NASA Technical Memorandum 101665

LABORATORY TEST METHODOLOGY FOR EVALUATING THE EFFECTS OF ELECTROMAGNETIC DISTURBANCES ON FAULT-TOLERANT CONTROL SYSTEMS

CELESTE M. BELCASTRO

November 1989

National Aeronautics and Space Administration

Langley Research Center
Hampton, Virginia 23665-5225

Laboratory Test Methodology for Evaluating the Effects of Electromagnetic Disturbances on Fault-Tolerant Control Systems

Celeste M. Belcastro
NASA Langley Research Center
Hampton, VA 23665-5225

ABSTRACT

Control systems for advanced aircraft, and especially those with relaxed static stability, will be critical to flight and will, therefore, have very high reliability specifications which must be met for adverse as well as nominal operating conditions. Severe operating conditions can result from electromagnetic disturbances caused by lightning, high energy radio frequency (HERF) transmitters, and nuclear electromagnetic pulses (NEMP). For this reason, tools and techniques must be developed to verify the integrity of the control system in adverse operating environments. The most difficult and illusive perturbations to computer-based control systems that can be caused by an electromagnetic environment (EME) are functional error modes that involve no component damage. These error modes are collectively known as "upset", can occur simultaneously in all of the channels of a redundant control system, and are software dependent. Upset studies performed to date have not addressed the assessment of multi-channel systems and do not involve the evaluation of a control system operating in a closed-loop with the plant. This paper presents a methodology for performing upset tests on a multi-channel control system. In particular, the paper discusses

considerations for the design of upset tests to be conducted in the laboratory on fault-tolerant control systems operating in a closed loop with a simulated plant. Some of the considerations discussed are the generation and coupling of analog signals representative of electromagnetic disturbances to a control system under test, analog data acquisition, and digital data acquisition from multi-channel systems. In addition, the paper presents a case study of an upset test methodology for a fault-tolerant electronic engine control system.

I. Introduction

Advanced aircraft designs reduce aerodynamic drag via relaxed static stability and, therefore, control systems that are critical to the flight of the aircraft are required to maintain stability. In addition, fuel efficiency is greatly improved in advanced designs by using light-weight nonmetallic (composite) aircraft structures, rather than the metal ones currently in use. The trend in avionics technology is the implementation of control laws on digital computers that are interfaced to the sensors and control surfaces of the aircraft. Since digital computers are highly susceptible to transient electrical signals, the use of digital controls compounds the problem already incurred through the use of composite structures which do not provide the electrical shielding inherent in metal. As the function of the control system becomes more flight critical and the use of composite materials becomes more widespread, the problem of verifying the integrity of the control in adverse, as well

as nominal, operating environments becomes a key issue in the development of a control system.

One particularly harsh operating environment results from the presence of electromagnetic fields caused by sources such as lightning, high energy radio frequency (HERF) transmitters, and nuclear electromagnetic pulses (NEMP). As shown in Fig. 1, sources such as lightning, HERF, and NEMP generate electromagnetic fields outside of the aircraft which are dependent on the aircraft's geometry and structural material. These exterior electromagnetic fields penetrate the aircraft by leaking through joints, seams, and apertures so that interior electromagnetic fields are present. The interior fields cause analog electrical transients to be induced on the aircraft's wiring, and these signals can propagate to the onboard electronic equipment despite shielding and protective devices such as filters and surge suppressors. There are two types of effects to digital computer systems that can be caused by transient electrical signals. The first is actual component damage that requires repair or replacement of the equipment. The second type of damage to a digital system is characterized by functional error modes collectively known as "upset" which involve no component damage. In the case of upset, normal operation can be restored to the system by corrective action such as resetting/reloading the software or by an internal recovery mechanism, such as an automatic rollback to a system state just prior to the disturbance. The subject of effective internal upset recovery mechanisms is another current topic for research. See reference [1] for a more detailed account of the electromagnetic threat to advanced digital avionics systems.

To date, there are no comprehensive guidelines or criteria for performing tests or analyses on digital control systems to evaluate upset susceptibility or verify control integrity in electromagnetically adverse operating environments. Therefore, the objective of this research is to develop a methodology whereby a digital computer-based control system can be evaluated for upset susceptibility as well as control integrity when subjected to analog transient electrical signals like those that would be induced by an electromagnetic source. The electromagnetic source under consideration in this research is lightning. This paper discusses various issues in the design and implementation of upset tests which can be performed in the laboratory on a candidate fault-tolerant control system. A case study is described involving the upset test design of a full-authority electronic engine controller (EEC).

II. Upset Test Design for Fault-Tolerant Control Systems

Most upset studies conducted to date have involved general-purpose systems executing a generic application code during testing [2] - [6]. One upset study involved the evaluation of an Inertial Navigation System that was subjected to transient signals like those that could result from NEMP [7]. Since none of these studies involved a control system that has closed-loop dynamics with a plant, it is desirable that an upset methodology be formulated for such a system. The general laboratory test configuration for the upset evaluation of a control system is shown in Fig. 2. As shown in the figure, the test configuration involves two control units - the unit

under test and an unperturbed reference unit. The controller under test is perturbed by transient signals like those that could be induced by lightning. Each controller is interfaced to a simulation (hardware or software) of the plant in such a manner as to represent the closed-loop dynamics of the system. The operation of the two plant simulations are compared during tests so that cases in which acceptable control is not maintained by the faulted controller can be flagged in real time. Data obtained from the controllers during tests are stored for post processing and analysis. An alternative to having a faulted and reference controller is to have one controller which would be run with the plant simulation without faults for a period of time in a so-called "gold run". Unfaulted data would be recorded from the controller as well as the nominal operating parameters of the plant. Then, the plant parameter data obtained during faulted runs would be compared after testing to the nominal data and a determination made regarding the control integrity of the faulted controller. Since use of the two controllers would save a step in data processing, it is advantageous to use this configuration if two prototype controllers are available.

A. Generation of Analog Transients in the Laboratory

The waveform, shown in Fig. 3, that is most representative of those that occur on internal aircraft wiring due to lightning is a 1 - 50 MHz damped sinusoid which decreases in amplitude 50 - 75 % after four cycles [8]. This waveform can be generated by a capacitor discharge circuit with light damping [9]. However, use of a simple

RLC circuit is awkward because components must be changed in order to generate key frequencies in the 1 - 50 MHz range. Three pulse generators have been designed to fulfill the electromagnetic test requirements of the Royal Aerospace Establishment [10]. One pulse generator produces damped sinusoidal waveforms from 2 - 30 MHz, one is a fixed-frequency 100 kHz generator, and the third produces two waveforms for ground voltage lightning effects simulation.

The most versatile way to generate the transient signal, and the technique presented here, is a polynomial waveform synthesizer, which generates the waveform that corresponds to the entered equation. The output of the waveform generator can then be scaled to the proper amplitude via a wideband power amplifier. In this way, transient signals can be easily generated that cover a frequency range of interest and represent the induced effects of any electromagnetic source.

B. Coupling Analog Transients to the Controller Under Test

The mechanism for coupling analog signals into the digital controller must be such that the controller is not loaded down by mismatched impedance. In addition, the coupling mechanism must be representative of that which would occur in the natural operating environment, depicted in Fig. 1. The most widely used coupling techniques are resistive and inductive coupling. An advantage to resistive coupling is that no special equipment is needed. In addition, it is very easy using resistive coupling to inject transient

signals into integrated circuit pins as well as printed circuit board test points. The coupling method which best satisfies the above criteria is to induce voltage into a cable or cable bundle using a ferrite coupling transformer that can be clamped around the cable or bundle. Details of performing such tests are given in [11] and [12].

Another consideration is whether the transient signal injection should be synchronized with the operation of the controller or whether the transient should be injected asynchronously. If the transient is injected synchronously, it must be introduced into the controller during each operational state of the processor. Since the number of states in a digital control system is very large, the required amount of testing for this approach is impractical. For this reason, asynchronous injection of a statistically significant number of transient signals is more advantageous. In addition, asynchronously injected transients can occur during the transition between states and, therefore, more realistically represent the threat that could occur in a natural environment.

C. Controller Monitoring Strategies

In single channel systems, upset modes can be fairly easily detected using comparison monitoring techniques on a test unit and reference unit executing identical software and operating in bit synchronism. Any time the data bus, address bus, or control lines of the test unit differ from those of the reference unit, data can be recorded and analyzed. In this way, data is only recorded for transient injections from which errors have occurred. (It was

established in [2] and [3] that the occurrence and type of upset depends on the relative timing of the transient injection and the state of the processor. For this reason, upset does not occur each time the transient signal enters the system.) An advantage to this technique is that, since error-free data is not recorded, the amount of required data reduction is reduced. In addition, this method inherently provides very broad upset detection criteria.

Conversely, upset detection in fault-tolerant systems is much more complex. Fault-tolerant controllers usually employ one of two basic redundancy strategies - voting or primary/secondary channels. Comparison monitoring techniques cannot be used in upset testing of fault-tolerant systems since reconfigurations in the test unit would cause miscomparisons to be generated without faulty operation being present. For these types of systems, upset detection criteria must be carefully selected since they effectively define upset for the test unit.

D. Data Acquisition

It is recommended that both analog and digital data be recorded during upset tests. The analog data to be recorded are the waveforms induced in the digital controller. In this way, various threshold characteristics of transient signals that cause upset can be determined. Norms such as peak absolute amplitude, maximum absolute rate of rise, peak absolute impulse, rectified impulse, and root action integral have been suggested in the literature for measuring NEMP stress waveform attributes [13]. These norms were used in an NEMP upset study and found to be inadequate [7].

Therefore, appropriate frequency-dependent norms for characterizing upset stress attributes of electromagnetically induced transient signals from sources such as lightning, HERF, and NEMP remains a topic for further research.

Digital data to be acquired from the controller should include the calculated control commands obtained from the data bus, the internal status word of the processor, as well as the address bus and appropriate processor control lines. Range checks can be used to determine if the calculated control commands are appropriate for the control regime in progress. Commands that would be acceptable in one control mode could be devastating in another, so calculated command data can only be evaluated in the context of the application. The internal status word of the processor should be monitored for the results of self tests, parity checks, and other fault-tolerant strategies that might be present in the digital controller under test. Monitoring the results of the processor's own self-health evaluation can signal the beginning of a functional error mode or upset. Upset modes that occur without indication from self-health checks may suggest self tests that could be effective against upset in future processor designs. Monitoring address bus activity establishes cases in which the processor accesses invalid or nonexistent memory space. When this happens, the processor executes whatever data word it finds there as a valid instruction and often never returns to the correct memory space or correct operation until the system is reinitialized. Monitoring the control lines of the processor establishes the operational mode of the processor and, therefore, enables the experimenter to determine if invalid memory space data has been

decoded as an instruction. Exact details of the digital data acquisition are dependent on the controller under test.

In redundant systems with voting, the digital data described above must be obtained from all processors as well as the voter, and reconfiguration data must also be obtained. In redundant systems with primary/secondary channels, the digital data described above as well as the flags and signals related to which channel is in primary control and which is commanding the various control loops must be recorded. Digital data recorded from multiprocessor systems should be time-stamped so that concurrent activities of processors in the system can be correlated for post processing.

III. Case Study: Upset Test Set-up for a Fault-Tolerant Engine Controller

The upset test methodology for digital controllers described in Section II is planned to be applied to an electronic engine control (EEC) unit. The EEC is a commercial controller manufactured by the Hamilton Standard Division of United Technologies, which provides electronic controls for Pratt & Whitney engines. The EEC is a full-authority engine controller and is a dual-channel system which operates with a primary/secondary channel strategy. A block diagram of the EEC is shown in Fig. 4. As shown in the diagram, the EEC receives signals from the airframe, actuator position sensors, and engine parameter sensors. The inputs to each channel are also available to the other channel so that the best inputs can be selected by both channels. The control commands are calculated with the

selected inputs and one output is selected to be sent to the actuators. In addition to its control function, the EEC performs a comprehensive self-health evaluation during background activity.

The EEC to be used in the test set-up is a modified version of the commercial unit. Modifications to the EEC include access to the data bus, address bus, and control lines of the microprocessors of each channel to enable measurements in the laboratory. In addition, nominal flight parameter values for eight different flight conditions are stored in Read Only Memory (ROM) as well as the nominal values for all but three of the engine parameters. The eight flight conditions to be used during tests are take-off, cruise, acceleration, deceleration, reverse, idle, partial power, and climb. The variable inputs to the EEC are Throttle Resolver Angle (TRA), Inlet Air Temperature (T2), and Engine Speed (N1). These inputs can be varied for the eight flight cases during testing, and will be initially generated as shown in Fig. 5. The TRA input will be generated using a resolver, T2 will be generated using a resistive potentiometer, and N1 will be generated using a pulse generator. Therefore, for initial tests, the EEC will be running open-loop and the calculated commands will be stored in memory. In the next testing phase, these three loops will be closed so that the dynamics of the controller and plant can be simulated in real time. Subsequent plans are to modify the EEC so that additional variable inputs are provided.

During testing, each processor in both the test unit and reference unit will be monitored for activity on the data bus, address bus, and control lines. Upset for the EEC will initially be defined as:

(i) Selected parameter values for N1, T2, TRA are out of range for n cycles;

(ii) Calculated control commands are out of range for the given flight mode for n cycles;

(iii) Invalid memory space is accessed for n cycles.

Indication of the occurrence of any of these activities on the data bus, address bus, and control lines of the processors in the test unit will result in the data being recorded for that test run. As testing proceeds, the list of activities defining upset for the EEC will be expanded as necessary.

A block diagram of the upset test instrumentation is shown in Fig. 6. The damped sinusoidal waveform of Fig. 3 is generated by a polynomial waveform synthesizer and amplified by a wideband power amplifier with a maximum output power of 1000 W and a frequency range of 10 kHz - 220 MHz. This analog signal is inductively coupled into the EEC and the induced waveform is recorded on a waveform digitizer/analyzer on which some analysis, such as FFT and energy/power spectrum, can be performed directly. Digital data from the EEC is recorded on a digital analysis system with 240 input lines that can capture data from four microprocessors simultaneously with time correlation. Data can be displayed on the digital analysis system in timing, state, or graphical format. Analog and digital data from the waveform digitizer/recorder and the digital analysis system are then transferred via IEEE 488 bus to a personal

computer, which is used for some of the analysis, display of data, and transmission to a VAX 11/750 for further analysis.

IV. Future Work

Upset tests will be performed on the EEC in both an open-loop and a closed-loop configuration in order to compare upset characteristics relative to each of these modes. The analog signals induced on the EEC will be recorded and appropriate norms will be defined which characterize upset stress thresholds. Digital data recorded from the EEC will be scrutinized for selected inputs that are out of range, calculated commands which are inappropriate for the given flight regime, accesses to invalid memory space, and problems which are flagged by self-health tests.

The objectives of initial testing are to demonstrate the methodology, establish an upset data base for a fault-tolerant control system, define characteristic induced waveform threshold norms for upset stress, and obtain statistical information about upset in a fault-tolerant controller. Long range goals include the development of on-line upset detection and correction strategies, upset tolerant design techniques, an upset assessment tool for data analysis, and an upset reliability estimation procedure.

SUMMARY

An upset test methodology is being developed for fault-tolerant control systems and applied to the upset test design of an

electronic engine controller. The methodology involves generating electrical transients like those that would occur naturally in a lightning environment, coupling these signals into a controller under test, and collecting both analog and digital data from the controller during tests. The primary objective of this methodology is to develop assessment techniques for fault-tolerant control systems operating in electromagnetically harsh environments due to lightning, HERF, and NEMP. The motivation for the development of assessment techniques is the trends in the aeronautics industry towards flight-critical digital control systems onboard advanced composite aircraft.

REFERENCES

1. Hess, R. F., et. al., "Sharing the Protection of Aircraft Electronic Systems Against the Effects of High-Level Electromagnetic Environments Between Traditional Protection and System Architecture", Proceedings of the 8th Digital Avionics Systems Conference, October, 1988, pp. 294-307

2. Belcastro, C. M. , "Digital System Upset - The Effects of Simulated Lightning-induced Transients on a General-Purpose Microprocessor", NASA Technical Memorandum 84652, April, 1983

3. Belcastro, C. M. , "Data and Results of a Laboratory Investigation of Microprocessor Upset caused by Simulated Lightning-Induced Analog Transients", NASA Technical Memorandum 85821, June, 1984

4. Hanson, R. J. , "Conducted Electromagnetic Transient-Induced Upset Mechanisms: Microprocessor and Subsystem Level Effects", EOS/ESD Symposium Proceedings, 1987

5. Glaser, R. E. , Masson, G. M. , "The Containment Set Approach to Upsets in Digital Systems", IEEE Transactions on Computers, Vol. C-31, No. 7, July, 1982

6. Schmid, M. E. , et. al. , "Upset Exposure by Means of Abstraction Verification", FTCS 12th Annual Symposium Fault-Tolerant Computing, June, 1982

7. Hanson, R. J. , "Subsystem EMP Strength Verification Methods: Upset Detection and Evaluation for Military Subsystems", Kaman Sciences Corp. DC-FR-4088.330-1 (Revised Draft), March 24, 1988

8. Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning, SAE AE4L Committee Report AE4L-87-3, Revision A, October, 1988

9. Test Waveforms and Techniques for Assessing the Effects of Lightning-Induced Transients, SAE AE4L Committee Report AE4L-81-2, December 15, 1981

10. Hobbs, R. A. , "The Design, Construction, Performance and Calibration of Pulse Generators to Fulfill the Requirements of Specifications Defense Standard 59-41, FS(F) 510 and FS(F) 457", RAE TM FS(F) 550, September, 1988

11. Ketterling, George W. , "EM Transient Protection Requirements for Avionics LRUs", IEEE AES Magazine, April, 1986

12. Environmental Conditions and Test Procedures for Airborne Equipment, EUROCAE ED 14, Proposal to SAE AE4L Committee for DO 160C, Section 22, April, 1989

13. Thomas, R. E. , Diloreto, A. G. , "EMP Upset: Overview and Test Methodologies", AFWL-TR-84-60, March, 1985

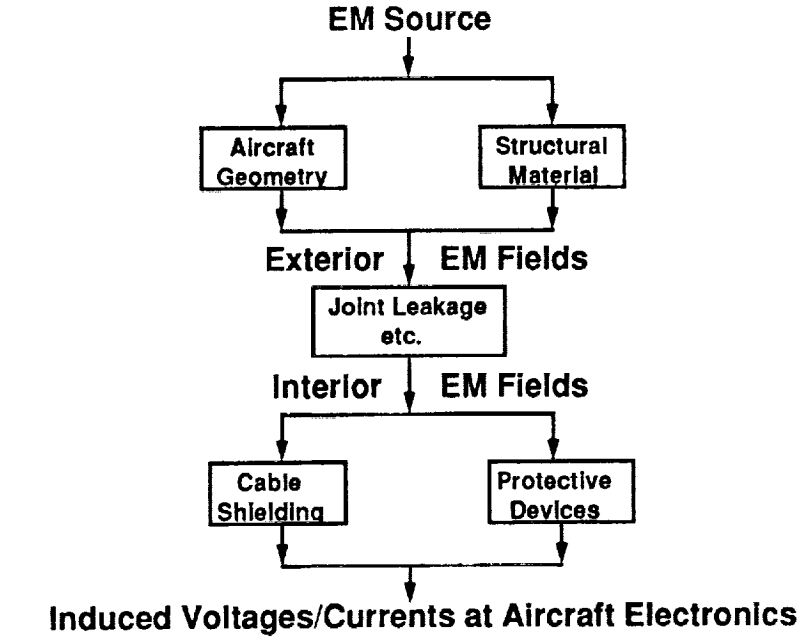


Figure 1: Coupling of Electromagnetic Fields into Aircraft

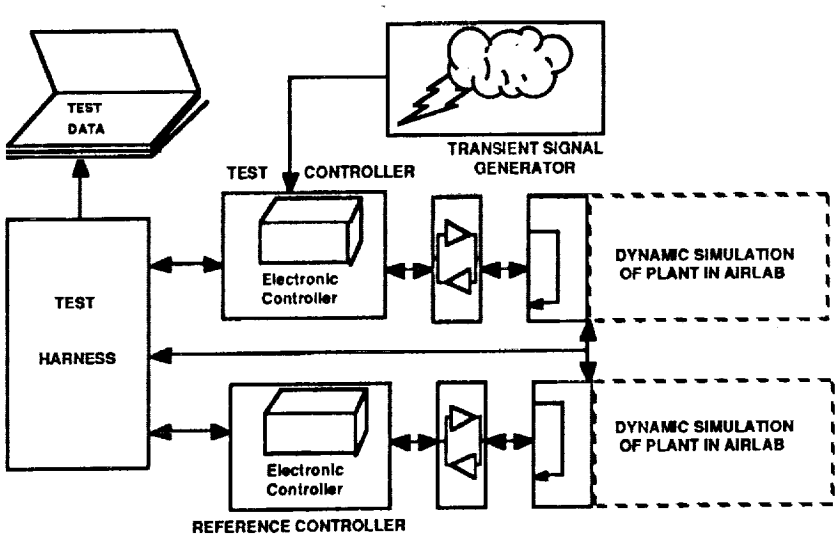
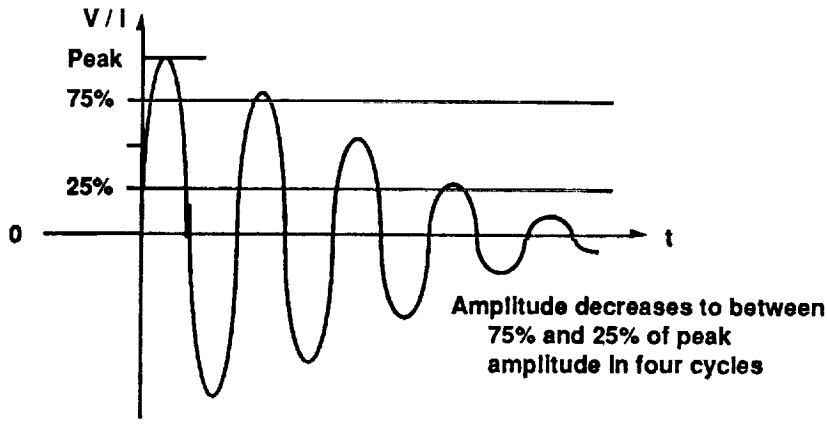


Figure 2: Laboratory Configuration for Control System Upset Testing



Frequency (MHz)	Method	Purpose
10 (± 20%)	Pin/Bulk Cable	Damage/Upset
1 (± 20%)	Pin/Bulk Cable	Damage/Upset
1 - 50	Bulk Cable	Upset

Figure 3: SAE-AE4L Committee Damped Sinusoidal Voltage/Current Waveform

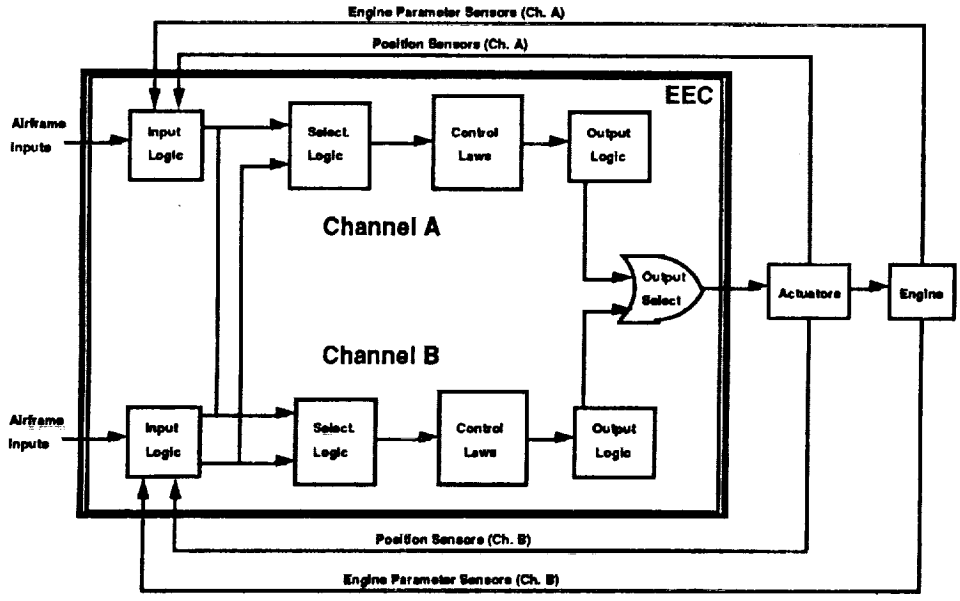


Figure 4: Block Diagram of the Electronic Engine Controller (EEC)

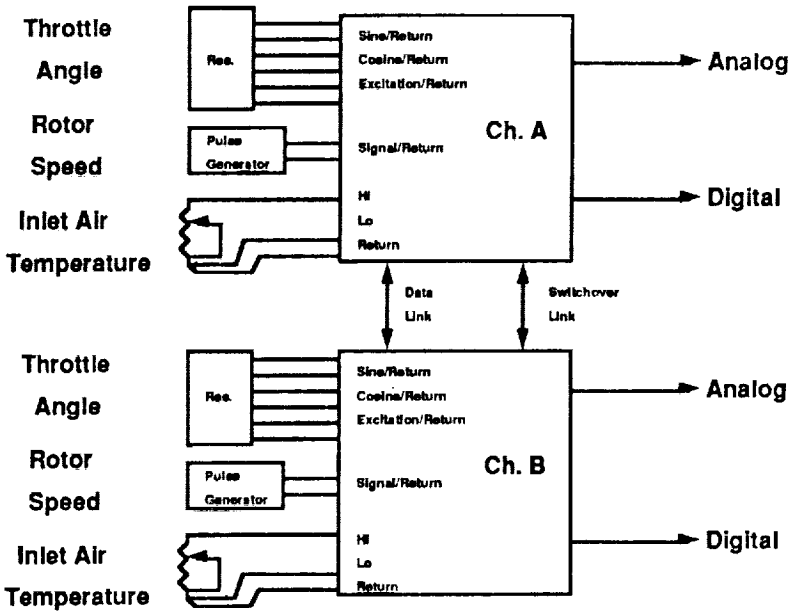


Figure 5: Simulated EEC Inputs for TRA, N1, T2

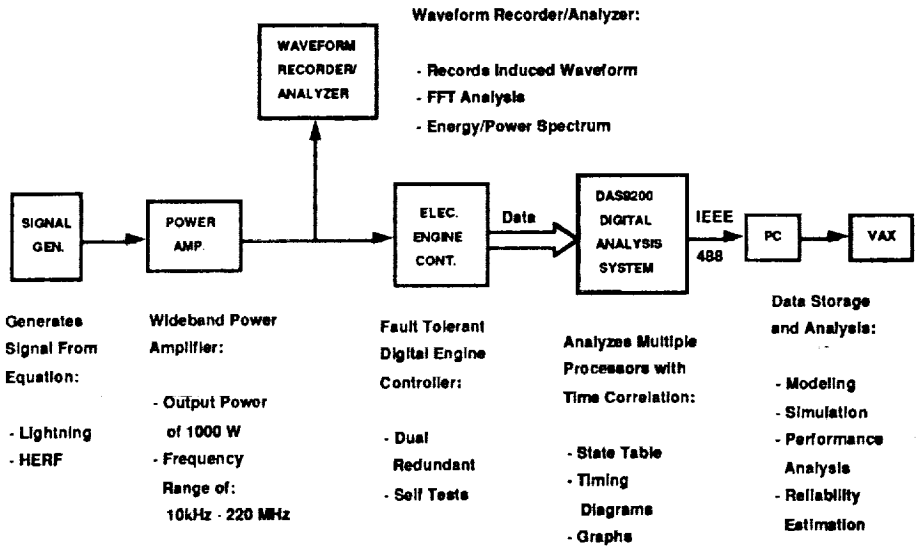


Figure 6: Upset Test Instrumentation for EEC Assessment

NASA National Aeronautics and Space Administration

Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
NASA TM-101665		

4. Title and Subtitle	5. Report Date
Laboratory Test Methodology for Evaluating the Effects of Electromagnetic Disturbances on Fault-Tolerant Control Systems	November 1989
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Celeste M. Belcastro	
	10. Work Unit No. 505-66-21-04

9. Performing Organization Name and Address	11. Contract or Grant No.
NASA Langley Research Center Hampton, VA 23665-5225	
	13. Type of Report and Period Covered
12. Sponsoring Agency Name and Address	Technical Memorandum
National Aeronautics and Space Administration Washington, DC 20546-0001	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Control systems for advanced aircraft, especially those with relaxed static stability, will be critical to flight and will, therefore, have very high reliability specifications which must be met for adverse as well as nominal operating conditions. Severe operating conditions can result from electromagnetic disturbances caused by lightning, high energy radio frequency (HERF) transmitters, and nuclear electromagnetic pulses (NEMP). Tools and techniques must be developed to verify the integrity of the control system in adverse operating environments. The most difficult and illusive perturbations to computer-based control systems caused by an electromagnetic environment (EME) are functional error modes that involve no component damage. These error modes are collectively known as "upset", can occur simultaneously in all of the channels of a redundant control system, and are software dependent. Upset studies performed to date have not addressed the assessment of multi-channel systems and do not involve the evaluation of a control system operating in a closed-loop with the plant. This paper presents a methodology for performing upset tests on a multi-channel control system and discusses considerations for the design of upset tests to be conducted in the laboratory on fault-tolerant control systems operating in a closed loop with a simulated plant. Considerations discussed include the generation and coupling of analog signals representative of electromagnetic disturbances to a control system under test, analog data acquisition, and digital data acquisition from multi-channel systems. The paper also presents a case study of an upset test methodology for a fault-tolerant electronic engine control system.

17. Key Words (Suggested by Author(s))	18. Distribution Statement
Digital System Upset Reliability Performance Analysis System Validation Electromagnetic Effects	Unclassified - Unlimited Star Category 66

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of pages	22. Price
Unclassified	Unclassified	19	A03