Designation: F3061/F3061M − 16a

Standard Specification for Systems and Equipment in Small Aircraft[1]

This standard is issued under the fixed designation F3061/F3061M; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This specification covers international standards for the systems and equipment aspects of airworthiness and design for "small" aircraft.

1.2 The applicant for a design approval must seek the individual guidance of their respective CAA body concerning the use of this standard as part of a certification plan. For information on which CAA regulatory bodies have accepted this standard (in whole or in part) as a means of compliance to their Small Aircraft Airworthiness regulations (hereinafter referred to as "the Rules"), refer to ASTM F44 webpage (www.ASTM.org/COMMITTEE/F44.htm) which includes CAA website links.

1.3 The values stated in either SI units or inch-pound units are to be regarded separately as standard. The values stated in each system may not be exact equivalents; therefore, each system shall be used independently of the other. Combining values from the two systems may result in non-conformance with the standard.

1.4 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 Following is a list of external standards referenced throughout this document; the earliest revision acceptable for use is indicated. In all cases later document revisions are acceptable if shown to be equivalent to the listed revision, or if otherwise formally accepted by the governing civil aviation authority; earlier revisions are not acceptable.

2.2 *ASTM Standards:*[2]

F3066/F3066M Specification for Powerplant Systems Specific Hazard Mitigation
F3083/F3083M Specification for Emergency Conditions, Occupant Safety and Accommodations
F3116/F3116M Specification for Design Loads and Conditions

2.3 *Other Standards:*

14 CFR Part 23 Amendment 62 Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes
EUROCAE ED-107, Rev A Guide to Certification of Aircraft in a High-Intensity Radiated Field (HIRF) Environment
FAA-S-8081-14B, Change 5 Private Pilot Practical Test Standards for Airplane
RTCA/DO-178, Rev B Software Considerations in Airborne Systems and Equipment Certification
RTCA/DO-254 Design Assurance Guidance for Airborne Electronic Hardware
RTCA/DO-335 Guidance for Installation of Automatic Flight Guidance and Control Systems (AFGCS) for Part 23 Airplanes

2.4 *SAE Standards:*[3]

SAE AIR825/4, Rev A Chemical Oxygen Systems
SAE ARP4754, Rev A Guidelines for Development of Civil Aircraft Systems
SAE ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
SAE ARP5583, Rev A Guide to Certification of Aircraft in a High-Intensity Radiated Field (HIRF) Environment
SAE AS8017, Rev A Minimum Performance Standard for Anticollision Light Systems
SAE AS8037, Rev – Minimum Performance Standard for Aircraft Position Lights

3. Terminology

3.1 Terminology specific to this standard is provided below. For general terminology, refer to the Terminology standard referenced in Section 2.

[1] This specification is under the jurisdiction of ASTM Committee F44 on General Aviation Aircraft and is the direct responsibility of Subcommittee F44.50 on Systems and Equipment.

Current edition approved Aug. 1, 2016. Published September 2016. Originally approved in 2015. Last previous edition approved in 2016 as F3061/F3061M – 16. DOI: 10.1520/F3061_F3061M-16A.

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[3] Available from SAE International (SAE), 400 Commonwealth Dr., Warrendale, PA 15096, http://www.sae.org.

3.2 *Definitions of Terms Specific to This Standard:*

3.2.1 *aircraft type code, n*—an Aircraft Type Code (ATC) is defined by considering both the technical considerations regarding the design of the aircraft and the airworthiness level established based upon risk-based criteria. An ATC is expressed as an alphanumeric character string as illustrated in Fig. 1. An explanation of each character in the string is provided below.

3.2.1.1 *Discussion*—The first character in the Aircraft Type Code indicates the risk-based airworthiness level of the aircraft.

(1) A "1" indicates an airworthiness level corresponding to Level 1; this corresponds to seating for one or fewer passengers (excluding crew).

(2) A "2" indicates an airworthiness level corresponding to Level 2; this corresponds to seating for two or more passengers but no more than six (excluding crew).

(3) A "3" indicates an airworthiness level corresponding to Level 3; this corresponds to seating for seven or more passengers but no more than nine (excluding crew).

(4) A "4" indicates an airworthiness level corresponding to Level 4; this corresponds to seating for ten or more passengers but no more than nineteen (excluding crew).

3.2.1.2 *Discussion*—The second character in the Aircraft Type Code indicates the number of engines employed on the aircraft.

(1) An "S" indicates a single-engine aircraft.

(2) An "M" indicates a multiengine aircraft.

3.2.1.3 *Discussion*—The third character in the Aircraft Type Code indicates the type of engine(s) employed on the aircraft.

(1) An "R" indicates use of a reciprocating engine.

(2) A "T" indicates use of a turbine engine.

3.2.1.4 *Discussion*—The fourth character in the Aircraft Type Code indicates the stall speed of the aircraft.

(1) An "L" indicates a stall speed less than or equal to 83 km/h [45 knots].

(2) An "M" indicates a stall speed greater than 83 km/h [45 knots] but less than or equal to 113 km/h [61 knots].

(3) An "H" indicates a stall speed greater than 113 km/h [61 knots].

3.2.1.5 *Discussion*—The fifth character in the Aircraft Type Code indicates the cruise speed of the aircraft.

(1) An "L" indicates a cruise speed less than or equal to 463 km/h [250 knots] (or Mach ≤ 0.6).

(2) An "H" indicates a cruise speed greater than 463 km/h [250 knots] (or Mach > 0.6).

3.2.1.6 *Discussion*—The sixth character in the Aircraft Type Code indicates the allowed meteorological conditions of the aircraft.

(1) A "D" indicates an aircraft limited to Day VFR conditions only.

(2) An "N" indicates an aircraft limited to Day or Night VFR conditions only.

(3) A "I" indicates an aircraft certified for IFR operations.

3.2.1.7 *Discussion*—The seventh character in the Aircraft Type Code indicates the maximum operational altitude of the aircraft.

(1) An "L" indicates an aircraft with a maximum operational altitude equal to or less than 7620 m [25 000 ft].

(2) An "H" indicates an aircraft with a maximum operational altitude greater than 7620 m [25 000 ft].

3.2.1.8 *Discussion*—The eighth character in the Aircraft Type Code indicates the allowed flight maneuvers for the aircraft.

(1) An "N" indicates an aircraft that is limited to non-aerobatic maneuvers.

(2) An "A" indicates an aircraft that is certified for aerobatic maneuvers.

3.2.2 *BTPS, n*—BTPS stands for "Body Temperature and Pressure, Saturated." This is defined to be a temperature of 37°C and a pressure equal to the ambient pressure to which the body is exposed minus 6.27 kPa [47 mmHg]; this is the tracheal pressure displaced by water vapor pressure when the breathed air becomes saturated with water vapor at 37°C.

3.2.3 *catastrophic failure condition, n*—a catastrophic failure condition is one that would result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crew member, normally with the loss of the aircraft.

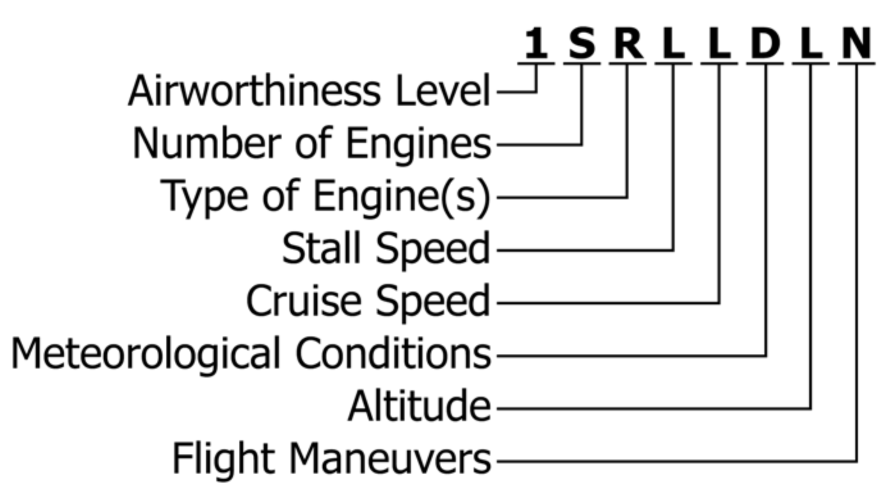

FIG. 1 Illustration of Aircraft Type Code

3.2.4 *chemical oxygen generator, n*—a chemical oxygen generator is defined as a device which produces oxygen by chemical reaction; for more detailed information, refer to SAE AIR 825/4.

3.2.5 *complex system, n*—A complex system is a system whose operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods or structured assessment methods, such as Failure Modes and Effects Analysis (FMEA) or Fault Tree Analysis (FTA). Increased system complexity is often caused by such items as sophisticated components and multiple interrelationships.

3.2.6 *continued safe flight and landing, n*—continued safe flight and landing is defined as the capability for continued controlled flight and landing, possibly using emergency procedures, but without requiring pilot skill beyond that needed to pass the Private Pilot Practical Test Standard for Airplane (refer to FAA-S-8081-14B), or requiring pilot forces beyond those defined in 14 CFR §23.143. Landing may occur either at an airport or at an emergency landing location consistent with established emergency procedures. Some aircraft damage may be realized, either during flight or upon landing.

3.2.7 *conventional system, n*—a conventional system is a system whose function, the technological means to implement its function, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly used.

3.2.8 *design appraisal, n*—a design appraisal is a qualitative appraisal of the integrity and safety of the system design. An effective appraisal requires experienced judgment.

3.2.9 *development assurance level, n*—a development assurance level is an indication of the level of those planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis.

3.2.10 *extremely improbable, n*—extremely improbable means that an event is considered so unlikely that it is not anticipated to occur during the entire operational life of all aircraft of one type.

3.2.11 *extremely remote, n*—extremely remote means that an event is not anticipated to occur to each aircraft during its total life, but may occur a few times when considering the total operational life of all aircraft of the type.

3.2.12 *failure condition, n*—a failure condition is a condition having an effect on the aircraft or its occupants or both, either direct or consequential, which is caused or contributed to by one or more failures or errors. The severity of a failure condition may be affected by flight phase, relevant adverse operational or environmental conditions, or other external events, or combinations thereof.

3.2.13 *hazardous failure condition, n*—a hazardous failure condition is one that would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be: a large reduction in safety margins or functional capabilities; physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or, serious or fatal injuries to a relatively small number of persons other than the flight crew.

3.2.14 *high speed, n*—an aircraft's performance level is considered High Speed if V_{NE} or V_{NO} is greater than 463 km/h [250 knots], or M_{MO} is greater than M0.6.

3.2.15 *installation appraisal, n*—an installation appraisal is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal industry-accepted installation practices should be evaluated.

3.2.16 *instrument, n*—the term instrument includes devices that are physically contained in one unit or component, and devices that are composed of two or more physically separate units or components connected together (such as a remote indicating gyroscopic direction indicator that includes a magnetic sensing element, a gyroscopic unit, an amplifier, and an indicator connected together).

3.2.17 *low speed, n*—an aircraft's performance level is considered low speed if V_{NE} or V_{NO} is less than or equal to 463 km/h [250 knots], or M_{MO} is less than or equal to M0.6.

3.2.18 *major failure condition, n*—a major failure condition is one that would reduce the capability of the aircraft or the ability of the flight crew to cope with adverse operating conditions to the extent that there would be: a significant reduction in safety margins or functional capabilities; a significant increase in flight crew workload or in conditions impairing the efficiency of the flight crew; discomfort to the flight crew; or, physical distress to passengers or cabin crew, possibly including injuries.

3.2.19 *minor failure condition, n*—a minor failure condition is one that would not significantly reduce aircraft safety, and which involves crew actions that are well within their capabilities. Minor Failure Conditions may include: a slight reduction in safety margins or functional capabilities; a slight increase in crew workload, such as routine flight plan changes; or, some physical discomfort to passengers or cabin crew.

3.2.20 *negligible failure condition, n*—a negligible failure condition is one that would have no procedural or operational effect on the flight crew as documented in the Airplane Flight Manual, or on the operation or capabilities of the aircraft; however, the event may result in an inconvenience to aircraft occupants.

3.2.21 *primary display, n*—primary display refers to the display of a parameter that is located such that the pilot looks at it first when wanting to view that parameter.

3.2.22 *primary function, n*—a primary function is a function that is installed to comply with applicable requirements for a required function and that provides the most pertinent controls or information instantly and directly to the pilot.

3.2.23 *primary system, n*—a primary system is a system that provides a primary function.

3.2.24 *probable, n*—probable means that the event is anticipated to occur one or more times during the entire operational life of each aircraft.

3.2.25 *qualitative analysis, n*—a qualitative analysis relies on analytical processes that assess system and aircraft safety in an objective, non-numerical manner.

3.2.26 *quantitative analysis, n*—a quantitative analysis relies on analytical processes that apply mathematical methods to assess the system and aircraft safety.

3.2.27 *redundancy, n*—the term redundancy refers to the presence of more than one independent means for accomplishing a given function. Each means of accomplishing the function need not be identical.

3.2.28 *remote, n*—remote means that the event is not anticipated to occur to each aircraft during its total life, but may occur several times when considering the total operational life of all aircraft of the type.

3.2.29 *secondary system, n*—a secondary system is a redundancy system that provides the same function as the primary system.

3.2.30 *similarity, n*—the term similarity refers to a condition where the equipment type, form, function, design, and installation have only minor differences to previously approved equipment. The safety and operational characteristics and other qualities of the new installation should have no appreciable effects on the airworthiness of the aircraft.

3.2.31 *simple system, n*—a simple system is a system that can be evaluated by only qualitative analysis and that is not a complex system. Functional performance is determined by combination of tests and analyses.

3.2.32 *single failure, n*—a single failure is considered to be any occurrence, or set of occurrences, that: cannot be shown to be independent from each other; affects the operation of components, parts, or elements of a system such that they can no longer function as intended; or, results in inadvertent system operation.

3.2.33 *STPD, n*—STPD stands for "Standard Temperature and Pressure, Dry." This is defined to be a temperature of 0°C and a pressure equal to 101.33 kPa (760 mmHg) with no water vapor.

3.2.34 *unsafe system operating condition, n*—an unsafe system operating condition is any system operating condition which, if not detected and properly accommodated by crew action, would significantly contribute to or cause one or more serious injuries.

4. Basic Information

NOTE 1—Table 1 provides correlation between various Aircraft Type Codes and the individual requirements contained within this section; refer to 3.2.1. For each subsection, an indicator can be found under each ATC character field; three indicators are used:

An empty cell ( ) in all applicable ATC character field columns indicates that an aircraft must meet the requirements of that subsection.

A white circle (○) in multiple columns indicates that an aircraft is exempt from the requirements of that subsection *only* if all such ATC character fields are applicable.

A mark-out (×) in any of the applicable ATC character field columns indicates that an aircraft is exempt from the requirements of that subsection.

Example—An aircraft with an ATC of 1SRLLDLN is being considered. Since all applicable columns are empty for subsection 4.1.1, that subsection is applicable to the aircraft. Since the "1" airworthiness level column, the "L" stall speed column, and the "D" meteorological column for subsection 4.1.6 all contain white circles, then that subsection is not applicable; however, for an aircraft with an ATC of 1SRMLDLN, subsection 4.1.6 would be applicable since the "M" stall speed column

TABLE 1 ATC Compliance Matrix, Section 4

Section	Airworthiness Level				Number of Engines		Type of Engine(s)		Stall Speed			Cruise Speed		Meteorological Conditions			Altitude		Maneuvers	
	1	2	3	4	S	M	R	T	L	M	H	L	H	D	N	I	L	H	N	A
4																				
4.1																				
4.1.1																				
4.1.2																				
4.1.3																				
4.1.4																				
4.1.5																				
4.1.6	○								○					○						
4.1.7																				
4.1.8																				
4.1.8.1																				
4.1.8.2																				
4.2																				
4.2.1																				
4.2.1.1		×	×	×						×	×				×	×				
4.2.1.2	○								○					○						
4.2.1.3	○								○					○						
4.2.1.4	○								○					○						
4.2.2	○								○					○						
4.2.2.1	○								○					○						
4.2.2.2	○								○					○						
4.2.2.3	○								○					○						
4.2.2.4	○								○					○						
4.2.2.5	○								○					○						
4.2.3	○								○					○						
4.2.3.1	○								○					○						
4.2.4									○					○						
4.2.4.1									○					○						
4.2.4.2									○					○						

does not contain a white circle. Subsection 4.2.1.1 would also not be applicable to the second aircraft, since it contains an × in the "M" stall speed column.

NOTE 2—The requirements of this chapter are applicable to all systems and equipment installed in the aircraft. These requirements are in addition to and do not supersede any additional system specific requirements identified elsewhere in these design standards or contained in the rules of the governing civil aviation authority.

4.1 *Function and Installation:*

4.1.1 Each item of installed equipment must be of a kind and design appropriate to its intended function.

4.1.2 Each item of installed equipment must be marked in a way that makes it clear to an installer the equipment's identification, function, or operating limitations, or any applicable combination of these factors. It is acceptable to reference equipment installation manuals for function or limitation information.

4.1.3 Each item of installed equipment must be installed according to limitations specified for that equipment.

4.1.4 Each item of installed equipment must function properly when installed.

4.1.5 The aircraft systems and equipment required for type certification or by operating rules must be designed and installed so that they perform as intended under the aircraft operating and environmental conditions.

NOTE 3—The intent of this requirement is to provide assurance that the required systems and equipment will function as intended in the expected operating and environmental conditions. It is recognized that random failures will occur throughout the aircraft life and that the failed device may no longer "perform as intended". The acceptability of such failures or combination of failures and their associated risks are addressed under the requirements of 4.2.

4.1.6 All aircraft systems and equipment must be designed and installed so that they do not adversely affect the safety of the aircraft or its occupants.

4.1.7 All aircraft systems and equipment must be designed and installed so that they do not adversely affect the proper functioning of those systems or equipment, or both, covered by 4.1.5.

4.1.8 Those systems and equipment not required for type certification or by operating rules are not required to perform their intended function under all aircraft operating and environmental conditions, provided that the resultant failure conditions are classified as "Negligible Failure Condition" in the assessment conducted per 4.2.1; refer to 3.2.20.

4.1.8.1 Non-required systems and equipment with failure conditions classified more severe than "Negligible Failure Condition" are not required to perform their intended function under all aircraft operating and environmental conditions, provided the failure is appropriately annunciated to the crew.

4.1.8.2 When addressing the requirements of 4.2, if any credit is taken for the installation, or any aspect, of these non-required systems, the portion of the system for which credit is taken must comply with 4.1.4.

4.2 *System Safety Requirements:*

4.2.1 An assessment of the aircraft and system functions must be performed to identify and classify the various Failure Conditions associated with each function; refer to 3.2.12. A Functional Hazard Assessment (FHA) in accordance with the methodology outlined in SAE ARP4761 is one means of performing this assessment; however, other simpler methodologies (for example, a design and installation appraisal) may be employed as appropriate to the complexity and criticality of the system(s).

4.2.1.1 The equipment, systems, and installations must be designed to minimize hazards to the aircraft in the event of a probable malfunction or failure.

4.2.1.2 The aircraft systems and associated components, considered separately and in relation to other systems, must be designed and installed so that each Catastrophic Failure Condition is "extremely improbable"; refer to 3.2.3 and 3.2.10.

4.2.1.3 The aircraft systems and associated components, considered separately and in relation to other systems, must be designed and installed so that each Hazardous Failure Condition is "extremely remote"; refer to 3.2.11 and 3.2.13.

4.2.1.4 The aircraft systems and associated components, considered separately and in relation to other systems, must be designed and installed so that each Major Failure Condition is "remote"; refer to 3.2.18 and 3.2.28.

4.2.2 Based on the results of the assessment per 4.2.1, the depth of analysis required to show compliance may be determined using Fig. 2 and the Assessment Levels defined in Table 2.

4.2.2.1 In showing compliance with the provisions of 4.2.2, for Negligible Failure Conditions (refer to 3.2.20), a design and installation appraisal to establish independence from other functions is necessary for the safety assessment. In general, common design practice provides physical and functional isolation from related components which are essential to safe operation.

4.2.2.2 In showing compliance with the provisions of 4.2.2, for Minor Failure Conditions (refer to 3.2.19), a design and installation appraisal to establish independence from other functions is necessary for the safety assessment. This appraisal should consider the effects of system failures on other systems and their functions. In general, common design practice provides physical and functional isolation from related components which are essential to safe operation.

4.2.2.3 In showing compliance with the provisions of 4.2.2, for Major Failure Conditions (refer to 3.2.18), a Qualitative Analysis (refer to 3.2.25) must be performed to determine compliance with the requirements of Table 3; in certain circumstances, a Quantitative Analysis (refer to 3.2.26) may also be required. There are several methods of performing a valid Qualitative Analysis:

(a) A "similarity argument" allows validation of a requirement by comparison to the requirements of similar certified systems. A similarity argument gains strength as the period of experience with the system increases. If the system is similar in its relevant attributes to those used in other aircraft and if the functions and effects of failure would be the same, then a design and installation appraisal and satisfactory service history of either the equipment being analyzed or of a similar design is usually acceptable for showing compliance. It is the applicant's responsibility to provide data that is: accepted, approved, or both; and, that supports any claims of similarity to a previous installation.

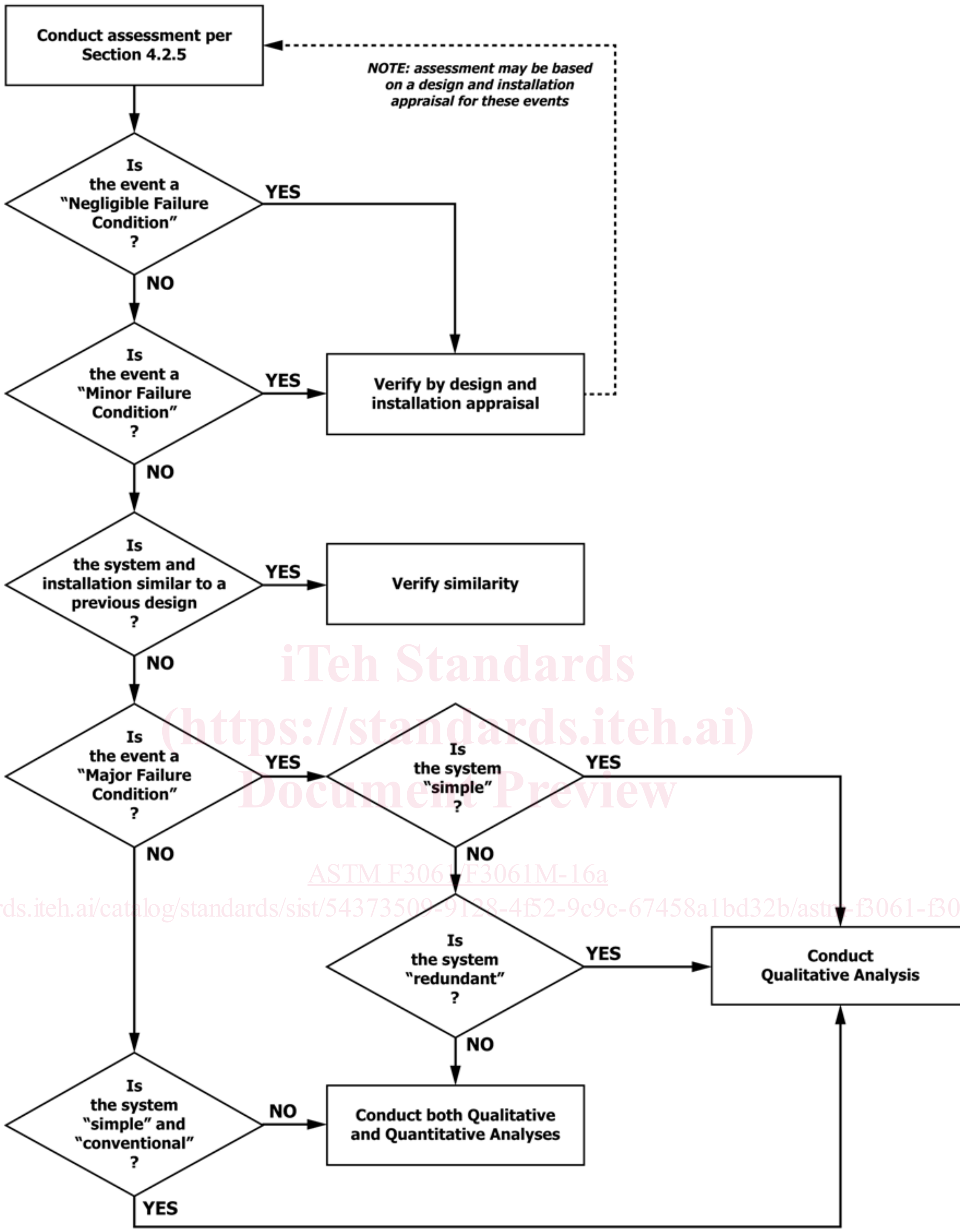

FIG. 2 Depth of Analysis Flowchart

(b) For systems that are not complex, and where similarity arguments cannot be used, "qualitative occurrence arguments" may be presented to demonstrate that the Major Failure Conditions of the system, as installed, are consistent with the requirements of Table 3; for example, redundant systems may qualify for this approach.

(c) For systems that are complex and possess low redundancy (for example, a system with a self-monitoring microprocessor), a qualitative functional Fault Tree Analysis (FTA) or Failure Modes and Effects Analysis (FMEA) supported by failure rate data and fault detection coverage analysis must be presented to demonstrate that the Major Failure Conditions of the system, as installed, are consistent with the requirements of Table 3.

(d) A Qualitative Analysis of a redundant system is usually complete if it shows isolation between redundant system

TABLE 2 Assessment Level Selection Matrix

Airworthiness Level	Engine Information			
	Reciprocating		Turbine	
	1	>1	1	>1
Level 1[A]	I	II	II	II
Level 2[A]	I	II	II	II
Level 3[A]	III	III	III	III
Level 4[A]	IV	IV	IV	IV

[A] Refer to 3.2.1.1.

TABLE 3 Probability Requirements

		Classification of Failure Conditions				
		Negligible[B]	Minor[B]	Major[B]	Hazardous[B]	Catastrophic[B]
Classification Considerations	Effect on Aircraft	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
	Effect on Occupants	Inconvenience for passengers	Physical discomfort for passengers	Physical distress to passengers, possibly including injuries	Serious or fatal injury to an occupant	Multiple fatalities
	Effect on Flight Crew	No effect on flight crew	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal injury or incapacitation
Assessment Level[A]		Allowable Qualitative Probability[B]				
ALL		No Probability Requirement	Probable[B]	Remote[B]	Extremely Remote[B]	Extremely Improbable[B]
Assessment Level[A]		Allowable Quantitative Probabilities[C]				
I		No Probability Requirement	$<10^{-3}$	$<10^{-4}$	$<10^{-5}$	$<10^{-6}$ (See [D])
II			$<10^{-3}$	$<10^{-5}$	$<10^{-6}$	$<10^{-7}$ (See [D])
III			$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-8}$ (See [D])
IV			$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-9}$ (See [D])

[A] Refer to Table 2.
[B] Refer to Section 3.
[C] Numerical values indicate an order of probability range and are provided here as a reference; refer to 4.2.2.5.
[D] At the aircraft function level, no single failure resulting in a Catastrophic Failure Condition is permitted.

channels and satisfactory reliability for each channel. For complex systems where functional redundancy is required, a qualitative functional FTA or FMEA may be necessary to demonstrate that redundancy actually exists (for example, no single failure affects all functional channels).

4.2.2.4 In showing compliance with the provisions of 4.2.2, for Hazardous and Catastrophic Failure Conditions (refer to 3.2.13 and 3.2.3, respectively), a thorough safety assessment is necessary. Except as specified below, a detailed safety analysis must be completed for each Hazardous and Catastrophic Failure Condition identified in accordance with 4.2.1. Such an assessment usually consists of an appropriate combination of qualitative and quantitative analyses; a System Safety Analysis (SSA) in accordance with the methodology outlined in SAE ARP4761 is one means of performing these analyses; however, other simpler methodologies may be employed as appropriate.

(a) For simple and conventional installations (that is, low complexity and similarity in relevant attributes), it may be possible to assess a Hazardous or Catastrophic Failure Condition as being Extremely Remote (refer to 3.2.11) or Extremely Improbable (refer to 3.2.10), respectively, on the basis of experienced engineering judgment using only qualitative analysis. The basis for such an assessment will be the degree of redundancy, the established independence and isolation of the channels, and the reliability record of the technology involved. Satisfactory serviexperience on similar systems commonly used in many aircraft may be sufficient when a close similarity is established regarding both the system design and operating conditions.

(b) For complex systems where true similarity can be rigorously established in all relevant attributes, including installation attributes, it may be possible to assess a Hazardous or Catastrophic Failure Condition as being Extremely Remote or Extremely Improbable, respectively, on the basis of experienced engineering judgment using only qualitative analysis. The basis for such an assessment will be a high degree of similarity in both design and application.

(c) No Catastrophic Failure Condition should result from the failure of a single component, part, or element of a system. Experienced engineering judgment and service history should show that a Catastrophic Failure Condition due to a single failure mode is not a practical possibility. The logic and rationale used in the assessment should be straightforward and obviously substantiate that the failure mode simply would not occur unless it is associated with an unrelated failure condition that would, in itself, be Catastrophic.

4.2.2.5 In showing compliance with the provisions of 4.2.2, where Quantitative Analysis is required by Fig. 2, the analysis should demonstrate that the probability of the failure condition occurrence meets the probability range shown in Table 3. It is recognized that there is inherent variance in predictions used to demonstrate that these probabilities are met; it may therefore be acceptable, provided the analysis can be shown to be conservative and is acceptable to the governing civil aviation authority, to be slightly above the probabilities shown in Table 3.

4.2.3 Software and Airborne Electronic Hardware must be designed with the appropriate development assurance level as specified in Table 4 or in accordance with the Development Assurance Level (DAL) assignment methodology outlined in SAE ARP4754.

4.2.3.1 In showing compliance with the provisions of 4.2.3, once a DAL is assigned, acceptable means of compliance may be found in RTCA DO-178 or RTCA-DO254 or both; refer to Section 2.

4.2.4 Information concerning an unsafe system operating condition must be provided in a timely manner to the crew to enable them to take appropriate corrective action.

4.2.4.1 In showing compliance with the provisions of 4.2.4, if immediate pilot awareness and immediate or subsequent corrective action is required, the information required by 4.2.4 must be presented in accordance with 14 CFR §23.1309(d), Sentence 2.

4.2.4.2 In showing compliance with the provisions of 4.2.4, the assessment discussed in 4.2.1 should be used to determine what Failure Conditions would become "Unsafe System Operating Conditions" if the crew failed to take any action or observe appropriate precautions; refer to 3.2.12 and 3.2.34.

5. Electrical Systems

NOTE 4—Table 5 provides correlation between various Aircraft Type Codes and the individual requirements contained within this section; refer to 3.2.1. For each subsection, an indicator can be found under each ATC character field; three indicators are used:

An empty cell ( ) in all applicable ATC character field columns indicates that an aircraft must meet the requirements of that subsection.

A white circle (○) in multiple columns indicates that an aircraft is exempt from the requirements of that subsection *only* if all such ATC character fields are applicable.

A mark-out (×) in any of the applicable ATC character field columns indicates that an aircraft is exempt from the requirements of that subsection.

Example—An aircraft with an ATC of 1SRLLDLN is being considered. Since all applicable columns are empty for Subsection 5.2.1, that subsection is applicable to the aircraft. Since both the "L" stall speed column and the "D" meteorological column for Subsection 5.1.1 contain white circles, then that subsection is not applicable; however, for an aircraft with an ATC of 1SRMLDLN, Subsection 5.1.1 would be applicable since the "M" stall speed column does not contain a white circle. Subsection 5.2.1.2 would not be applicable to either aircraft, since it contains an × in the "1" airworthiness level column.

NOTE 5—This chapter provides specifications for the electrical generation and distribution systems used to power various aircraft systems and equipment. It intentionally does not address any electrical power systems that may be employed in electrically-powered aircraft propulsion systems; such power systems are outside the scope of this chapter.

5.1 *Power Source Capacity and Distribution:*

5.1.1 Each installation whose functioning is required for type certification or under operating rules and that requires a power supply is an "essential load" on the power supply. The power sources and the system must be able to supply the power loads specified in 5.1.1.1 through 5.1.1.6 in probable operating combinations and for probable durations. The power loads may be assumed to be reduced under a monitoring procedure consistent with safety in the kinds of operation authorized. Loads not required in controlled flight need not be considered for the two-engine-inoperative condition on aircraft with three or more engines.

5.1.1.1 When required by 5.1.1, the power sources and the electrical distribution system, when functioning normally, must be able to support all connected loads.

5.1.1.2 When required by 5.1.1, the power sources and the electrical distribution system must be able to support all essential loads after the failure of any one engine.

5.1.1.3 When required by 5.1.1, the power sources and the electrical distribution system must be able to support all essential loads after the failure of any one power converter.

5.1.1.4 When required by 5.1.1, the power sources and the electrical distribution system must be able to support all essential loads after the failure of any one energy storage device.

TABLE 4 Development Assurance Level Requirements

Assessment Level[A]	Classification of Failure Conditions				
	Negligible	Minor	Major	Hazardous	Catastrophic
	Software (SW) and Airborne Electronic Hardware (AEH) Development Assurance Levels (DALs)[B]				
I	No SW and/or HW DAL Requirement	P=D	P=C, S=D (See[C])	P=C, S=D (See[C])	P=C, S=C (See[C])
II		P=D	P=C, S=D (See[C])	P=C, S=C (See[C])	P=C, S=C (See[C])
III		P=D	P=C, S=D (See[C])	P=C, S=C (See[C])	P=B, S=C (See[C])
IV		P=D	P=C, S=D (See[C])	P=B, S=C (See[C])	P=A, S=B (See[C])

[A] Refer to Table 2.
[B] The letters of the alphabet used above denote the typical SW and AEH DALs. "P" indicates the primary system; "S" indicates the secondary system; "A", "B", "C", and "D" indicate the DAL in accordance with RTCA/DO-178B or RTCA/DO-254 as applicable. For example, an indication of "P=A" would translate to a SW or AEH DAL of "A" on the primary system.
[C] A secondary system is not necessarily required; however, if a secondary system is needed to meet the probability goals of Table 3, then that secondary system must meet the stated DAL goal.

TABLE 5 ATC Compliance Matrix, Section 5

Section	Airworthiness Level				Number of Engines		Type of Engine(s)		Stall Speed			Cruise Speed		Meteorological Conditions			Altitude		Maneuvers	
	1	2	3	4	S	M	R	T	L	M	H	L	H	D	N	I	L	H	N	A
5																				
5.1																				
5.1.1									○					○						
5.1.1.1									○					○						
5.1.1.2									○					○						
5.1.1.3									○					○						
5.1.1.4									○					○						
5.1.1.5									○					○						
5.1.1.6									○					○						
5.2																				
5.2.1																				
5.2.1.1				×																
5.2.1.2	×	×	×																	
5.2.2																				
5.2.3																				
5.2.4																				
5.2.5																				
5.2.6																				
5.2.7	×	×	×																	
5.2.8	×	×	×																	
5.2.9	×	×	×																	
5.2.10	×	×	×																	
5.2.11	×	×	×																	
5.2.12																				
5.2.12.1																				
5.2.12.2																				
5.2.12.3																				
5.2.12.4																				
5.2.12.5																				
5.2.12.6																				
5.2.12.7																				
5.2.13																				
5.2.13.1																				
5.2.13.2	×	×	×																	
5.2.14																				
5.2.15																				
5.2.16																				
5.2.17									○					○						
5.2.17.1									○					○						
5.2.17.2									○					○						
5.3																				
5.3.1																				
5.3.1.1																				
5.3.1.2																				
5.3.1.3																				
5.3.2																				
5.3.3																				
5.3.4																				
5.3.5																				
5.3.6																				
5.3.6.1																				
5.3.6.2																				
5.3.6.3																				
5.3.7									○					○				×		
5.3.8									○					○			×			
5.4																				
5.4.1																				
5.4.1.1																				
5.4.1.2																				
5.4.2																				
5.4.3																				
5.4.4																				
5.4.5																				
5.4.5.1																				
5.5																				
5.5.1																				
5.5.2																				
5.5.3																				
5.5.4																				
5.5.4.1																				
5.5.4.2																				
5.6																				
5.6.1																				

TABLE 5 *Continued*

Section	Airworthiness Level				Number of Engines		Type of Engine(s)		Stall Speed			Cruise Speed		Meteorological Conditions			Altitude		Maneuvers	
	1	2	3	4	S	M	R	T	L	M	H	L	H	D	N	I	L	H	N	A
5.6.2																				
5.7																				
5.7.1																				
5.7.2																				
5.7.3																				
5.7.4																				
5.7.5	×																			
5.7.6																				
5.7.7	×																			
5.7.8	×																			
5.8																				
5.8.1	×																			
5.8.2	×																			
5.8.3	×																			
5.9																				
5.9.1																				
5.9.2																				

5.1.1.5 When required by 5.1.1, the power sources and the electrical distribution system must be able to support all essential loads after the failure of any two engines on aircraft with three or more engines.

5.1.1.6 When required by 5.1.1, the power sources and the electrical distribution system must be able to support all essential loads for which an alternate source of power is required, after any failure or malfunction in any one power supply system, any one distribution system, or any other utilization system.

5.2 *Electrical Systems and Equipment:*

5.2.1 Electric power sources, their transmission cables, and their associated control and protective devices, must be able to furnish the required power at the proper voltage to each load circuit essential for safe operation.

5.2.1.1 Compliance with 5.2.1 must be shown by an electrical load analysis or by electrical measurements that account for the electrical loads applied to the electrical system in probable combinations and for probable durations.

5.2.1.2 Compliance with 5.2.1 must be shown by an electrical load analysis that accounts for the electrical loads applied to the electrical system in probable combinations and for probable durations.

5.2.2 Each electrical system, when installed, must be free from hazards in itself, in its method of operation, and in its effects on other parts of the aircraft.

5.2.3 Each electrical system, when installed, must be protected from fuel, oil, water, other detrimental substances, and mechanical damage.

5.2.4 Each electrical system, when installed, must be designed so that the risk of electrical shock to crew, passengers, and ground personnel is reduced to a minimum.

5.2.5 Electric power sources must function properly when connected in combination or independently.

5.2.6 No failure or malfunction of any electric power source may impair the ability of any remaining source to supply load circuits essential for safe operation.

5.2.7 Each system must be designed so that essential load circuits can be supplied in the event of reasonably probable faults or open circuits including faults in heavy current carrying cables.

5.2.8 A means must be accessible in flight to the flight crewmembers for the individual and collective disconnection of the electrical power sources from the system.

5.2.9 The system must be designed so that voltage and frequency, if applicable, at the terminals of all essential load equipment can be maintained within the limits for which the equipment is designed during any probable operating conditions.

5.2.10 If any particular system or item of equipment requires two independent sources of electrical power, their electrical energy supply must be ensured by means such as duplicate electrical equipment, throwover switching, or by the use of multichannel or loop circuits separately routed.

5.2.11 For the purpose of complying with 5.2.6 through 5.2.10, the distribution system includes the distribution busses, their associated feeders, and each control and protective device.

5.2.12 There must be at least one generator/alternator if the electrical system supplies power to load circuits essential for safe operation. In addition, the requirements of 5.2.12.1 through 5.2.12.7 must be met.

5.2.12.1 Each generator/alternator must be able to deliver its continuous rated power, or such power as is limited by its regulation system.

5.2.12.2 Generator/alternator voltage control equipment must be able to dependably regulate the generator/alternator output within rated limits.

5.2.12.3 Automatic means must be provided to prevent damage to any generator/alternator due to reverse current into the generator/alternator.

5.2.12.4 Automatic means must be provided to prevent adverse effects on the aircraft electrical system due to reverse current into the generator/alternator.

5.2.12.5 A means must be provided to disconnect each generator/alternator from the battery and other generators/alternators.

5.2.12.6 There must be a means to give immediate warning to the flight crew of a failure of any generator/alternator.

5.2.12.7 Each generator/alternator must have an overvoltage control designed and installed to prevent damage to the electrical system, or to equipment supplied by the electrical system that could result if that generator/alternator were to develop an overvoltage condition.

5.2.13 A means must exist to indicate to appropriate flight crewmembers the electric power system quantities essential for safe operation.

5.2.13.1 For aircraft with direct current systems, an ammeter that can be switched into each generator/alternator feeder may be used and, if only one generator/alternator exists, the ammeter may be in the battery feeder.

5.2.13.2 The essential electric power system quantities include the voltage and current supplied by each generator/alternator.

5.2.14 Electrical equipment must be so designed and installed that in the event of a fire in the engine compartment, during which the surface of the firewall adjacent to the fire is heated to 1095°C [2000°F] for 5 min or to a lesser temperature substantiated by the applicant, the equipment essential to continued safe operation and located behind the firewall will function satisfactorily and will not create an additional fire hazard.

5.2.15 If provisions are made for connecting external power to the aircraft, and that external power can be electrically connected to equipment other than that used for engine starting, means must be provided to ensure that no external power supply having a reverse polarity, or a reverse phase sequence, can supply power to the aircraft electrical system.

5.2.16 If provisions are made for connecting external power to the aircraft, and that external power can be electrically connected to equipment other than that used for engine starting, the external power connection must be located so that its use will not result in a hazard to the aircraft or ground personnel.

5.2.17 It must be shown by analysis, tests, or both, that the aircraft can be operated safely in VFR conditions, for a period of not less than 5 min, with the normal electrical power (electrical power sources excluding the battery and any other standby electrical sources) inoperative, with critical type fuel (from the standpoint of flameout and restart capability), and with the aircraft initially at the maximum certificated altitude. In showing compliance with this requirement, parts of the electrical system may remain on if the conditions of 5.2.17.1 and 5.2.17.2 are both met.

5.2.17.1 In showing compliance with 5.2.17, parts of the electrical system may remain on if a single malfunction, including a wire bundle or junction box fire, cannot result in loss of the part turned off and the part turned on.

5.2.17.2 In showing compliance with 5.2.17, parts of the electrical system may remain on if the parts turned on are electrically and mechanically isolated from the parts turned off.

5.3 *Storage Battery Design and Installation:*

5.3.1 Each storage battery design and installation must maintain safe cell temperatures and pressures during any probable charging and discharging condition.

5.3.1.1 No uncontrolled increase in cell temperature may result when the battery is recharged (after previous complete or most critical discharge) at maximum regulated voltage or power.

5.3.1.2 No uncontrolled increase in cell temperature may result when the battery is recharged (after previous complete or most critical discharge) during a flight of maximum duration.

5.3.1.3 No uncontrolled increase in cell temperature may result when the battery is recharged (after previous complete or most critical discharge) under the most adverse cooling condition likely to occur in service.

5.3.2 Compliance with 5.3.1 must be shown by tests unless experience with similar batteries and battery management systems or installations has shown that maintaining safe cell temperatures and pressures presents no problem.

5.3.3 Each storage battery must be designed and installed such that no explosive or toxic gases emitted by any battery in normal operation, or as the result of any probable malfunction in the charging system or battery installation, may accumulate within the aircraft in such quantities as would cause risk of fire/explosion or be harmful to the aircraft occupants, or both.

5.3.4 Each storage battery design and installation must prevent damage to surrounding structures or adjacent essential equipment from corrosive fluids or gases that may escape from the battery.

5.3.5 Each nickel cadmium battery installation capable of being used to start an engine or auxiliary power unit must have provisions to prevent any hazardous effect on structure or essential systems that may be caused by the maximum amount of heat the battery can generate during a short circuit of the battery or of its individual cells.

5.3.6 Nickel cadmium battery installations capable of being used to start an engine or auxiliary power unit must meet the requirements of either 5.3.6.1, 5.3.6.2, or 5.3.6.3.

5.3.6.1 If the requirements of either 5.3.6.2 or 5.3.6.3 are not met, nickel cadmium battery installations capable of being used to start an engine or auxiliary power unit must have a system to control the charging rate of the battery automatically so as to prevent battery overheating.

5.3.6.2 If the requirements of either 5.3.6.1 or 5.3.6.3 are not met, nickel cadmium battery installations capable of being used to start an engine or auxiliary power unit must have a battery temperature sensing and over-temperature warning system with a means for disconnecting the battery from its charging source in the event of an over-temperature condition.

5.3.6.3 If the requirements of either 5.3.6.2 or 5.3.6.3 are not met, nickel cadmium battery installations capable of being used to start an engine or auxiliary power unit must have a battery failure sensing and warning system with a means for disconnecting the battery from its charging source in the event of battery failure.

5.3.7 In the event of a complete loss of the primary electrical power generating system, the battery must be capable of providing electrical power to those loads that are essential to continued safe flight and landing for at least 30 min (which includes the time to recognize the loss of generated power and to take appropriate load shedding action).

5.3.8 In the event of a complete loss of the primary electrical power generating system, the battery must be capable of providing electrical power to those loads that are essential to continued safe flight and landing for at least 60 min (which includes the time to recognize the loss of generated power and to take appropriate load shedding action).

5.4 *Circuit Protective Devices:*

5.4.1 Protective devices, such as fuses or circuit breakers, must be installed in all electrical circuits.

5.4.1.1 The provisions of 5.4.1 do not apply to main circuits of starter motors used during starting only.

5.4.1.2 The provisions of 5.4.1 do not apply to circuits in which no hazard is presented by their omission.

5.4.2 A protective device for a circuit essential to flight safety may not be used to protect any other circuit.

5.4.3 Each resettable circuit protective device ("trip free" device in which the tripping mechanism cannot be overridden by the operating control) must be designed so that a manual operation is required to restore service after tripping.

5.4.4 Each resettable circuit protective device ("trip free" device in which the tripping mechanism cannot be overridden by the operating control) must be designed so that if an overload or circuit fault exists, the device will open the circuit regardless of the position of the operating control.

5.4.5 If the ability to reset a circuit protective device or replace a fuse is essential to safety in flight, a means must be provided so that it can be readily reset or replaced in flight; refer to 14 CFR §23.1357(d).

5.4.5.1 For fuses identified as replaceable in flight, there must be onboard one spare of each rating or 50 % spare fuses of each rating, whichever is greater.

5.5 *Master Switch Arrangement:*

5.5.1 There must be a master switch arrangement to allow ready disconnection of each electric power source from power distribution systems, except as provided in 5.5.4.

5.5.2 The point of disconnection required by 5.5.1 must be adjacent to the sources controlled by the master switch arrangement.

5.5.3 If separate switches are incorporated into the master switch arrangement required by 5.5.1, a means must be provided for the switch arrangement to be operated by a single action; refer to 14 CFR 23.1361(a).

5.5.4 Load circuits may be connected so that they remain energized when the master switch is open if the circuits are isolated, or physically shielded, to prevent their igniting flammable fluids or vapors that might be liberated by the leakage or rupture of any flammable fluid system, and the requirements of either 5.5.4.1 or 5.5.4.2 are met.

5.5.4.1 The circuits are required for continued operation of the engine.

5.5.4.2 The circuits are protected by circuit protective devices with a rating of five amperes or less adjacent to the electric power source. Two or more circuits must not be used to supply a load of more than five amperes.

5.6 *Switches:*

5.6.1 Each switch must be able to carry its rated current.

5.6.2 Each switch must be constructed with enough distance or insulating material between current carrying parts and the housing so that vibration in flight will not cause shorting.

5.7 *Electrical Cables and Equipment:*

5.7.1 Each electric connecting cable must be of adequate capacity.

5.7.2 Any equipment that is associated with any electrical cable installation and that would overheat in the event of circuit overload or fault must be flame resistant.

5.7.3 Any electrical cables or equipment that would overheat in the event of circuit overload must not emit dangerous concentrations of toxic fumes.

5.7.4 Main power cables (including generator/alternator cables) in the fuselage must be designed to allow a reasonable degree of deformation and stretching without degradation or failure.

5.7.5 Main power cables (including generator/alternator cables) in the fuselage must be separated from flammable fluid lines, or be shrouded by means of electrically insulated flexible conduit (or equivalent) which is in addition to the normal cable insulation.

5.7.6 Means of identification must be provided for electrical cables, terminals, and connectors.

5.7.7 Electrical cables must be installed such that the risk of mechanical damage or damage caused by fluids, vapors, or sources of heat, or a combination thereof, is minimized.

5.7.8 Where a cable cannot be protected by a circuit protection device or other overload protection, it must not cause a fire hazard under fault conditions.

5.8 *Electrical System Fire Protection:*

5.8.1 Each component of the electrical system must meet the applicable fire protection requirements of 10.3 and Specification F3066/F3066M.

5.8.2 Electrical cables, terminals, and equipment in designated fire zones that are used during emergency procedures must be fire-resistant.

5.8.3 Insulation on electrical wire and electrical cable must be self-extinguishing when tested at an angle of 60° in accordance with the applicable portions of 14 CFR 23, Appendix F, or other approved equivalent methods. The average burn length must not exceed 76 mm [3 in.] and the average flame time after removal of the flame source must not exceed 30 s. Drippings from the test specimen must not continue to flame for more than an average of 3 s after falling.

5.9 *Electronic Equipment:*

5.9.1 Radio and electronic equipment, controls, and wiring must be installed so that operation of any unit or system of units will not adversely affect the simultaneous operation of any other radio or electronic unit, or system of units, required by the rules of the governing civil aviation authority.

5.9.2 If installed communication equipment includes transmitter "off-on" switching, that switching means must be designed to return from the "transmit" to the "off" position when it is released and ensure that the transmitter will return to the off (non-transmitting) state.