4 DESIGN CONSIDERATIONS

The number of components and systems inside aeroplane fuel tanks whose failure could result in an ignition source within the fuel tank should be minimised. The following design practices are accepted by EASA for minimising ignition sources:

4.1 Fibre optics

Wiring entering the tank for such purposes as temperature monitoring and fuel quantity indication should be minimised. The use of alternate technology, such as fibre optics, may provide a means of reducing or eliminating electrically powered components from inside the fuel tanks.

4.2 Fuel pump electrical power supply

4.2.1 Fuel pump power wiring

If practical, fuel pumps should be located such that the electrical power for the pumps is routed outside the fuel tanks in such a manner that failures in the electrical power supply cannot create a hot spot inside the tank, or arc into the fuel tank. While the routing of the fuel pump power supply outside the fuel tank, and away from the fuel tank walls, may eliminate the potential for arcing directly into the fuel tank or heating of tank surfaces, the failure analysis should consider the need for electrical circuit-protective devices. If the power supply cannot be routed outside the tank, additional design features should be considered as discussed in paragraph 4.3.2 below.

Note: The applicant should consider, in the design of the pump wiring system and when showing compliance, the electromagnetic effects and electrical transients that may damage the wiring or pump.

4.2.2 Fuel pump electrical connectors

4.2.2.1 Arcing at the pump electrical connector has resulted in uncontrolled fuel leakage, an ignition source, and an uncontrolled fire outside the fuel tank. This can create a fuel tank ignition source due to the external fire heating the fuel tank surfaces. Fuel pumps should include features to isolate the electrical connector from the portion of the fuel pump where fuel is located. Applicants should show that the arcing that occurs in these designs cannot cause a cascading failure from arcing in the electrical connection, resulting in a fuel leak and a fire. One approach includes the incorporation of a dry area between the electrical connector and the fuel pump. Another approach includes extending the fuel pump power wire so the electrical connector is well away from the fuel pump. This approach has included a drip loop on the wire to prevent any fuel leaking onto the wire from being present at the electrical connector.

4.2.2.2 Alternatively, or in addition to isolating electrical connectors from the fuel, limiting the electrical energy passing into the fuel tank can prevent an ignition source from occurring. The design of traditional fuel pumps has resulted in the need to install AFCB or GFI protection features to limit the energy release during an arcing event to prevent an ignition source from occurring.

4.3 Location of the pump inlet

Debris that may enter a fuel pump inlet can cause sparks inside the fuel tank. One means to address this ignition source has been to locate the pumps such that the pump inlet remains covered with fuel whenever the pump is operating within the aeroplane operating envelope. Another means has been to prevent the propagation of any ignition from the pump into the fuel tank by using flame arrestor technology. (The performance of the flame arrestor should be validated by test to verify its effectiveness at stopping a flame front.) Any protective means, including those shown in paragraphs 4.3.1 and 4.3.2 below, should be demonstrated to be effective under the pitch, roll attitude, and negative G conditions anticipated to occur in service.

4.3.1 Main feed tanks

The installation of baffles in the tank structure, and the use of collector tanks that are continually filled with fuel using ejector pumps, are methods that have proven successful in keeping the pump inlets and pump housings submerged in fuel.

4.3.2 Auxiliary tanks

For auxiliary tanks that use motor-driven fuel pumps and that are routinely emptied, the accepted design practices include shutting off the motor-driven pumps before uncovering the fuel pump inlet, and the installation of a flame arrestor in the scavenge pump inlet line, or scavenging the remaining fuel with ejector pumps. (Note that the installation of features such as a flame arrestor in the fuel system would need to meet the fuel system performance requirements in CS 25.951, Fuel System: General.)

4.4 Wiring

The following paragraphs on wiring represent acceptable approaches for dealing with the wiring used in and near fuel tanks. For specific requirements and further guidance, the applicant should review the wiring installation and design requirements in the electrical wiring interconnect systems (EWIS) rules of CS-25 Subpart H and the associated AMC.

4.4.1 Intrinsically safe wiring

All the wiring that is intended to conduct intrinsically safe levels of electrical power into or through the fuel tanks should incorporate protective features that prevent an exceedance of the intrinsically safe levels discussed in paragraphs 3.2 and 3.3 of this AMC. This wiring should also be protected from the transients induced by high intensity radiated fields (HIRF). The following protective features could be used to support that objective:

— Separation and shielding of the fuel tank wires from other aeroplane wiring and circuits,

— Shielding against HIRF and other electromagnetic effects, and

— The installation of transient-suppression devices to preclude unwanted electrical energy from entering the tank.

4.4.2 Higher energy wiring

This includes all wiring that is not intrinsically safe.

4.4.2.1 Wiring should not be routed through metallic conduits inside the fuel tank or adjacent to fuel tank surfaces such that damage, inappropriate maintenance, or other failure/wear conditions could result in arcing to the conduit or metallic tank surface and the consequent development of an ignition source in the fuel tank. If metallic or other conductive conduit materials are used, a single failure of electrical arcing of the wiring to the conduit, adjacent tank surfaces, or structure should be assumed to occur. In addition, circuit-protective features or other features should be incorporated to preclude the development of an ignition source in the fuel tank. The methods that may be used to address this foreseeable failure condition include the use of circuit-protective features such as dual conduits, thick-walled conduits, and/or fast-acting AFCB or GFI circuit breakers. Providing multiple layers of sleeving alone would not be considered acceptable, since wear could defeat the multiple layer protection.

4.4.2.2 Where electric wires are routed through metallic conduits installed in a fuel tank, high surface temperatures or arcing through the conduit walls can be created by short circuits. All the wiring conducting levels of power that exceed intrinsically safe levels (e.g., the fuel pump power supply) into or through a fuel tank should be evaluated assuming arcing to adjacent surfaces, such as metallic conduits or wing surfaces, unless fail-safe protective features are provided. A critical electrical wiring condition might be one in which the insulation is worn, cracked, broken, or of low dielectric strength, allowing intermittent or constant arcing to occur without consuming enough power to cause the circuit protection device, such as a thermal mechanical circuit breaker, to open. Inspection of wiring from in-service aeroplanes has shown that greater than expected wear may occur on sleeving and wiring insulation due to movement of the wire within the conduit. Roughness of the conduit material and variations in vibration levels for each installation may significantly increase wear. In addition, inspections have shown that some protective sleeving has been missing or improperly installed, or the wrong sleeving material has been used, resulting in damage to the insulation. For these reasons, the use of protective sleeving on wiring would not, by itself, be adequate for showing compliance. The design should be tolerant to these types of foreseeable failure or maintenance errors.

4.4.3Wire separation

The wiring designs used on transport category aeroplanes vary significantly between manufacturers and models; therefore, it is not possible to define a specific, universal separation distance, or the characteristics of physical barriers between wire bundles, to protect critical wiring from damage. The separation requirements for the wiring and other components of EWIS are contained in CS 25.1707, System separation: EWIS. AMC 25.1707 contains guidance on determining an adequate separation distance between EWIS and between EWIS and aeroplane systems and structures. Even if CS 25.1707 is not in the type certification basis of the aeroplane being modified, the guidelines contained in AMC 25.1707 should be applied, along with the guidelines contained in this AMC, when determining the adequate separation distance. Intrinsically safe wiring for fuel tanks needs to be protected from induced currents caused by power system switching transients, or electromagnetic interference due to close proximity to other aeroplane wiring. In addition, damage to wire insulation can result in unwanted electrical energy being transmitted into the fuel tank, if the damaged wire can come into contact with the conductor of another wire that is not intrinsically safe. Of particular concern is the possibility of a wire bundle fire that exposes and breaks wires that are not intrinsically safe, and also damages the insulation of intrinsically safe wiring that is in close physical proximity. The broken wires may still be energised and could contact conductors of the damaged intrinsically safe wire. If physical separation is used to protect intrinsically safe fuel system wiring from other wiring, or to protect fuel tank walls from high-power wiring, the applicant must establish the minimum physical separation. The applicant should conduct an analysis to verify that currents and energies greater than those specified in paragraphs 3.2 and 3.3 of this AMC will not be applied to intrinsically safe wiring, considering the factors listed below. The following factors are based on the guidance contained in paragraphs 3. and 4. of AMC 25.1707:

4.4.3.1 The electrical characteristics, power, and criticality of the signals in the wire bundle and adjacent wire bundles;

4.4.3.2 The installation design features including the number, type, fire resistance, and location of the support devices along the wire path of the intrinsically safe wire and adjacent higher power wires;

4.4.3.3 The maximum amount of slack wire resulting from wire bundle build tolerances and other wire bundle manufacturing variations;

4.4.3.4 The probable variations in the installation of the intrinsically safe fuel system wiring and adjacent wiring, including the position or omission of wire support devices and the amount of slack wire that is possible;

4.4.3.5 The expected operating environment, including the amount of deflection or relative movement that can occur and the effect of a failure of a wire support device, or a broken wire, or other methods used to maintain physical separation;

4.4.3.6 The effects of wire bundle fires;

4.4.3.7 Maintenance practices, as defined by the aeroplane manufacturer's standard wiring practices manual, and the ICA required by CS 25.1529, CS 25.1729; and

4.4.3.8 Localised separation.

Note: Some areas of an aeroplane may have localised areas where maintaining a general physical separation distance is not feasible. This is especially true in smaller transport category aeroplanes or in areas where wiring spans the wing-to-body join of larger transport aeroplanes. In those areas that limit the separation distance, additional means of ensuring physical separation and protection of the wiring may be necessary. Testing and/or analysis used to show that the reduced separation distance is acceptable should be conservative and consider the worst possible failure condition not shown to be extremely improbable. The applicant should substantiate that the means to achieve the reduced separation provides the necessary level of protection for wire-related failures and electromagnetic effects.

4.4.4 Inspection

Means should be provided to allow for the visual inspection of the wiring, physical barriers, and other physical means of protection. Non-destructive inspection aids may be used where it is impracticable to provide for direct visual inspection, if it is shown that the inspection is effective and the inspection procedures are specified in the maintenance manual required by CS 25.1529 and CS 25.1729.

4.4.5 Identification

Means must also be provided to make EWIS wires readily identifiable and visible to maintenance, repair, or alteration personnel. The method of identification must remain legible throughout the aeroplane's operational life. The complete regulatory requirements for EWIS identification are contained in CS 25.1711, Component identification: EWIS.

4.4.6 Circuit breakers

Service experience has indicated that thermal mechanical circuit breakers installed in fuel pump circuits have not been shown, on some aeroplane designs, to preclude arcing of electrical wiring through metallic barriers into the fuel tank, barriers such as conduits, fuel pump housings, electrical connectors, or the tank wall. Evidence suggests that arcing from the wiring to metallic surfaces may not result in a hard short, which would trip the circuit breaker, and may result in intermittent low-level arcing that gradually arcs through the metallic barrier into the fuel tank. For these failure conditions, circuit-protective devices such as AFCBs or GFIs may be used to provide the fail-safe features necessary to show compliance. Appendix A of this AMC provides guidance for the certification of an AFCB or GFI.

4.4.7 The use of non-metallic conduits

If a non-metallic conduit is used, its compatibility with fuel should be shown. The non-metallic conduit should be evaluated for the effects of ageing due to heat, corrosion at the connecting fittings, electrostatic charge build-up, and resistance to heat damage from internal shorts of the wires routed within the conduit.

4.4.8 Wire splices

Splices in fuel system wiring have been allowed as a standard repair procedure. The acceptability of splices will be based upon the system design and fail-safe features. The safety assessment may show that splices in fuel tank system wiring, such as fuel quantity indicating wiring within the fuel tank and fuel pump windings, are prohibited. This would be defined as a CDCCL.

4.4.9 The use of silver in fuel tanks

Silver can combine with sulphur or water and form silver-sulphide or oxide deposits between exposed conductors (terminal block connections, etc.). The silver-sulphide deposits reduce the resistance between the conductors and can ignite fuel vapour when exposed to very low levels of electrical energy. If the use of silver in electrical components and wiring in the tank is determined to be critical, it should be defined as a CDCCL. The energy levels that have been shown to ignite fuel vapour during laboratory tests approach the levels normally used on FQIS wires and probes (e.g. FAA Report No. DOT/FAA/AR-03/61, Silver-Sulphur Deposits on Fuel Quantity Indication System and Attendant Wiring). This issue should be carefully addressed.

4.4.10 The use of steel wool

Steel wool has been used as a cleaning tool to remove corrosion and to clean parts inside fuel tanks. Steel wool creates small conductive filaments that can cause ignition sources in a fuel tank if the steel wool makes a connection between two conductors in fuel tank quantity gauging system components. For this reason, applicants should not allow the use of steel wool inside fuel tanks, and should recommend using other abrasives. (However, as stated in paragraph 5.3.4.1 in this AMC, the applicant should assume the presence of conductive debris, such as steel wool, when performing the fuel tank ignition prevention analysis.)

5 SAFETY ANALYSIS

5.1 Ignition source failure analysis

Compliance with CS 25.981 requires each applicant to develop a failure analysis for the fuel tank installation to substantiate that ignition sources will not be present in the fuel tanks. The requirements of CS 25.981 are in addition to the more general propulsion failure analysis requirements of CS 25.901 and CS 25.1309 that have been applied to propulsion installations.

5.1.1 CS 25.981(a)(3) defines three failure scenarios that must be addressed in order to show compliance with the rule:

5.1.1.1 No single failure, regardless of the probability of occurrence of the failure, may cause an ignition source.

5.1.1.2 No single failure, regardless of the probability of occurrence, in combination with any latent failure condition not shown to be at least extremely remote (i.e., not shown to be extremely remote or extremely improbable), may cause an ignition source.

5.1.1.3 No combinations of failures that are not shown to be extremely improbable may cause an ignition source. That is, each combination of failures that can create an ignition source must be separately shown to be extremely improbable.

5.1.2 SAE ARP4761, 'Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment' dated December 1996, describes methods for completing an SSA. An assessment may range from a simple report, which offers descriptive details associated with a failure condition, interprets test results, compares two similar systems, or offers other qualitative information, to a detailed failure analysis that may include estimated numerical probabilities. The depth and scope of an acceptable SSA depend on the following:

5.1.3.1 The complexity and criticality of the functions performed by the system under consideration,

5.1.3.2 The severity of the related failure conditions,

5.1.3.3 The uniqueness of the design and the extent of the relevant service experience,

5.1.3.4 The number and complexity of the identified causal failure scenarios, and

5.1.3.5 The detectability of contributing failures.

Note: CS 25.981 and CS 25.901 are intended to address system failures or conditions that may result in the presence of an ignition source in the fuel tanks. These specifications are not intended to address the failures or conditions that could lead to the ignition of fuel vapour, which are addressed by other specifications, such as:

— Uncontained engine debris,

— External engine fires following an engine separation,

— Damage resulting from explosive materials such as bombs,

— Post-crash fire heating of tank surfaces,

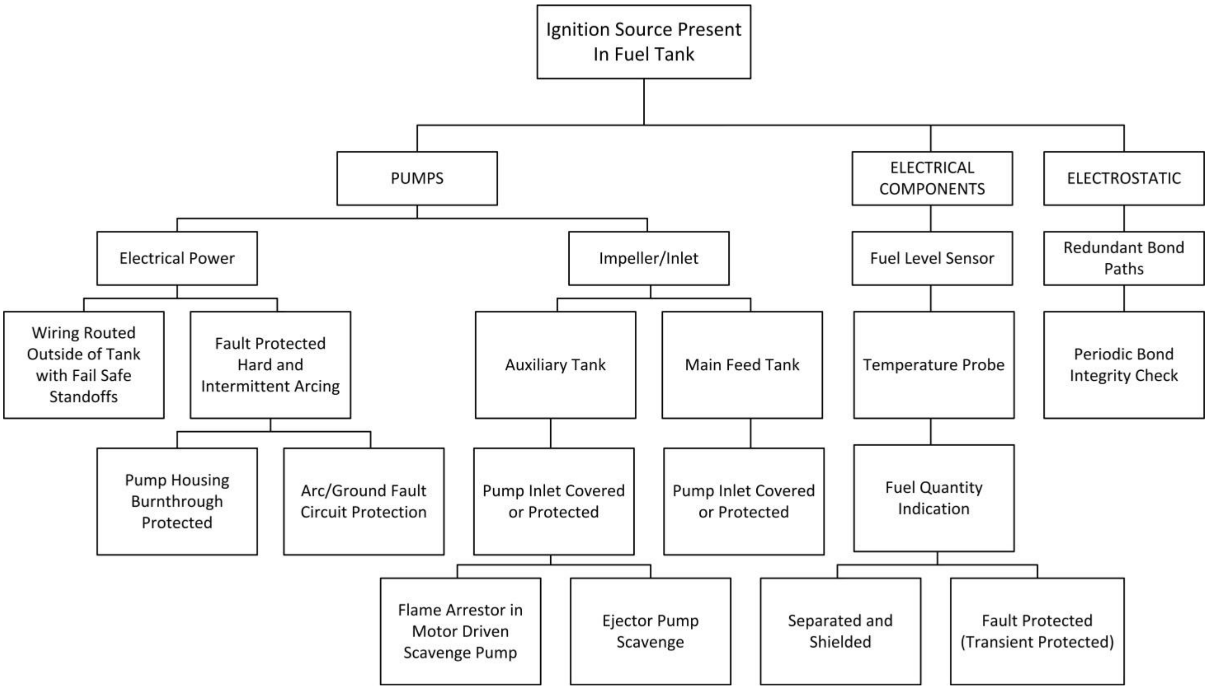
— Propagation of fire through the aeroplane vent system into the fuel tanks, or

— A fire originating within the engine that burns through the engine case.

5.2 Qualitative safety assessment

5.2.1 Typical aeroplane fuel tank systems have a limited number of possible ignition sources. Figure 1 below shows some causes of ignition sources and methods that may be used to meet the fail-safe requirements. The level of analysis required to show that ignition sources will not develop will depend on the specific design features of the fuel tank system being evaluated. Detailed quantitative analysis should not be necessary if a qualitative safety assessment shows that the features incorporated into the fuel tank system design protect against the development of ignition sources within the fuel tank system. For example, if intrinsically safe FQIS wiring entering the fuel tanks and the associated line replacement unit (LRU) were shown to have protective features such as separation (including circuit separation in the LRU) and shielding and/or transient suppression/energy limiting devices, the portion of the compliance demonstration for the associated wiring would likely be limited to showing the effectiveness of the features and defining any long-term maintenance requirements, including the mandatory replacement times, inspection intervals, related inspection procedures, or CDCCLs so that the protective features are not degraded.

Figure 1. Examples of Fuel Tank Ignition Source Considerations



5.2.2 In the case of the installation of a flame arrestor in the inlet line to a fuel pump, the compliance demonstration for the fuel pump may be limited to showing that the arrestor was effective at precluding propagation of the flame from the pump back down the inlet line into the tank, and showing that any anticipated failures or events could not violate the explosion-proof features of the pump assembly. A CDCCL may be necessary to maintain the flame arrestor design feature. If the flame arrestor cannot be shown to be effective for the life of the installation, an Airworthiness Limitation limiting the life of the flame arrestor would be necessary. In addition, revalidation of the fuel system with other regulations (e.g. icing and reduced flow due to contamination) would be required if modifications were incorporated into the fuel feed system. The SSA criteria, process, analysis methods, validation, and documentation should be consistent with the guidance material provided in SAE ARP4761, using the unique guidance specific to the fuel tank system as defined in this AMC.

5.3 Assumptions and considerations for fuel tank system analysis

The applicant should conduct the fuel tank system analysis based on the following assumptions:

5.3.1 Fuel tank flammability

The analysis should assume that the environment inside the fuel tank is always flammable. The conditions required to ignite fuel vapour from ignition sources vary with the pressures and temperatures within the fuel tank and can be affected by sloshing or spraying of fuel in the tank. Due to the difficulty in predicting fuel tank flammability, it should be assumed that a flammable fuel/air mixture exists in aeroplane fuel tanks and it is required that no ignition sources be present. The SSA should be prepared considering all the in-flight, ground, service, and maintenance conditions for the aeroplane, assuming that an explosive fuel/air mixture is present in the vapour space of fuel tanks and vent systems at all times, unless the fuel tank has features that mitigate the effects of tank ignition (e.g. polyurethane foam).

5.3.2 Failure condition classification

Unless design features are incorporated that mitigate the hazards resulting from a fuel tank ignition event (e.g. polyurethane foam, an adequate structural margin), the SSA should assume that the presence of an ignition source is a catastrophic failure condition.

5.3.3 Latent failures

5.3.3.1 In order to eliminate any ambiguity as to the restrictions on latent failures, CS 25.981(a)(3) explicitly requires that any anticipated latent failure condition must not leave the aeroplane one failure away from a catastrophic fuel tank ignition. In addition to this limitation on latency, CS 25.1309(c) limits the latent failure conditions to those that do not create an 'unsafe system operating condition.' Consequently, if a latent failure condition is not extremely remote (i.e., it is anticipated to occur) and it creates an 'unsafe system operating condition,' then flight crew alerting must be provided to 'enable them to take appropriate corrective action.' Notwithstanding these restrictions on latency, there are practical limitations on the available means of compliance. For example, detecting a failure condition requires a finite period of time, and there are not always 'appropriate corrective actions' that can be taken during the flight. Consequently, for the purpose of complying with CS 25.981(a)(3), the period of latency for any anticipated significant latent failure condition should be minimised and not allowed to exceed one flight cycle. For the purpose of complying with CS 25.1309(c), whenever the aeroplane is operating one failure away from a catastrophic fuel tank ignition, this should be considered an 'unsafe system operating condition,' recognising that sometimes the only appropriate corrective action when problem detection is available is to continue to the destination but not to initiate another flight without making appropriate repairs.

5.3.3.2 Another practical limitation on the available means of compliance is the technological feasibility of providing inherent failure detection within the design for all significant failures. Sometimes periodic inspection is the only practicable means of reliably detecting a failure condition. Consequently, when such inspections are identified within the analysis as the means of detection, the inspection method and frequency must be sufficient to conclude that the probability of occurrence of the significant latent failure condition is extremely remote.

5.3.3.3 Any mandatory replacement time, inspection interval, related inspection procedure, and all the CDCCLs identified as required to prevent development of ignition sources within the fuel tank system for CS 25.981(a) must be identified in the Airworthiness Limitations Section of the ICA as fuel system Airworthiness Limitations. The Airworthiness Limitations Section should include the following:

5.3.3.3.1 A designation of the maintenance actions and alterations that must be inspected (critical inspections), including at least those that could result in a failure, malfunction, or defect endangering the safe operation of the aircraft, if not performed properly or if improper parts or materials are used.

Note: A validation inspection should be conducted to reaffirm all or a portion of the initial inspection requirements for those critical inspections that, if not performed properly or if improper parts or materials are used, could result in a failure, malfunction, or defect endangering the safe operation of the aeroplane. For those air carriers that use a mechanic for the initial inspection, an inspector should be used to conduct the validation inspection. For those air carriers that use an inspector for the initial inspection, another qualified inspector should be used to conduct the validation inspection.

5.3.3.3.2 The procedures, standards, and limits necessary for critical inspections and acceptance or rejection of the items required to be inspected, and for periodic inspections and calibration of precision tools, measuring devices, and test equipment.

5.3.4 Failure conditions

In accordance with CS 25.981(a)(3), the analysis must consider the effects of manufacturing variability, ageing, wear, corrosion, and likely damage. For the purpose of compliance with CS 5.981, 'extremely remote' failure conditions and 'extremely improbable' failure conditions are defined in AMC 25.1309. Likely damage is damage that, using engineering judgment or past experience, would lead one to conclude that an occurrence is foreseeable. Examples of likely damage are:

— a wire bundle located where a mechanic could use it as a handhold;

— an instrument located where, if someone dropped a wrench, damage would result; or

— a fuel probe located where a mechanic could use it as a step in the tank.

5.3.4.1 The analysis should be conducted considering the deficiencies and anomalies listed in paragraph 2.3 of this AMC, the failure modes identified by the review of service information (including review of supplier service data), and any other failure modes identified by the functional hazard assessment of the fuel tank system. For example, the applicant should assume the presence of conductive debris such as lockwire, steel wool, nuts, bolts, rivets, etc. CS 25.981 requires that the effects of manufacturing variability, ageing, wear, corrosion, and likely damage must be considered when showing compliance, which is needed to show compliance with CS 25.901(c). Credit for fail-safe features must be substantiated.

5.3.4.2 The level of manufacturing variability, ageing, wear, corrosion, and likely damage that must be considered should be determined based upon an evaluation of the detectability of degraded or out-of-specification configurations, and established and documented within the analysis. In-service and production functional tests, component acceptance tests, and maintenance checks may be used to substantiate the degree to which these states must be considered. For example, inspection of fuel tank system bonding on production aeroplanes has shown that some bonds were inadequate. Functional testing of all bonding was incorporated to address this deficiency. In some cases (e.g. component bonding or ground paths), a degraded state will not be detectable without periodic functional tests of the feature. For these features, inspection/test intervals should be