance

The civil aviation type design certification authority in Europe since 2003 is the European Aviation Safety Agency (EASA).

Certification specifications (CS) 23, 25, 27, and 29 cover aircraft certification and the requirements are contained in the first part, called Book 1, each having a similar organization and content by section numbers as the corresponding 14 CFR Parts 23 to 29. Acceptable means of compliance (AMC) are contained in the second part of CS, called Book 2.

EASA also published General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliance as AMC-20. Of interest for this AIR is AMC 20-3, Certification of Engines Equipped with Electronic Engine Control Systems, which was published in December 2007 (amendment 2 of AMC-20).

3.2 Engine Level

Engine type designs are certificated separately from the aircraft.

3.2.1 FAA Regulations and Advisory Material

The FAA publishes the engine design standards as Part 33 of Title 14 of the CFR. Of interest, are sections 14 CFR 33.17, 33.28, 33.53, and 33.91.

FAA ACs guidance of interest are AC 33.17-1A, 33.28-3, and 33.91-1. AC 33.17-1A provides guidance and acceptable methods compliance to the associated engine fire protection regulations. This FAA advisory material is harmonized with EASA AMC E 130.

FAA AC 33.28-3 defines an overheat condition as follows: “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.”

3.2.2 EASA Specifications and Advisory Material

EASA publishes certification specifications for engines CS-E. The AMC E 130 gives the acceptable means of compliance, pass/fail criteria, and guidance for fire protection.

EASA AMC 20-3 defines an overheat condition as follows: “It is considered that an overheat condition exists when the temperature of the system components is greater than the maximum safe design operating temperature for the components, as declared by the engine applicant in the engine instructions for installation.”

NOTE: In the following discussion, the term “FADEC” is equivalent to “EEC” used elsewhere in this AIR.

It should be noted that EASA has applied program-specific certification review items (CRIs) at both the aircraft and engine level on the topic of “FADEC overheat and fire resistance.” The basic position taken by EASA in these CRIs can be summarized by the following points:

- The FADEC is often considered critical equipment and often performs both engine and aircraft functions; therefore, the compliance demonstration may need to involve both the aircraft and engine level regulatory authorities.
- The applicant should demonstrate, in deterministic and systematic manners, that in case of exposure to overheat or fire the FADEC system behavior will not induce any hazardous or catastrophic aircraft consequences.
- For demonstration of compliance, reliance exclusively on testing without additional engineering analysis is normally not an acceptable means of compliance. Testing alone does not allow a deterministic and systematic prediction of FADEC behavior in case of overheat or fire conditions.
- In addition to any fire or overheat tests, the compliance demonstration should rely on solid engineering, including system description and analysis of the behavior of the FADEC under the subject conditions.

3.3 Component Level Considerations

For EEC component level substantiation for fire and overheat, two areas of potential hazard are typically the focus of the design and regulatory compliance effort:

1. Support of combustion through the burning of the EEC constituent materials (fire exposure), and
2. EEC functional behavior during the fire or overheat exposure.

For fire testing, the component must first be categorized as either needing to be fireproof, fire resistant, or no fire requirement, depending on the component location and the function it performs. In a fire, the component could be constructed or located such that it serves as a fire wall, fire barrier, flammable fluid container, and/or part of the control system that must function during a fire. An analysis must be performed for each component to establish the fire test setup and operating conditions. This analysis must include an evaluation of the most critical operating conditions, the most vulnerable design feature on the component, the possible direction of the flame impingement, and the location of the flame impingement. When a fire test is conducted, the following acceptance criteria must be considered:

- Maintain the ability to perform the functions (e.g., fuel shutoff and fire detectors) intended to be provided in case of a fire within the time allowed.
- Post-test burning, either by combustion of the constituent material of the test article or by combustion of any flammable fluid leaking from the component. Post-test burning may be considered acceptable if it does not increase the overall fire hazard.

For overheat, the component must demonstrate the capability to operate per design intent or fail in a manner that does not result in hazardous engine effects when exposed to an overheat condition. Since it is often not possible to define the worst-case overtemperature conditions for an aircraft installation, a test to failure is usually implemented. Hazardous engine effects, as described in 14 CFR 33.75(g)(2), includes the inability to shut down, uncontrolled overspeeds, and may include other operating conditions. The overheat condition consists of exposure to ambient temperature above specified operating conditions which can be caused by a failure of some other engine or aircraft system and which could be sustained for an indeterminate time. The occurrence of an overheat condition must be detectable by the component or engine/aircraft system to support proper maintenance actions and associated return-to-service criteria.

When an overheat test is conducted, the following acceptance criteria must be considered:

- Proper detection of an overheat condition (if this is a required function of the component).
- The component must demonstrate the capability under overheat conditions to maintain engine shutdown capability where applicable, and not cause any hazardous engine effects.
- Maintenance actions required or allowed following an overheat event should be considered. If there are provisions in the instructions for continued airworthiness (e.g., line maintenance or repair shop maintenance) allowing the component to remain in service following certain overheat conditions, the demonstration must include validation of those provisions.

In addition to an overheat test, analysis of component functional behavior when exposed to faults or failures that can occur due to overheat exposure may be requested by certification authorities.

4. ENGINE HAZARDS ASSOCIATED WITH FIRE AND OVERHEAT

4.1 Fire and Overheat Requirements for Electronic Engine Control Systems

The relevant certification requirements for this include FAA 14 CFR part 33.28(d), EASA CS-E 50 (c)(3), (c)(4), and CS-E 1030(b)(3) (covering time limited dispatch). These require that engine protection systems meet the following criteria in all dispatchable configurations:

- Provide protection against hazardous engine events listed in 33.75(g)(2), in any dispatchable configuration, using appropriate trigger thresholds.
- Provide protection system actions that are compatible with aircraft in all flight phases, so that the airframer can comply with §§ 25.901, 25.903, and 25.1309 for transport category airplanes and similar rules for other aircraft categories.
- Meet § 33.75 safety analysis and § 33.28(d) LOTC/LOPC rates.
- Provide protection system self-test capabilities per § 33.28(f).
- Provide timely annunciation of protection system activation to aircraft for crew awareness per § 33.28(c)(iii).
- Provide the capability to recover after a protection system trigger event, after applicable self-test criteria are met post-event, per § 25.903(e).

The engine turbomachinery and control system designers should work with the aircraft designer early in a certification program, to evaluate the acceptability of protection system actions in all flight phases. Any potential false activation of protection systems should be carefully analyzed and steps should be taken to mitigate such occurrences. Analysis of potential false activation should include common mode events such as icing, fuel system behaviors, birdstrike, and EMI/HIRF/lightning.

Safe operation means that the EEC does not cause any of the hazards to occur that are listed in the functional hazard assessment (FHA) and in the preliminary system safety assessment (PSSA) for the propulsion system in question.

Hazardous engine effects are defined in certification requirements 14 CFR 33.75(g)(2) and CS-E 510(g)(2). Engine control system failures or malfunctions that can lead to these effects must be mitigated. The hazardous effects that are typically associated with the engine control system are: non-containment of high-energy debris, significant thrust in the opposite direction to that commanded by the pilot, and complete inability to shut the engine down.