25

Electromagnetic Environment (EME)

Richard Hess
Honeywell

25.1 Introduction

The advent of digital electronic technology in electrical/electronic systems has enabled unprecedented expansion of aircraft system functionality and evolution of aircraft function automation. As a result, systems incorporating such technology are used more and more to implement aircraft functions, including Level A systems that affect the safe operation of the aircraft; however, such capability does not come free. The EME (electromagnetic environment) is a form of energy, which is the same type of energy (electrical) that is used by electrical/electronic equipment to process and transfer information. As such, this environment represents a fundamental threat to the proper operation of systems that depend on such equipment. It is a common mode threat that can defeat fault-tolerant strategies reliant upon redundant electrical/electronic systems.

Electrical/electronic systems, characterized as Level A, provide functions that can affect the safe operation of an aircraft and depend upon information (i.e., guidance, control, etc.) processed by electronic equipment. Thus, the EME threat to such systems may translate to a threat to the airplane itself. The computers associated with modern aircraft guidance and control systems are susceptible to upset from lightning and sources that radiate RF at frequencies predominantly between 1 and 500 MHz and produce aircraft internal field strengths of 5 to 200 V/m or greater. Internal field strengths greater than 200 V/m are usually periodic pulses with pulsewidths less than 10 μs. Internal lightning-induced voltages and currents can range from approximately 50 V and 20 A to over 3000 V and 5000 A.

Electrical/electronic system susceptibility to such an environment has been suspect as the cause of "nuisance disconnects," "hardovers," and "upsets." Generally, this form of system upset occurs at significantly lower levels of EM field strength than that which could cause component failure, leaves no trace, and is usually nonrepeatable.

25.2 EME Energy Susceptibility

It is clear that the sources of electromagnetic (EM) threats to the electrical/electronic system, either digital or analog, are numerous. Although both respond to the same threats, there are factors that can make the threat response to a momentary transient (especially intense transients like those that can be produced by lightning) far more serious in digital processing systems than in analog systems. For example, the information bandwidth and, therefore, the upper noise response cutoff frequency in analog devices is limited to, at most, a few megahertz. In digital systems it is often in excess of 100 MHz and continues to increase. This bandwidth difference, which is at least 10 times more severe in digital systems, allows substantially more energy and types of energy to be coupled into the digital system. Moreover, the bandwidths of analog circuits associated with autopilot and flight management systems are on the order of 50 Hz for servo loops and much less for other control loops (less than 1 Hz for outer loops). Thus, if the disturbance is short relative to significant system time constants, even though an analog circuit device possessing a large gain and a broad bandwidth may be momentarily upset by an electromagnetic transient, the circuit will recover to the proper state. It should be recognized that, to operate at high speeds, proper circuit card layout control and application of high-density devices is a must. When appropriate design tools (signal integrity, etc.) are applied, effective antenna loop areas of circuit card tracks become extremely small, and the interfaces to a circuit card track (transmission line) are matched. Older (1970s–1980s) technology with wirewrap backplanes and processors built with discrete logic devices spread over several circuit cards were orders of magnitude more susceptible. Unlike analog circuits, digital circuits and corresponding computational units, once upset, may not recover to the proper state and may require external intervention to resume normal operation. It should be recognized that (for a variety of reasons) large-gain bandwidth devices are and have been used in the digital computing platforms of aircraft systems. A typical discrete transistor can be upset with 10^{-5} J, 2000 V at 0.1 mA for 50 μs. A typical integrated circuit can be upset with only 10^{-9} J, 20 V at 1 μA for 50 μs. As time goes on and processor semiconductor junction feature sizes get smaller and smaller, this problem becomes worse.

It should be noted that in addition to upset, lightning-induced transients appearing at equipment interfaces can, because of the energy they possess, produce hard faults (i.e., damage circuit components) in interface circuits of either analog or digital equipment. Mechanical, electromechanical, electrohydraulic, etc. elements associated with conventional (not electronic primary flight controls with associate "smart" actuators) servo loops and control surface movement are either inherently immune or vastly more robust to EME energy effects than the electronic components in an electrical/electronic system.

Immunity of electronic components to damage is a consideration that occurs as part of the circuit design process. The circuit characteristic (immunity to damage) is influenced by a variety of factors:

1. Circuit impedances (resistance, inductance, capacitance), which may be distributed as well as lumped;
2. The impedances around system component interconnecting loops along with the characteristic (surge) impedance of wiring interfacing with circuit components;
3. Properties of the materials used in the construction of a component (e.g., thick-film/thin-film resistors);
4. Threat level (open circuit voltage/short circuit current), resulting in a corresponding stress on insulation, integrated circuit leads, PC board trace spacing, etc.; and
5. Semiconductor device nonlinearities (e.g., forward biased junctions, channel impedance, junction/gate breakdown).

Immunity to upset for analog processors is achieved through circuit design measures, and for digital processors it is achieved through architectural as well as circuit design measures.

25.2.1 Soft Faults

Digital circuit upset, which has also been known by the digital computer/information processing community as a "soft fault," is a condition known to occur even in relatively benign operating environments. Soft faults occur despite the substantial design measures (timing margins, transmission line interconnects,

ground and power planes, clock enablers of digital circuits) to achieve a relatively high degree of integrity in digital processor operation.

In a normal operating environment, the occurrence of soft faults within digital processing systems is relatively infrequent and random. Such occasional upset events should be treated as probabilistic in nature and can be the result of:

- Coincidence of EME energy with clocked logic clock edges, etc.
- Occasional violation of a device's operational margin (resulting margin from the design, processing, and manufacturing elements of the production cycle).

From this perspective, the projected effect of a substantial increase in the severity of the electromagnetic environment will be an increased probability of a soft fault occurrence. That is, in reality a soft fault may or may not occur at any particular point in time but, on the average, soft faults will occur more frequently with the new environmental level.

Once developed, software is "burned into nonvolatile" memory (becomes "firmware"); the result will be a special purpose real-time digital electronic technology data processing machine with the inherent potential for "soft faults." Because it is a hardware characteristic, this potential exists even when a substantial amount of attention is devoted to developing "error-free" operating system and application programs(s) (software) for the general purpose digital machine (computing platform, digital engine, etc.).

25.2.2 MTBUR/MTBF

In the past, service experience with digital systems installed on aircraft has indicated that the confirmed failure rates equal or exceed predicted values that were significantly better than previous generation analog equipment. However, the unscheduled removal rate remains about the same. In general, the disparity in mean time between unscheduled removal (MTBUR) and the mean time between failure (MTBF) continues to be significant. The impact of this disparity on airline direct operating costs is illustrated in Figure 25.1.

To the extent that soft faults contribute to the MTBUR/MTBF disparity, any reduction in soft fault occurrence and propagation could translate into reduction of this disparity.

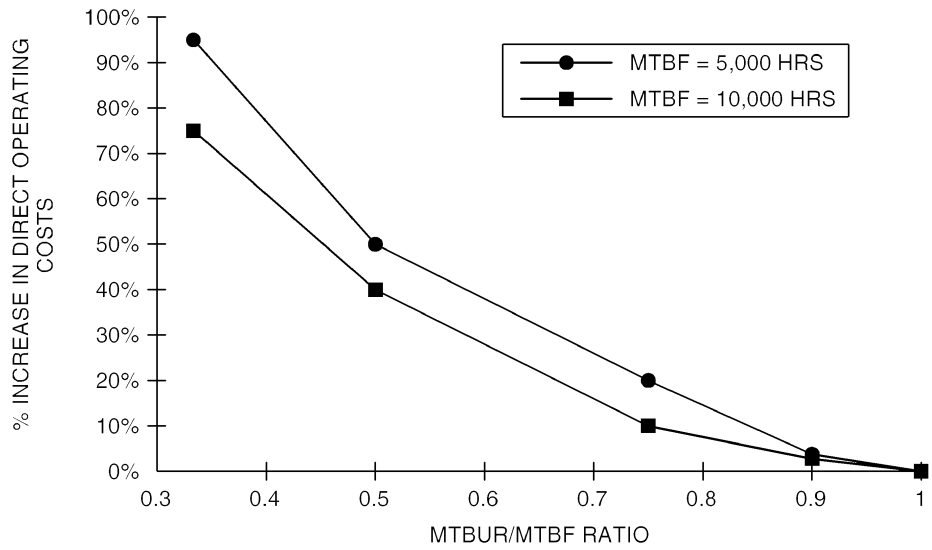


FIGURE 25.1 MTBUR/MTBF ratio impact of operating costs.

25.3 Civil Airworthiness Authority Concerns

The Federal Aviation Administration (FAA) and European Joint Aviation Authorities (more commonly known as JAA) have identified the lightning and High Intensity Radiated Field (HIRF) elements of the EME as a safety issue for aircraft functions provided by electrical/electronic systems.

The following factors, identified by the FAA and JAA, have led to this concern about lightning and HIRF effects:

- Increased reliance on electrical and electronic systems to perform functions that may be necessary for the continued safe flight and landing of the aircraft.
- Reduction of the operating power level of electronic devices that may be used in electrical and electronic systems, which may cause circuits to be more reactive to induced lightning and RF voltages and currents leading to malfunction or failure.
- Increased percentage of composite materials in aircraft construction. Because of their decreased conductivity, composite materials may result in less inherent shielding by the aircraft structure.
- Since current flowing in the lightning channel will be forced (during lightning attachment) into and through the aircraft structure without attenuation, decreased conductivity for aircraft structure materials can be particularly troubling for lightning.

The direct effects of lightning (dielectric puncture, blasting, melting, fuel ignition, etc.) have been recognized as flight hazards for decades, and in 1972 the SAE formed the AE4 Special Task F (which later became AE4L) to address this issue. In the early 1980s, the FAA began developing policy relative to the effects of lightning on electrical/electronic systems (indirect effects) and AE4L supported the FAA and JAA by providing the technical basis for international standards (rules/regulations) and guidance material that, for aircraft type certification, would provide acceptable means for demonstrating compliance to those rules/regulations. AE4L also supported RTCA Special Committee 135 (SC-135) to integrate lightning environment conditions and test procedures into airborne equipment standards (DO-160) and the EUROCAE standards counterpart (ED-14). In 1987, EUROCAE formed Working Group 31 to be the European counterpart of AE4L.

In 1986, the FAA and JAA identified High Energy Radio Frequency (HERF) electromagnetic fields as an issue for aircraft electrical/electronic systems. Some time later the term HERF was changed to its present designation, which is High Intensity Radiated Field (HIRF). Subsequent to the FAA identifying HIRF as a safety issue, SAE and EUROCAE formed Committee AE4R and Working Group 33, respectively, to support the FAA and JAA in much the same way as was the case with AE4L and lightning. In addition, unlike the case for lightning, RTCA SC-135 formed a HIRF working group (the corresponding European group was already part of EUROCAE/WG33) to integrate HIRF requirements into DO-160/ED-14.

In the interim between the absence and existence of a rule for lightning and HIRF, special conditions have been or are issued to applicants for aircraft type certification (TC, STC, ATC). The rationale for the special condition is given in words to the effect:

> These series of aircraft will have novel or unusual design features associated with the installation of new technology electrical and electronic systems, which perform critical or essential functions. The applicable airworthiness regulation does not contain adequate or appropriate safety standards for the protection of these systems from the effects of lightning and radio frequency (RF) energy. This notice contains the additional safety standards that the Administrator considers necessary to ensure that critical and essential functions the new technology electrical and electronic systems perform are maintained when the airplane is exposed to lightning and RF energy.

Presently, the FAA's Federal Aviation Regulations (FARs) have been updated to include the "indirect effects" of lightning, but not HIRF. In the time period between the absence and existence of a rule for HIRF, special conditions for HIRF are being issued to applicants for aircraft certification. However, the FAA has established the Aviation Rule-Making Advisory Committee, which in turn established the

Electromagnetic Effects Harmonization Working Group (EEHWG) to develop the rule-making package for HIRF and for amendments to the lightning rules.

Portable electronic devices (PEDs) have not been identified for regulatory action, but in 1992 the FAA requested the RTCA to study the EME produced by PEDs. In response to an FAA request relative to PEDs, RTCA formed Special Committee 177 (SC-177) in 1992. In 1996, SC-177 issued a report titled "Portable Electronic Devices Carried Onboard Aircraft" (DO-233). Currently, control of PEDs and their associated electromagnetic (EM) emissions are handled by integrating some of the RTCA recommendations into airline policy regarding instructions (prohibition of personal cellular phone use, turn-off of PEDs during taxi, take-off, and landing, etc.) given to passengers.

25.3.1 EME Compliance Demonstration for Electrical/Electronic Systems

FAA/JAA FAR(s)/JAR(s) require compliance demonstration either explicitly or implicitly for the following EME elements:

- Lightning
- HIRF (FAA)
- HIRF (JAA)
- EMC

At the aircraft level, the emphasis should be on lightning and HIRF because most of the energy and system hazards arise from these threats. Their interaction with aircraft systems is global and also the most complex, requiring more effort to understand. Intrasystem electromagnetic emissions fall under the broad discipline of EMC. PEDs are a source of EM emissions that fall outside of the categories of equipment normally included in the EMC discipline. Like lightning and HIRF, the interaction of PED emissions with aircraft electrical/electronic systems is complex and could be global.

The electrical and/or electronic systems that perform functions "critical" to flight must be identified by the applicant with the concurrence of the cognizant FAA ACO. This may be accomplished by conducting a functional hazard assessment and, if necessary, preliminary system safety assessments (see SAE ARP 4761). The term "critical" means those functions whose failure would contribute to, or cause, a catastrophic failure condition (loss of aircraft). Table 25.1 provides the relationship between function failure effects and development assurance levels associated with those systems that implement functions that can affect safe aircraft operation.

TABLE 25.1 Nomenclature Cross Reference Between AC25.1309 and SAE-ARP 4754

Failure Condition Classification	Development Assurance Level
Catastrophic	Level A
Severe Major/Hazardous	Level B
Major	Level C
Minor	Level D
No Effect	Level E

The terms "Level A," etc. designate particular system development assurance levels. System development assurance levels refer to the rigor and discipline of processes used during system development (design, implementation, verification/certification, production, etc.). It was deemed necessary to focus on the development processes for systems based upon "highly integrated" or "complex" (whose safety cannot be shown solely by test and whose logic is difficult to comprehend without the aid of analytical tools) elements, i.e., primarily digital electronic elements.

Development assurance activities are ingredients of the system development processes. As has been noted, systems and appropriate associated components are assigned "development assurance levels" based on failure condition classifications associated with aircraft-level functions implemented by systems and components.

The rigor and discipline needed in performing the supporting processes will vary, depending on the assigned development assurance level.

There is no development process for aircraft functions. Basically, they should be regarded as intrinsic to the aircraft and are categorized by the role they play for the aircraft (control, navigation, communication, etc.). Relative to safety, they are also categorized (from FAA advisory material) by the effect of their failures, i.e., catastrophic, severe major/hazardous, major, etc.

EMC has been included in FAA regulations since the introduction of radio and electrical/electronic systems into aircraft. Electrical equipment, controls, and wiring must be installed so that operation of any one unit, or system of units, will not adversely affect the simultaneous operation of any other electrical unit or system essential to aircraft safe operation. Cables must be grouped, routed, and spaced so that damage to essential circuits will be minimized if there are faults in heavy current-carrying cables. In showing compliance with aircraft electrical/electronic system safety requirements with respect to radio and electronic equipment and their installations, critical environmental conditions must be considered. Radio and electronic equipment, controls, and wiring must be installed so that operation of any one component or system of components will not adversely affect the simultaneous operation of any other radio or electronic unit, or system of units, required by aircraft functions.

Relative to safety and electrical/electronic systems, the systems, installations, and equipment whose functioning is required for safe aircraft operation must be designed to ensure that they perform their intended functions under all foreseeable operating conditions. Aircraft systems and associated components, considered separately and in relation to other systems, must be designed so that:

- The occurrence of any failure condition that would prevent the continued safe flight and landing of the airplane is extremely improbable.
- The occurrence of any other failure condition that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.

25.3.2 EME Energy Propagation

As has been noted in the introductory paragraph and illustrated in Figure 25.2, lightning and HIRF are threats to the overall aircraft. Since they are external EME elements, of the two, lightning produces the most intense environment, particularly by direct attachment.

Both lightning and HIRF interactions produce internal fields. Lightning can also produce substantial voltage drops across the aircraft structure. Such structural voltages provide another mechanism (in addition to internal fields) for energy to propagate into electrical/electronic systems. Also, the poorer the conductivity of structural materials, the greater the possibility that there are

- Voltage differences across the structure
- Significant lightning diffusion magnetic fields
- Propagation of external environment energy

Figure 25.3 gives the HIRF spectrum and associated aircraft/installations features of interest.

In general, the propagation of external EME energy into the aircraft interior and electrical/electronic systems is a result of complex interactions of the EME with the aircraft exterior structures, interior structures, and system installations (see Figures 25.3 through 25.7). Figure 25.8 gives representative transfer functions, in the frequency domain, of energy propagation into electrical/electronic systems, and Figure 25.9 provides time domain responses to a lightning pulse resulting from transfer functions having the low-frequency characteristic $V_o(f) = kf[Hi(f)]$ and a high frequency "moding" (resonant) characteristic (e.g., open loop voltage of cabling excited by a magnetic field; see Figure 25.8).

Paths of electromagnetic wave entry from the exterior to the interior equipment regions are sometimes referred to as points of entry. Examples of points of entry may be seams, cable entries, windows, etc. As noted, points of entry are driven by the local environment, not the incident environment. The internal field levels are dependent on both the details of the point of entry and the internal cavity.

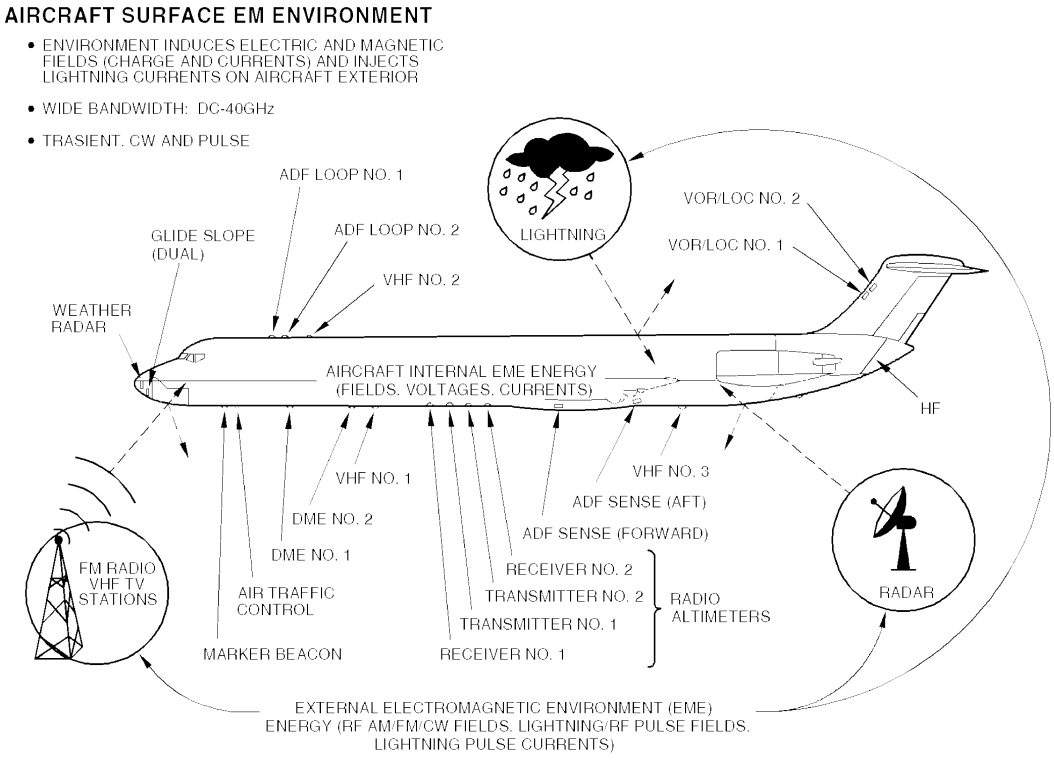


FIGURE 25.2 External EME (HIRF, lightning) interaction.

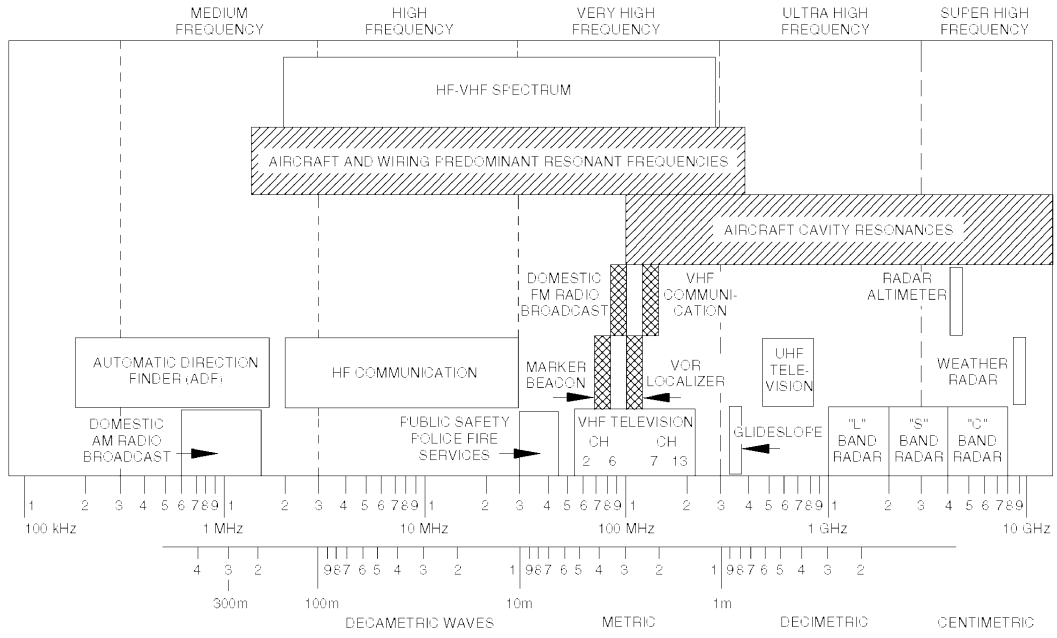


FIGURE 25.3 RF spectrum and associated installation dimensions of interest.

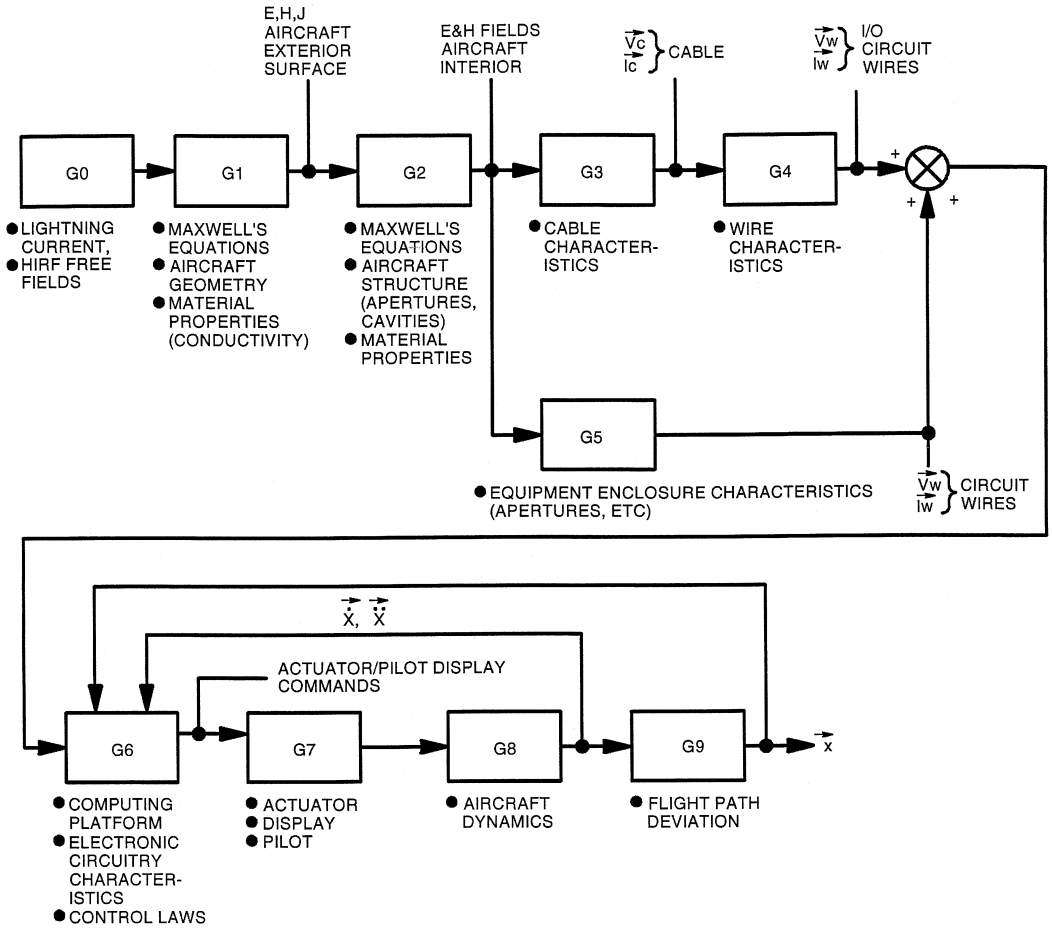
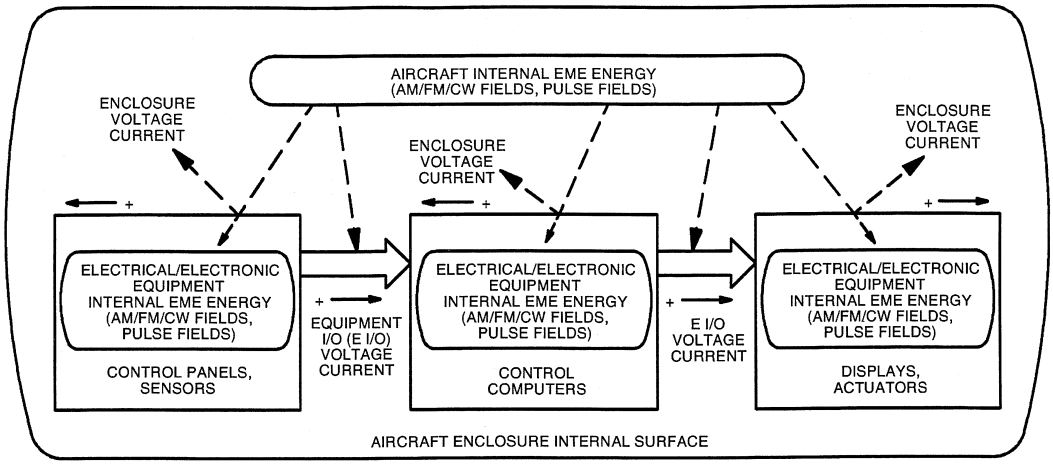


FIGURE 25.4 EME propagation process transfer function perspective.

Resulting internal fields can vary over a wide range of intensity, wave shape, and wave impedance. (Below 10 MHz within a metal aircraft, the magnetic fields due to lightning predominate because of the electric field shielding properties of metal skins. For HIRF "high-frequency" bands in some internal regions, internal field levels may exceed the incident field levels.)

The EME local to the equipment or system within the installation (the EME energy coupled to installation wiring which appears at equipment interface circuits) and the degree of attenuation or enhancement achieved for any region are the product of many factors such as external EME characteristics, materials, bonding of structure, dimensions and geometric form of the region, and the location and size of any apertures allowing penetration into the aircraft (G0 through G5 of Figure 25.4 which could have any of the characteristics of Figure 25.8.)

In HIRF high-frequency bands (frequencies on the order of 100 MHz and higher) the internal field resulting from such influences, as noted above, will in most cases produce a nonuniform field within the region or location of the system or equipment. The field cannot be considered as uniform and homogeneous. The field will not necessarily allow the adoption of single-point measurement techniques for the accurate determination of the equivalent internal field for to be used as the test level for systems. Several hot spots typically exist within any subsection of the aircraft. This is particularly true at cavity resonant conditions. Intense local effects are experienced at all frequencies in the immediate vicinity of any apertures for a few wavelengths away from the aperture itself. For apertures small with respect to wavelength, measurements of the fields within the aperture would yield fields much larger than those



- External energy penetrates to interior via apertures, composites, seams, joints, and antennas
- Voltages and currents induced on flight control system components and cables
  - RF energy below 1 megahertz - induced coupling at these frequencies is inefficient and thus will probably be of lesser concern
  - RF energy between 1 and 300 megahertz is of major concern as aircraft wiring, when their lengths are on the order of a wavelength divided by two ($\lambda/2$) or longer at these frequencies, acts as a highly efficient antenna
  - RF energy coupling to aircraft wiring drops off at frequencies above 300 megahertz (at these higher frequencies, the EM energy tends to couple through box apertures rather than through aircraft wiring)

FIGURE 25.5 Aircraft internal EME energy electrical/electronic system.

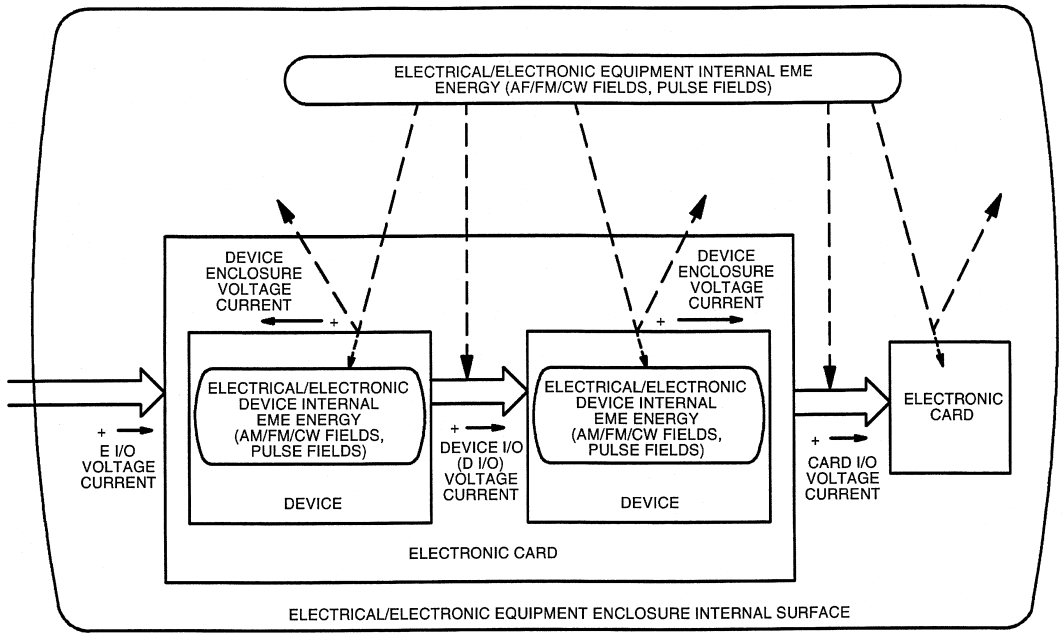
further inside the aircraft because the fields fall off inversely proportional to radius cubed. For apertures on the order of a wavelength in size or larger, the fields may penetrate unattenuated.

The HIRF spectrum of RF energy that couples into aircraft wiring and electrical/electronic systems can be summarized into three basic ranges:

- HIRF energy below 1 MHz — induced coupling at these frequencies is inefficient and thus will be of lesser concern.
- HIRF energy between 1 and 400 MHz — induced coupling is of major concern since aircraft wiring acts as a highly efficient antenna at these frequencies.
- HIRF energy above 400 MHz — coupling to aircraft wiring drops off at frequencies above 400 MHz. At these higher frequencies the EM energy tends to couple through equipment apertures and seams and to the quarter wavelength of wire attached to the line replaceable unit (LRU). In this frequency range, aspects of equipment enclosure construction become important.

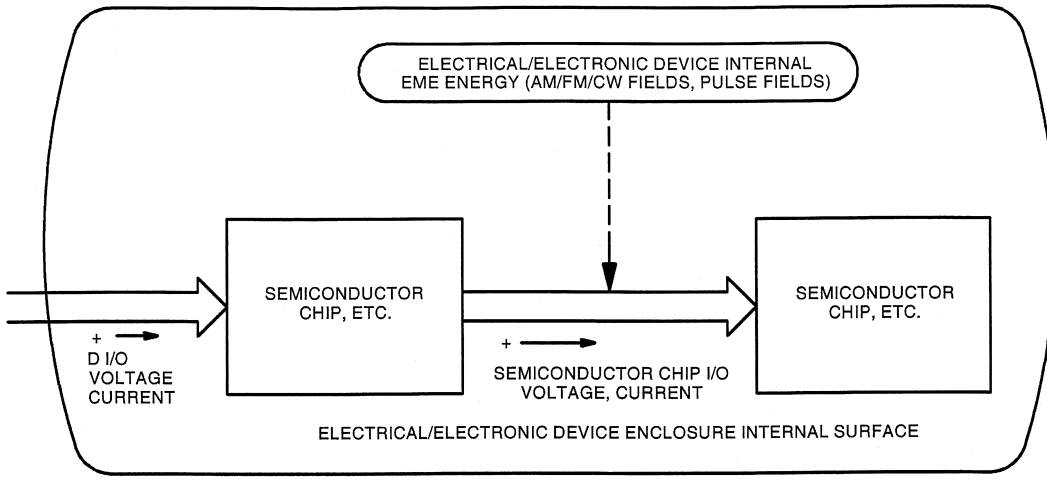
The extension of electrical/electronic systems throughout the aircraft ranges from highly distributed (e.g., flight controls) to relatively compact. Wiring associated with distributed systems penetrates several aircraft regions. Some of these regions may be more open to the electromagnetic environment than others, and wiring passing through the more open regions is exposed to a higher environment. Thus, at frequencies below 400 MHz, the wiring of a highly distributed system could have a relatively wide range of induced voltages and currents that would appear at equipment interface circuits.

The flight deck of the aircraft is an example of an open region. The windscreen "glass" presents approximately zero attenuation to an incoming field at and above the frequency for which its perimeter is one wavelength. Some enhancement above the incident field level generally exists in and around the aperture at this resonance condition.



- Voltage, fields, currents and charge on system components penetrate into equipment enclosure interiors via holes, seams, and airplane wiring (cables)
- Energy (voltage and current) picked up by wires and printed conductors on cards and carried to electronic devices

FIGURE 25.6 Electrical/electronic equipment internal EME interaction electrical/electronic circuitry.



- Card and device conductors carry energy to the semiconductor chips, etc.
- Possible effects
  - Damage
  - Upset

FIGURE 25.7 Electrical/electronic device internal EME interaction electrical/electronic circuitry.

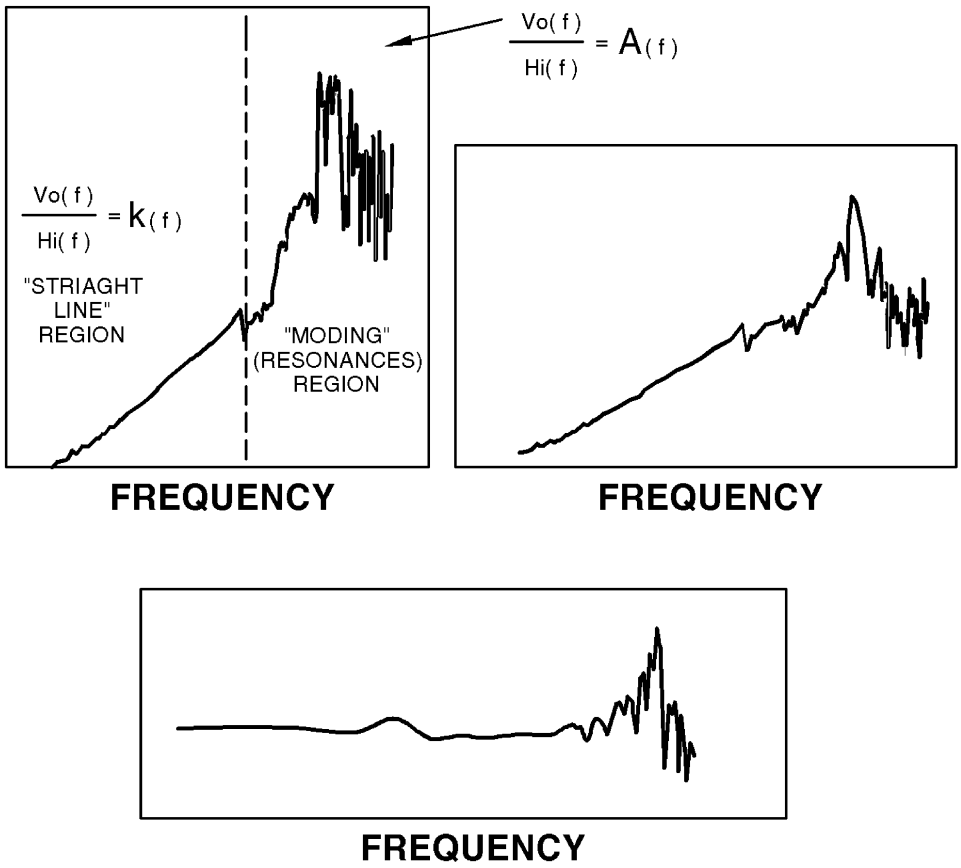


FIGURE 25.8 Frequency domain representation of EME energy attenuation/coupling transfer functions.

Lightning is a transient electromagnetic event, as is the resulting internal environment. Relative to a spectral representation, lightning energy would be concentrated in the zero to 50 MHz range (most energy is below 3 MHz). However, since lightning is such an intense transient, significant energy can be present up to and sometimes above 10 MHz.

Relative to the higher frequency range (above 100 MHz) strong resonances of aircraft interior volumes (cavities) such as the flight deck, equipment bay, etc, could occur. At the very high frequencies the EME can be in the form of both very intense and very short duration. From a cavity resonance issue, since the time constant of a relatively good cavity resonator is on the order of 1 μs, the pulse can be gone before significant field energy is developed within the cavity.

25.4 Architecture Options for Fault Mitigation

New system architecture measures have been evolving which could complement/augment traditional schemes to provide protection against EME energy effects. Architecture options can be applied at the overall system level or within the digital computing platform for the system. These options include the following:

- Distributed bus architecture
- Error Detection and Corrective (EDC) schemes
- Fiber optic data transfer
- Computation recovery

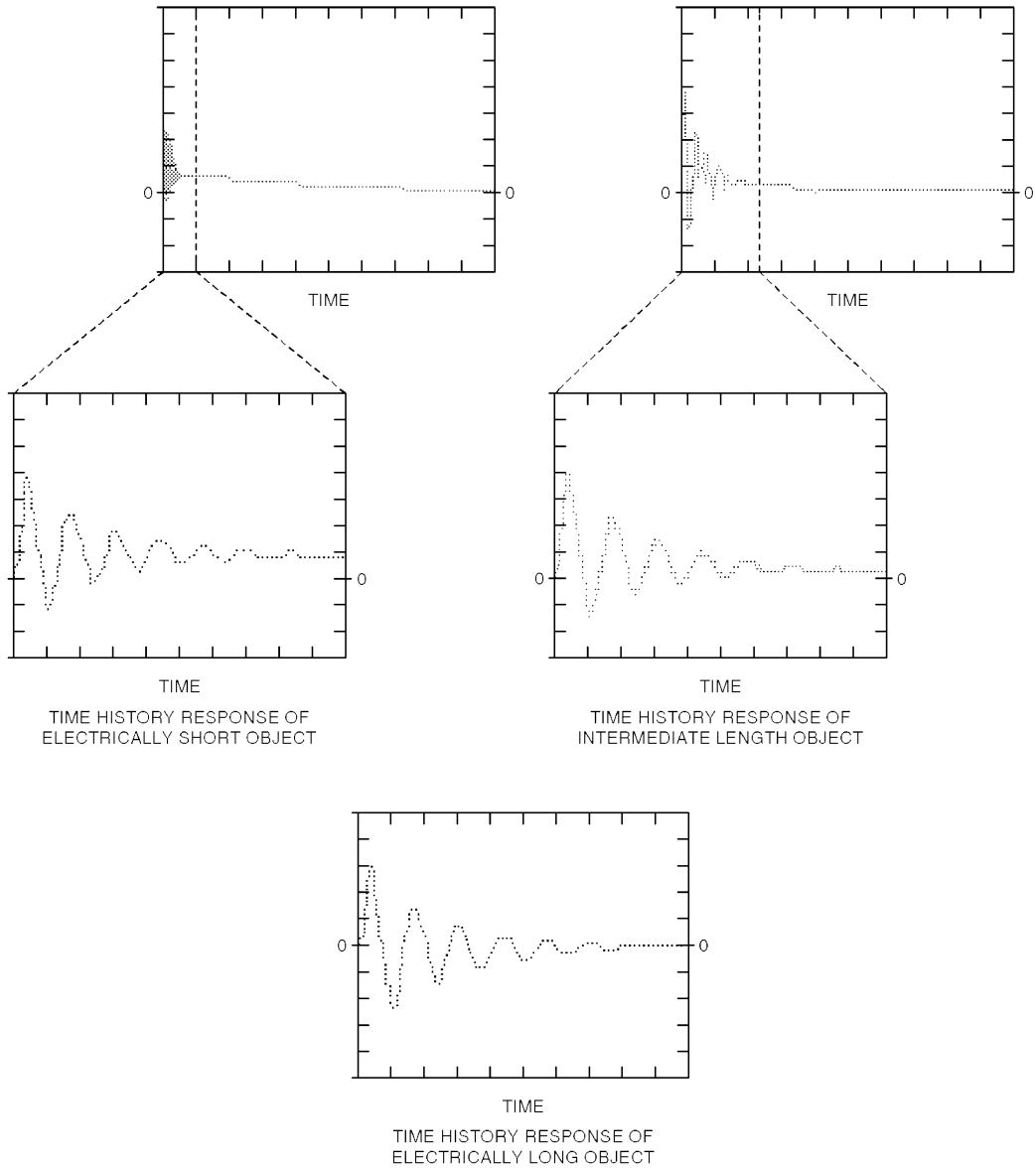


FIGURE 25.9 Responses for lightning EM pulse field interaction with objects of different "electrical lengths."

25.4.1 Electrical/Electronic System

In the past, soft faults in digital avionics were physically corrected by manual intervention, recycle power, etc. More recently, system-level measures for the automatic correction of soft faults have begun to be developed. It is perceived that significant benefits can be gained through soft fault protection measures designed into the basic system mechanization. System-level soft fault protection methodologies provide the ability to tolerate disruption of either input/output data or internal computation. Accordingly, there are two distinct classes of disruption:

- Disruption at the system equipment interface boundary causing corruption of data flowing to or from the affected subsystem.

- Disruption that reaches within system equipment to corrupt internal data and computation. As a worst case scenario, it must be presumed that any memory elements within the computational machine (registers, memory, etc.) may be affected at the time of disruption.

The short-term disruption of input/output data at an equipment boundary can be managed via a variety of existing methodologies. Data errors must be detected and the associated data suppressed until the error status is cleared. The data processing algorithm should tolerate data loss without signaling a hard fault. The length of time that can be tolerated between valid refreshes depends on the data item and the associated time constants (response) of the system and corresponding function being implemented.

The ability to tolerate disruption that reaches computation and memory elements internal to system equipment without propagation of the associated fault effect is a more difficult problem. For systems with redundant channels, this means tolerance of the disruption without loss of any of the redundant channels. Fault clearing and computation recovery must be rapid enough to be "transparent" relative to functional operation and flight deck effects.

Such computational recovery requires that the disruption be detected and then the state of the affected system be restored. Safety-critical systems are almost always mechanized with redundant channels. Outputs of channels are compared in real time, and an errant channel is blocked from propagating a fault effect. One means available for safety-critical systems to detect disruption is the same cross-channel monitor. If a miscompare between channels occurs, a recovery is attempted. For a hard fault, the miscompare condition will not have been remedied by the recovery attempt.

A basic approach to "rapid" computational recovery would be to transmit function state variable data from valid channels to the channel that has been determined faulted and for which a recovery is to be attempted (Figure 25.10). However, the cross-channel mechanization is ineffective against a disruption that has the potential to affect all channels.

25.4.2 Digital Computing Platform

The platform for the Airplane Information Management System (AIMS) used on Boeing 777 aircraft and Versatile Integrated Avionics (VIA) technology is an example of an architectural philosophy in the design of computing platforms. Essentially, VIA is a repackaged version of the AIMS technology. As mentioned, first-generation digital avionics have been plagued with high MTBUR (no-fault-found) rates.

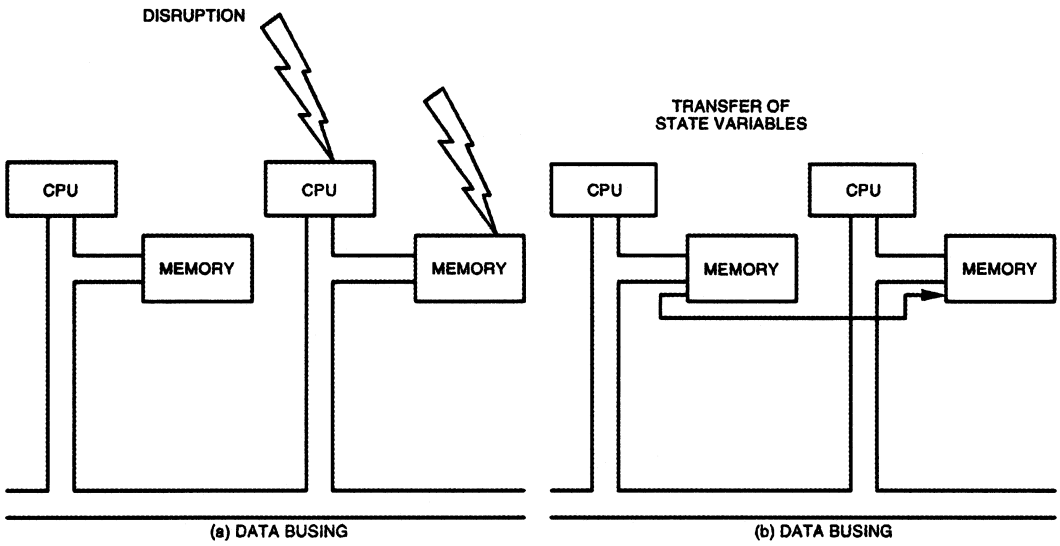


FIGURE 25.10 Redundant CPUs cross-lane recovery (can accomplish some degree of "rapid" recovery).

One primary goal of the Boeing 777 program was to greatly improve operational readiness and associated life-cycle cost performance for the airlines. The AIMS functionally redundant, self-checking pairs architecture was specifically selected to attack these problems. The high integration supported by AIMS required a very comprehensive monitoring environment that is ideal for in-channel "graceful" recovery.

In AIMS, the more dramatic step of making hardware monitoring active on every CPU clock cycle was taken. All computing and I/O management resources are lockstep compared on a processor cycle-by-cycle basis. All feasible hardware soft or hard faults are detected. In this approach, if a soft or hard fault event occurs, the processor module is immediately trapped to service handlers and no data can be exported. In past systems, the latency between such an event and eventual detection (or washout) was the real culprit. The corrupted data would propagate through computations and eventually affect some output. To recover, drastic actions (reboots or rearms) were often necessary. In AIMS, critical functions such as displays (because the flight crew could "see" hiccups) have a "shadowing" standby computational resource. The shadow sees the same input set at the same time as the master self-checking pair. If the master detects an event, within nanoseconds the faulty unit is blocked from generating outputs. The Honeywell SAFEbus® system detects the loss of output by the master and immediately passes the shadow's correct data for display.

In the faulted processor module, the core system has two copies of processor "state data" fundamental in the self-checking pair. Unlike past systems where the single thread processor may be so defective it cannot record any data, at least one half of the AIMS self-checking pair should be successful. Thus, the process of diagnosing hardware errors involves comparing what each half of the pair thought was going on. Errors, down to processor address, control, or data bits can be easily isolated. If the event was a soft fault, the core system allows a graceful recovery before the processor module is again allowed to export data. On the surface it appears to be a more sensitive system. However, even with the comprehensive monitoring (potentially a brittle operation), from the standpoint of a self-checking (dual-lockstep) pairs processor data comparison, in these platforms the automatic recovery capabilities should provide a compensating, more robust operation. In other words, from a macro time perspective, system functions will continue to be performed even though, on a micro time basis, a soft fault occurred.

In addition to the isolation of hardware faults (hard or soft), effective temporal and physical partitioning for execution of application software programs involving a variety of software levels has been achieved by the monitoring associated with the self-checking pairs processor and a SAFEbus® communication technology approach.

Defining Terms

DO-160: RTCA Document 160, Environmental Conditions and Test Procedures for Airborne Equipment, produced by RTCA Special Committee 135. Harmonized with ED-14.

ED-14: EUROCAE Document 14, Counterpart to DO-160, produced by EUROCAE Working Groups 14, 31, and 33. Harmonized with DO-160.

EMC: Electromagnetic Compatibility is a broad discipline dealing with EM emissions from and susceptibility to electrical/electronic systems and equipment.

EME: Electromagnetic Environment, which for commercial aircraft, consists of lightning, HIRF, and the electrical/electronic system and equipment emissions (intra and inter) portion (susceptibility not included) of EMC.

MTBF: Mean Time Between Failures (World Airlines Technical Operations Glossary).

MTBUR: Mean Time Between Unscheduled Removals (World Airlines Technical Operations Glossary).

EUROCAE: European Organization for Civil Aviation Equipment; for the European aerospace community, serving a role comparable to that of the RTCA and SAE.

PED: Portable Electronic Device, an emerging source of EM emissions not included in the EMC discipline.

References

1. AC25.1309, "System Design and Analysis."
2. SAE ARP-4761, "Guidelines and Tools for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," issued December, 1996.
3. SAE ARP-4754, "Certification Consideration for Highly Integrated or Complex Aircraft Systems," issued November, 1996.
4. R.F. Hess, "Options for Aircraft Function Preservation in the Presence of Lightning," *Int. Conf. Lightning Static Electr.*, Toulouse, France, June 1999.
5. Aviation Regulations
   XX.581 Lightning Protection
   XX.1316 System Lightning Protection
6. AC/AMJ 20-136, "Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning."
7. N8110.67 (FAA Notice), "Guidance for the Certification of Aircraft Operating in High Intensity Radiated Field (HIRF) Environments."
8. SAE ARP5413, "Certification of Aircraft Electrical/Electronic Systems for the Indirect Effects of Lightning," issued August, 1999.
9. SAE AE4L Report: AE4L-87-3 ("Orange Book"), "Certification of Aircraft Electrical/Electronic Systems for the Indirect Effects of Lightning," September 1996 (original publication February 1987).
10. SAE ARP5412, "Aircraft Lightning Environment and Related Test Waveforms," 1999.
11. SAE Report: AE4L-97-4, "Aircraft Lightning Environment and Related Test Waveforms Standard," July 1997.
12. EUROCAE ED-14D/RTCA DO-160D, "Environmental Conditions and Test Procedures for Airborne Equipment."
13. MIL-STD-464, "Electromagnetic Environmental Effects Requirements for Systems."
14. Clarke, Clifton A. and Larsen, William E., FAA Report DOT/FAA/CT 86/40, "Aircraft Electromagnetic Compatibility," June 1987.
15. Hess, R.F. "Implications Associated with the Operation of Digital Data Processing in the Relatively Harsh EMP Environments Produced by Lightning," *Int. Aerosp. and Ground Conf. Lightning and Static Elect.*, Paris, France, June 1985.