/N-08
61445
p. 16

NASA Technical Memorandum 104158

FORMULATION OF A STRATEGY FOR MONITORING CONTROL INTEGRITY IN CRITICAL DIGITAL CONTROL SYSTEMS

Celeste M. Belcastro,
Robert Fischl, and Moshe Kam

November 1991

NASA
National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23665-5225

Formulation of a Strategy for Monitoring Control Integrity in Critical Digital Control Systems

Celeste M. Belcastro
NASA Langley Research Center
Hampton, VA 23665-5225
Member, AES Society, IEEE

Robert Fischl, Senior Member IEEE
Moshe Kam, Member IEEE
Drexel University
Philadelphia, PA 19104

Abstract

Advanced aircraft will require flight-critical computer systems for stability augmentation as well as guidance and control that must perform reliably in adverse, as well as nominal, operating environments. Digital system upset is a functional error mode that can occur in electromagnetically harsh environments, involves no component damage, can occur simultaneously in all channels of a redundant control computer, and is software dependent. This paper presents a strategy for dynamic upset detection to be used in the evaluation of critical digital controllers during the design and/or validation phases of development. The motivation for this work is the development of tools and techniques that can be used in the laboratory to validate and/or certify critical controllers operating in adverse environments that result from disturbances caused by an electromagnetic source such as lightning, high-intensity radiated fields (HIRF), and nuclear electromagnetic pulses (NEMP). The upset detection strategy presented in the paper provides dynamic monitoring of a given control computer for degraded functional integrity that can result from redundancy management errors and control command calculation errors that could occur in an electromagnetically harsh operating environment. In addition, analytical redundancy of the control laws provides a reference of the correct control command for the given dynamic mode of the plant. This reference command is used to determine the effectiveness of the control in the given dynamic situation. The paper discusses the use of Kalman filtering, data fusion, and decision theory in monitoring a given digital controller for control calculation errors, redundancy management errors, and control effectiveness.

Introduction

Advanced aircraft will require systems for stability augmentation as well as guidance and control that will be critical to the flight of the aircraft. The trend in avionics technology is the implementation of control laws on digital computers that are interfaced to the sensors and control surface actuators of the aircraft. Since these control systems will be flight-critical, the problem of verifying the integrity of the control computer in adverse, as well as nominal, operating environments becomes a key issue in the development and certification of a critical control system.

An operating environment of particular concern results from the presence of electromagnetic fields caused by sources such as lightning, high-intensity radiated fields (HIRF), and nuclear electromagnetic pulses (NEMP). Electromagnetic fields may 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 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. Functional error modes of a critical controller which can be termed as upset in the system are characterized by: (i) faulty I/O processing and command calculations that result in off-nominal system behavior or degraded system performance; and (ii) faulty redundancy management decisions that result in degraded system performance and/or reliability. 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 prior to the disturbance. The subject of effective and reliable internal upset recovery mechanisms is another current topic for research.

The usual features of fault tolerant systems such as redundant input and output checking and selection, surge suppression devices and filters, and a redundant microprocessor architecture with voting may not be sufficient to ensure correct operation in an electromagnetically adverse operating environment. Surge suppression devices and filters are effective for large amplitude, high frequency transients. However, low amplitude signals at frequencies near the clock speeds of digital circuitry can be generated by electromagnetic fields and propagate to electronic equipment onboard an aircraft. In addition, redundancy protects against single-mode failures that occur in one channel of the system, but does not protect against the potential common-mode failure (i.e. upset) of all channels in the redundant system as a result of transient signals induced by a single electromagnetic disturbance.

To date, there are no comprehensive guidelines or criteria for detecting upset in fault tolerant digital control computers, designing reliable internal upset recovery mechanisms, or performing tests or analyses on digital controllers to verify control integrity or evaluate upset susceptibility/reliability in electromagnetically adverse operating environments. In order to assess a digital control computer for upset susceptibility, the issue of upset detection must be addressed. Real-time considerations for upset detection would reduce post data processing requirements during validation/certification testing. Therefore, the objective of this research is to develop a detection methodology for real-time laboratory implementation whereby a given digital computer-based control system can be evaluated for upset susceptibility when subjected to analog transient electrical signals like those that would be induced by an electromagnetic source such as lightning, HIRF, or NEMP. In the event of the occurrence of upset during testing, the detection methodology will also provide a framework for diagnosis of the upset in the given digital controller. An illustration of the basic laboratory set-up is shown in Figure 1. The fault tolerant controller to be evaluated for upset susceptibility is interfaced in the laboratory to a simulation of the plant, actuators, and redundant sensors so that closed-loop dynamics are represented during testing. The controller with σ redundant processors (or microprocessors, designated as μP_1 - μP_σ) is subjected to disturbances like those that could occur in an electromagnetic environment. In the case of lightning, transient signals that would be induced on internal wiring are generated. In the case of HIRF, electromagnetic fields that could occur from radars or high-power radio transmitters are generated. The control system is dynamically monitored for upset in real-time during testing. The objective of the paper is to present an upset detection strategy for monitoring a given fault tolerant controller for degraded control integrity resulting from redundancy management errors, control command calculation errors, and control effectiveness errors that could occur in an electromagnetically harsh operating environment. Kalman filtering, statistical decision theory, and data fusion are used in the detection of redundancy management errors and control command calculation errors. Analytical redundancy of the control laws provides a reference of the correct control command for a given dynamic mode of the plant. This reference command is used in the control effectiveness decision.

Problem Formulation

Consider the block diagram shown in Figure 2 of a given control system consisting of the plant, redundant sensors, actuators, and fault tolerant control computer. Input/output conversions and signal conditioning between the plant and controller are represented by the indicated blocks. Input processing functions including analog-to-digital (A/D) conversion, frequency-to-digital conversion, surge suppressors for protection against high-level transient signals, and filters to reduce high-frequency noise have been represented by the A/D and Signal Conditioning block. Output processing functions such as signal conditioning and digital-to-analog (D/A) conversion are represented by the D/A and Signal Conditioning block. The given fault tolerant controller is modeled to consist of three basic blocks. The input selection and redundancy management block performs rate and/or range checks of the data values and generates the input data vector for each of the microprocessors. The redundant microprocessors calculate the control commands based on the input vector for each processor. Redundancy in the control computer protects against single-mode failure of components during normal operation. The output selection and redundancy management block performs rate and/or range checks on the calculated commands from each processor and determines via voting, or some other scheme, the command to be output from the controller for each control loop. The following linear model is proposed for the given control system of Figure 2. The elements of the model are defined by the given system and would be determined prior to assessment. For simplicity of notation, it will be assumed that each processor has it's own sensor set. Thus, it is assumed that there will be the same number of sensors for each measurement as there are processors.

Plant:
$$\dot{x}_p(t) = Ax_p(t) + Bu(t) + \phi w_p(t) \quad ; \quad x_p(t) \in R^p \qquad (1)$$

Sensors:
$$s_p^i(t) = C^i x_p(t) + \xi^i w_s^i(t) \qquad i = 1, 2, \ldots, \sigma \quad ; \quad s_p^i(t) \in R^m \qquad (2)$$
where: $s_p^i(t) = [s_{p_1}^i(t) \;\; s_{p_2}^i(t) \;\cdots\; s_{p_m}^i(t)]' \quad ; \quad s_{p_f}^i(t) \in R$

Input Selection and Redundancy Management:

$$y_{in}^i(k) = [y_{in_1}^i(k) \;\; y_{in_2}^i(k) \;\cdots\; y_{in_m}^i(k)]' \quad ; \quad y_{in}^i(k) \in R^m$$

$$y_{in_f}^i(k) = E_f^i(k) S_{p_f}(k) + \psi_f^i w_{in_f}^i(k) \qquad i = 1, 2, \ldots, \sigma \quad ; \quad y_{in_f}^i(k), S_{p_f}(k) \in R^\sigma \qquad (3)$$
where: $S_{p_f}(k) = [s_{p_f}^1(k) \;\; s_{p_f}^2(k) \;\cdots\; s_{p_f}^\sigma(k)]' \quad ; \quad f = 1, 2, \ldots, m$

Redundant Controllers:

$$x_c^i(k+1) = F_c^i x_c^i(k) + G_c^i y_{in}^i(k) + \zeta_c^i w_c^i(k) \quad ; \quad i = 1, 2, \ldots \sigma \quad ; \quad x_c^i(k) \in R^n \qquad (4)$$
where: $x_c^i(k) = [x_{c_1}^i(k) \;\; x_{c_2}^i(k) \;\cdots\; x_{c_n}^i(k)]' \quad ; \quad x_{c_j}^i(k) \in R$

Output Processing and Redundancy Management:

$$y_{out}(k) = [y_{out_1}(k) \;\; y_{out_2}(k) \;\cdots\; y_{out_n}(k)]' \quad ; \quad y_{out}(k) \in R^n$$

$$y_{out_j}(k) = L_j(k) x_{c_j}(k) + \eta_j w_{out_j}(k) \qquad j = 1, 2, \ldots, n \quad ; \quad y_{out_j}(k) \in R \qquad (5)$$
where: $x_{c_j}(k) = [x_{c_j}^1(k) \;\; x_{c_j}^2(k) \;\cdots\; x_{c_j}^\sigma(k)]' \quad ; \quad x_{c_j}(k) \in R^\sigma$

Actuators:
$$u(t) = N y_{out}(t) + \rho w_u(t) \quad ; \quad u(t) \in R^n \qquad (6)$$

where: $y_{out}(t) = [y_{out_1}(t) \;\; y_{out_2}(t) \;\cdots\; y_{out_n}(t)]' \quad ; \quad y_{out}(t) \in R^n$

Equations (1) - (6) represent a hybrid model of continuous-time and discrete-time components. Equation (1) is the continuous-time state equation for the plant. Matrix A is the plant state transition matrix, u(t) is the control input, and $w_p(t)$ reflects noise and/or modeling errors.

Equation (2) is the continuous-time sensor model for the ith redundant sensor with $w_s^i(t)$ representing the sensor noise. Equation (3) is the discrete-time model for the selection and management of redundant sensor inputs $S_{p_f}(k)$ for the fth measurement with the noise term $w_{in_f}^i(k)$ representing modeling error. Matrix $E_f^i(k)$ is shown to be time-varying to represent selection, rejection, voting, or fusion of redundant sensor measurements during operation of the system. If the given system has an input data selection process without data fusion, the elements of $E_f^i(k)$ will be zero or one and may be based on heuristics, such as the result of range and/or rate checks on the sensor measurements. In systems that fuse sensor measurements into a single value, matrix $E_f^i(k)$ would represent the input data fusion process. Equation (4) is the discrete-time state equation for the command vector calculation for the ith processor, and matrix F_c^i is the transition matrix. Matrix G_c^i is the measurement matrix for measurement vector $y_{in}^i(k)$ of the ith processor. Term $w_c^i(k)$ reflects noise and/or modeling errors associated with the command vector calculation from the ith processor. Equation (5) is the discrete-time model for the selection and management of the redundant command calculations with modeling error accounted for in the noise term $w_{out_j}(k)$. Matrix $L_j(k)$ is time-varying to represent selection or fusion of command calculations for the command vector $y_{out_j}(k)$ of the jth control loop during operation of the system. If the given system has a voting strategy for output command calculations, the elements of $L_j(k)$ will be zero or one and may be based on heuristics associated with the voting strategy. In systems that combine calculations into one output, $L_j(k)$ would represent the command calculation fusion process. Equation (6) is the continuous-time actuator model. The actuators receive the command vector $y_{out}(t)$ and affect the dynamics of the plant via u(t). The term $w_u(t)$ reflects noise and/or modeling errors.

The research problem is to develop a monitoring scheme for real-time laboratory implementation to be used in the validation/certification of a given fault tolerant controller, modeled as shown in Figure 2, during operation in an electromagnetic environment that could result from lightning or HIRF. An upset test methodology for control computers was discussed in [1]. However, this methodology relies on post-processing of data collected during every test. Since the detection strategy presented in this paper is for eventual real-time implementation, it will eliminate the need to store data during tests in which upset does not occur. In addition, the strategy provides an indication of where errors occurred for diagnostic purposes so that any desired post-processing of the data is simplified.

Fault Tolerant Control Monitoring Strategy

In order to detect redundancy management errors, control command calculation errors, and control effectiveness errors in the fault tolerant controller, measurements of the control system of Figure 2 must be taken by the monitor. These measurements are indicated in Figure 3, and their equations are given as:

Measurement of the Plant State: $z_p(k) = Tx_p(k) + v_p(k) \quad ; \quad z_p(k) \in R^p$ (7)

Measurement of Sensor Outputs: $z_s^i(k) = D^i s_p^i(k) + v_s^i(k) \; ; \; i = 1, 2, \ldots \sigma \; ; \; z_s^i(k) \in R^m$ (8)

Measurement of Input Vectors: $z_{in}^i(k) = J^i y_{in}^i(k) + v_{in}^i(k) \quad ; \quad z_{in}^i(k) \in R^m$ (9)

Measurement of Calculated Commands: $z_c^i(k) = H_c^i x_c^i(k) + v_c^i(k) \quad ; \quad z_c^i(k) \in R^n$ (10)

Measurement of Output Command Vector: $z_{out}(k) = My_{out}(t) + v_{out}(k) \quad ; \quad z_{out}(k) \in R^n$ (11)

Measurement of the Actuator: $z_u(k) = Pu(k) + v_u(k) \quad ; \quad z_u(k) \in R^n$ (12)

In equations (7) - (12), T, D^i, J^i, H^i_c, M, and P are the measurement matrices. The terms $v_p(k)$, $v^i_s(k)$, $v^i_{in}(k)$, $v^i_c(k)$, $v_{out}(k)$, and $v_u(k)$ represent measurement noise. All noise processes in equations (1) - (12) are assumed to be independent, white, and Gaussian.

The fault tolerant control computer is monitored for errors in redundancy management and control command calculations, as well as control effectiveness for the given dynamic mode of the plant. In the context of this mathematical formulation, upset is defined as a change in any of the matrices $E^i_f(k)$ of equation (3), F^i_c and G^i_c of equation (4), and $L_j(k)$ of equation (5) that causes a reduction in effectiveness and/or reliability of the control system. A concept for upset detection in critical digital control computers is presented in Figure 4. Redundancy management processes in the control computer to be monitored are the input parameter selection process, the output command selection process, and the management of redundant resources. An example of an error in the management of redundant resources is the computer deciding that one of the redundant sensors is bad and ignoring its measurements when, in fact, it is operating correctly. Since eliminating a good sensor reduces the redundancy and overall reliability of the system, this redundancy management error would constitute an upset. The redundancy management monitor effectively detects incorrect changes in the matrices $E^i_f(k)$ and $L_j(k)$ of equations (3) and (5), respectively. Elements of these matrices are compared to the input/output selection codes of the controller to determine if the controller has eliminated resources that are not faulty. Inputs to the input selection error detection portion of this monitor are measurements of the sensor outputs, $z^i_s(k)$, and measurements of the selected input vector for each channel, $z^i_{in}(k)$. If an error is not detected in the input selection process, the decision variable $d^i_{in}(k)$ will maintain its nominal value of -1. If an error is detected in the input selection process, the value of $d^i_{in}(k)$ becomes unity. Inputs to the output selection error detection part of this monitor are measurements of the selected output commands, $z_{out_j}(k)$. If an error is not detected in the output selection process, the decision variable $d_{out_j}(k)$ will maintain its nominal value of -1. If an error is detected in the output selection process, the value of $d_{out_j}(k)$ becomes unity. Individual decisions $d^i_{in}(k)$ and $d_{out_j}(k)$ are combined or fused into one redundancy management error decision, $d_r(k)$. The calculation of commands for each control loop j is also monitored for errors. This monitoring is done dynamically as the commands are calculated. Changes in the matrices F^i_c and G^i_c of equation (4) are detected by monitoring for changes in the dynamics of the control command calculation state equation. Inputs to the control calculation error detector are measurements of the selected input vector for each channel, $z^i_{in}(k)$, and the control command calculation vector of each channel, $z^i_c(k)$. Individual decisions, $d^i_{c_j}(k)$, are made for the command calculations made by each processor for each control loop and these decisions are combined or fused into one error decision, $d_c(k)$, for the calculation of control commands. Analytical redundancy of the control laws provides a reference of the correct control command for the given dynamic mode of the plant. Inputs to the analytical model of the control laws are measurements of the plant state, $z_p(k)$. This reference is used in a decision process to determine if the calculated command output vector, $y_{out}(k)$, is effective in regulating the plant under a given dynamic situation. Considerations such as range and rate limitations of the actuators will be inherent in the evaluation of control effectiveness. If a control effectiveness error is not detected, the decision variable $d_{e_j}(k)$ will maintain its nominal value of -1. If an error in control effectiveness is detected, the value of $d_{e_j}(k)$ becomes unity. Individual control effectiveness error decisions, $d_{e_j}(k)$, are made for each control loop and these decisions are combined or fused into one error decision, $d_e(k)$, for the effectiveness of the control command output vector. The decisions corresponding to redundancy management errors, control command calculation errors, as well as control command effectiveness errors are fused into one global upset decision, d(k), which has a nominal value of -1 and a value of unity for the upset decision. This global fusion process may be a logical OR rule, or may provide weightings corresponding to the relative costs of the three error processes. In tests during which upset occurs and is signaled by the unity value of d(k), the redundancy management error decisions $d^i_{in}(k)$ and $d_{out_j}(k)$, the control calculation error decisions $d^i_{c_j}(k)$, and the control effectiveness error decisions $d_{e_j}(k)$ are all stored in the monitor as a diagnostic aid for post-testing data analysis. A basic strategy for monitoring the control computer for erroneous command calculations, redundancy management errors, and control command effectiveness is now presented.

Control Command Calculation Error Monitor. The basic approach for monitoring errors in a control command calculation is shown in Figure 5. The control law is represented as a linear or linearized recursive state equation with state $x^i_{c_j}(k)$ for the command calculation of control loop j from microprocessor i. A Kalman Filter is used to generate the estimate vector composed of an estimate $\hat{x}^i_{c_j}(k)$ of the correct state for each of the j control command calculations based on measurements of the selected input vector $z^i_{in}(k)$ and the previous calculated command state vector $z^i_c(k-1)$. The estimate $\hat{x}^i_{c_j}(k)$ is compared to the current measurement $z^i_{c_j}(k)$ of the jth command calculated by the ith microprocessor, and a residual $r^i_{c_j}(k)$ is generated, based on the difference. A statistical decision rule is then applied to the residual and a decision $d^i_{c_j}(k)$ is made regarding the correctness of the command j calculation of processor i given the selected input vector. The decisions for command calculations j = 1, 2, ... , n are then fused into a single decision, $d^i_c(k)$, for the correctness of the command calculations from processor i. Similar methods were used in the detection of sensor failures in turbofan engines [2] and in the detection of failures in aircraft actuators and control surfaces [3]. In [2], analytical redundancy, Kalman filtering, and decision theory were used to detect sensor failures in an F100 turbofan engine. Instantaneous, or "hard", errors were detected by comparing measured sensor values with those of an analytical model, taking the absolute value, and comparing this residual to a threshold. Small bias errors and drift in sensor measurements, or "soft" errors, were detected using multiple-hypothesis testing methods in which each hypothesis corresponded to a particular sensor failure. Once a "hard" or "soft" sensor failure was detected, the elements of an interface switch matrix were changed so that a Kalman Filter estimate of the sensor value replaced the measurement in the input vector used in the control laws. The methodology of [2] was demonstrated on a hybrid real-time simulation of the F100 engine as well as on a full-scale F100 engine with good results. However, this methodology was not designed to detect failures in physically redundant systems and, therefore, does not use data fusion methods. In [3], analytical redundancy and decision theory was used to detect actuator failures and control surface failures in aircraft. The design methodology consisted of two failure detection and identification (FDI) algorithms or subsystems - one for actuator failures and one for control surface failures. In the actuator FDI subsystem, an analytical model was implemented to generate a prediction of the dynamic behavior of the actuators. This prediction was compared to measurements taken from the actuators, and a residual was generated and used in a decision process that consisted of trigger, verify, and isolate tests. The control surface FDI subsystem was designed in a similar fashion. The methodology of [3] was demonstrated using a six degree-of-freedom nonlinear simulation of a modified Boeing 737 airplane with good results. This methodology was not designed to detect failures in physically redundant systems and did not use data fusion techniques.

The basic approach shown in Figure 5 is extended for the dynamic monitoring of control calculations in redundant systems and is illustrated in Figure 6. The global decision $d_C(k)$ on whether or not control command calculation errors have occurred is based on the fusion of the command calculation error decisions $d_c^i(k)$ for the σ processors. The command calculation error decision $d_c^i(k)$ for each processor is generated by the process described as the basic approach shown in Figure 5. Previous work [4] compared two distributed detection strategies, each using a different type of data fusion. One strategy involved the fusion of estimates, and the other strategy involved the fusion of local decisions. The ROC curve of the strategy with decision fusion was shown to be more desirable for two cases.

Redundancy Management Error Monitor. Since the detection strategy of Figure 4 is for detecting errors in the controller and is to be implemented in the laboratory setting, depicted in Figure 2, which involves the simulation of redundant sensors, it will be assumed that sensor failures do not occur. The strategy for detecting input redundancy management errors is illustrated in Figure 7. Redundant parameter measurements from σ sensors are used by the monitor in the same input selection algorithm as that of each channel in the controller and a "prediction" of the selected parameter inputs are made. Note that this algorithm corresponds to $E_I^i(k)$ of equation (3). As shown in Figure 7, measurements of redundant sensor 1 inputs $z_{s_1}^1(k)$, $z_{s_1}^2(k)$, ... , $z_{s_1}^\sigma(k)$ are used in the monitor's input 1 selection rule which is identical to that of microprocessor 1 to obtain the reference selected value of input 1, $\hat{y}_{in_1}^1(k)$. This reference value is compared with a measurement of the input 1 value actually selected by microprocessor 1, $z_{in_1}^1(k)$, and a residual is generated. This residual, $r_{in_1}^1(k)$, is used in a statistical decision rule to determine if a correct or faulty selection of input 1 was made by microprocessor 1. This decision is designated as $d_{in_1}^1(k)$. The input selection error decision process is performed for each redundant input parameter and for each microprocessor in the controller. The input 1 selection decisions for the σ microprocessors are denoted as $d_{in_1}^1(k)$, $d_{in_1}^2(k)$, ... , $d_{in_1}^\sigma(k)$. These input selection error decisions for the σ processors are fused to obtain the selected input error decision $d_{in_1}(k)$. This error detection structure is implemented for the m input measurements to yiel the selected input error decisions $d_{in_1}(k)$, $d_{in_2}(k)$, ... , $d_{in_m}(k)$. These decisions are then fused to obtain the global error decision for the correctness of the input selection process of the controller, $d_{in}(k)$.

The output selection error detection strategy is shown in Figure 8. The Kalman filter estimates of the command calculations for each control loop from each processor are used by the monitor in the same output selection algorithm as that of the controller and a "prediction" of the selected parameter outputs are made. This algorithm corresponds to $L_j(k)$ in equation (5). As shown in Figure 8, estimates of the calculated control command for loop j from the σ processors, $\hat{x}_{c_j}^1(k)$, $\hat{x}_{c_j}^2(k)$, ... , $\hat{x}_{c_j}^\sigma(k)$, are used in the monitor's command j output selection rule which is identical to that of the controller to obtain the reference selected value of the jth control command output, $\hat{x}_{c_j}(k)$. These reference values are each compared with the measurement, $z_{out_j}(k)$, of the controller's selected command j output and a residual, $r_{out_j}(k)$, is formed. The residual is used in a statistical decision rule to determine if a correct or faulty selection of output command j was made by the controller. The decision for the jth command loop is designated $d_{out_j}(k)$. These decisions are then fused into a global decision, $d_{out}(k)$, for the correctness of the output decision process of the controller.

The error decisions $d_{in}(k)$ and $d_{out}(k)$ for the input and output selection processes, respectively, are then fused into a global redundancy management error decision $d_r(k)$ as shown in Figure 4.

Control Effectiveness Error Monitor. The strategy for monitoring the controller's command effectiveness is shown in Figure 9. The n control laws are implemented analytically and used to generate a reference, $y^{ref}_{out_j}(k)$, for each command loop. These reference commands are used in analytical models of the actuators to generate a reference for the plant command variables, $u^{ref}_j(k)$, provided by the actuators. The commands, $y_{out_j}(k)$, output by the controller for each loop are used in a simulation of the actuators to generate what would be the actual plant command variables, $u_j(k)$. A comparison is made between the measurement $z_{u_j}(k)$ of these variables and the reference $u^{ref}_j(k)$ in the formation of the residuals $r_{e_j}(k)$. Statistical decisions, $d_{e_j}(k)$, based on the residuals are made regarding the effectiveness of each control command output by the controller. These decisions are then fused into a global decision, $d_e(k)$, on the command effectiveness of the controller.

The error decisions for the redundancy management process $d_r(k)$, the control law calculations $d_c(k)$, and command effectiveness $d_e(k)$ are fused into the global upset decision d(k), as shown in Figure 4. In tests during which upset occurs and is signaled by the unity value of d(k), the redundancy management error decisions $d^i_{in}(k)$ and $d_{out_j}(k)$, the control calculation error decisions $d^i_{c_j}(k)$, and the control effectiveness error decisions $d_{ej}(k)$ are all stored in the monitor as a diagnostic aid for post-testing data analysis.

Summary and Future Work

The problem of verifying the integrity of flight-critical control computers in adverse, as well as nominal, operating environments becomes a key issue in the development and certification of control systems for advanced aircraft. A strategy for monitoring the control integrity of a critical digital controller has been presented. This strategy includes error decisions that can be stored during testing and used to aid in the diagnosis of functional error modes known as upset in the critical controller. The strategy uses Kalman filtering, analytical redundancy, data fusion, and statistical decision theory in the monitoring of control law calculations, the input/output selection process of redundant parameters, and the command effectiveness of the controller. With the formulation of the problem presented in this paper, subsequent steps can be taken in its solution such as the design of the algorithms for the individual monitoring processes in the strategy. In particular, statistical decision rules and data fusion algorithms must be designed. The design of Kalman filter gains that yield globally optimal results can be considered. In addition, an analysis of the design for detection sensitivity to changes in matrix parameter values must be conducted. Design tradeoffs to be considered include sensitivity and diagnostic capability versus complexity, reliable detection without false alarms, and sensitivity to erroneous parameter changes with robustness to modeling errors. These considerations are to be treated in subsequent papers.

References

1. Belcastro, C. M.: "Laboratory Test Methodology for Evaluating the Effects of Electromagnetic Disturbances on Fault-Tolerant Control Systems"; NASA TM-101665, November 1989
2. De Laat, J. C. and Merrill, W. C.: "Advanced Detection, Isolation, and Accommodation of Sensor Failures in Turbofan Engines"; NASA TP 2925, February 1990
3. Bundick, W. T. : "Development of an Adaptive Failure-Detection and Identification System for Detecting Aircraft Control-Element Failures"; NASA TP 3051, May 1991
4. Belcastro, C. M.; Fischl, R.; and Kam, M.: "Fusion Techniques Using Distributed Kalman Filtering for Detecting Changes in Systems"; Proceedings of the American Control Conference, June 1991

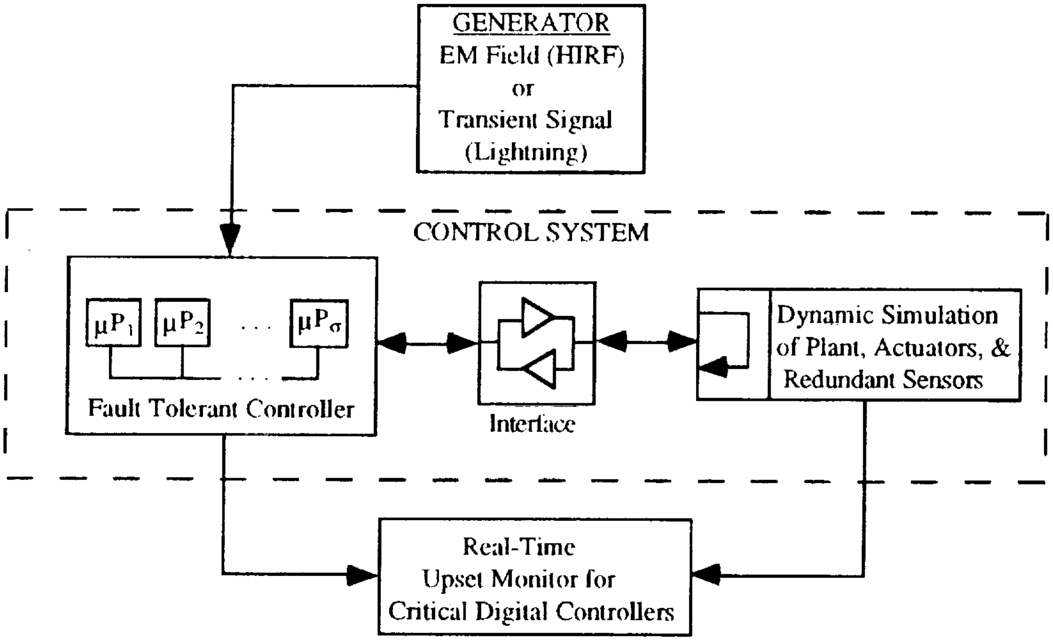
GENERATOR
EM Field (HIRF)
or
Transient Signal
(Lightning)
CONTROL SYSTEM
μP1
μP2
μPσ
Fault Tolerant Controller
Interface
Dynamic Simulation of Plant, Actuators, & Redundant Sensors
Real-Time Upset Monitor for Critical Digital Controllers

Figure 1: Basic Laboratory Configuration for Upset Evaluation of Critical Controllers

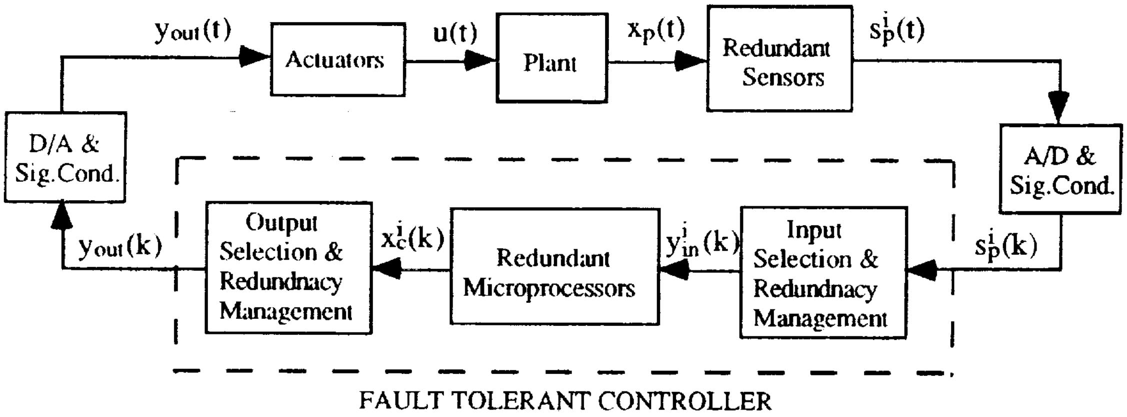
yout(t)
Actuators
u(t)
Plant
xp(t)
Redundant Sensors
sip(t)
A/D & Sig.Cond.
sip(k)
Input Selection & Redundnacy Management
yiin(k)
Redundant Microprocessors
xic(k)
Output Selection & Redundnacy Management
yout(k)
D/A & Sig.Cond.
FAULT TOLERANT CONTROLLER

Figure 2: Control System with Redundant Sensors and Microprocessors

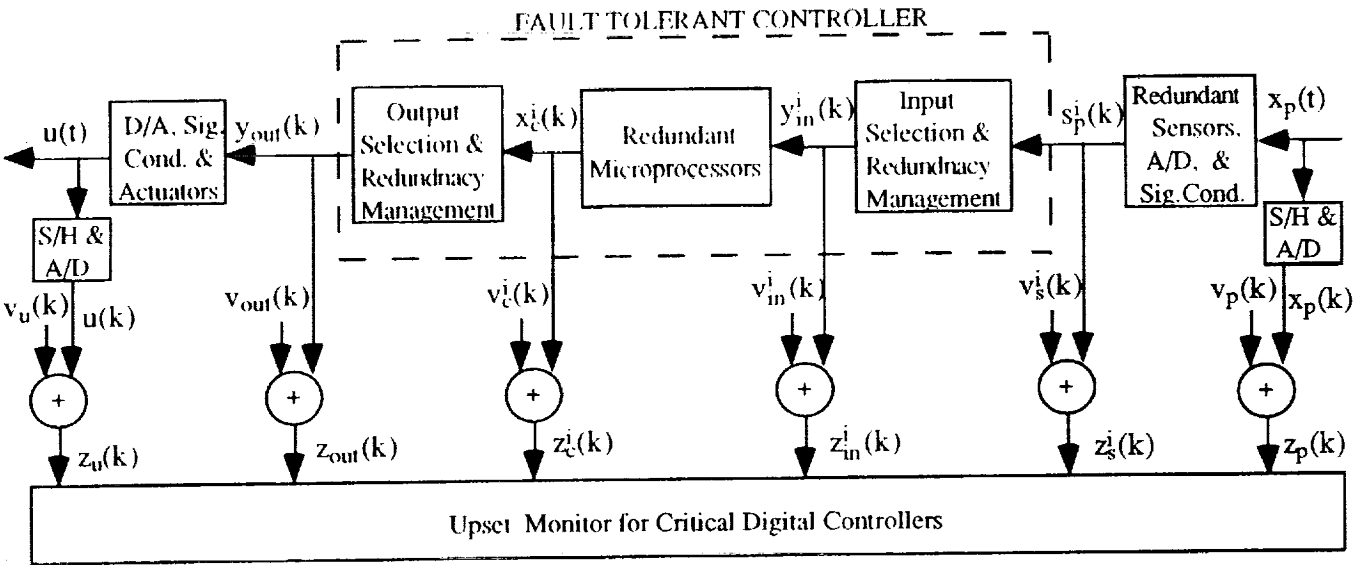
FAULT TOLERANT CONTROLLER
u(t)
D/A, Sig. Cond. & Actuators
$y_{out}(k)$
Output Selection & Redundnacy Management
$x_c^i(k)$
Redundant Microprocessors
$y_{in}^i(k)$
Input Selection & Redundnacy Management
$s_p^i(k)$
Redundant Sensors, A/D, & Sig.Cond.
$x_p(t)$
S/H & A/D
S/H & A/D
$v_u(k)$
u(k)
$v_{out}(k)$
$v_c^i(k)$
$v_{in}^i(k)$
$v_s^i(k)$
$v_p(k)$
$x_p(k)$
+
+
+
+
+
+
$z_u(k)$
$z_{out}(k)$
$z_c^i(k)$
$z_{in}^i(k)$
$z_s^i(k)$
$z_p(k)$
Upset Monitor for Critical Digital Controllers

Figure 3: Fault Tolerant Controller Measurements

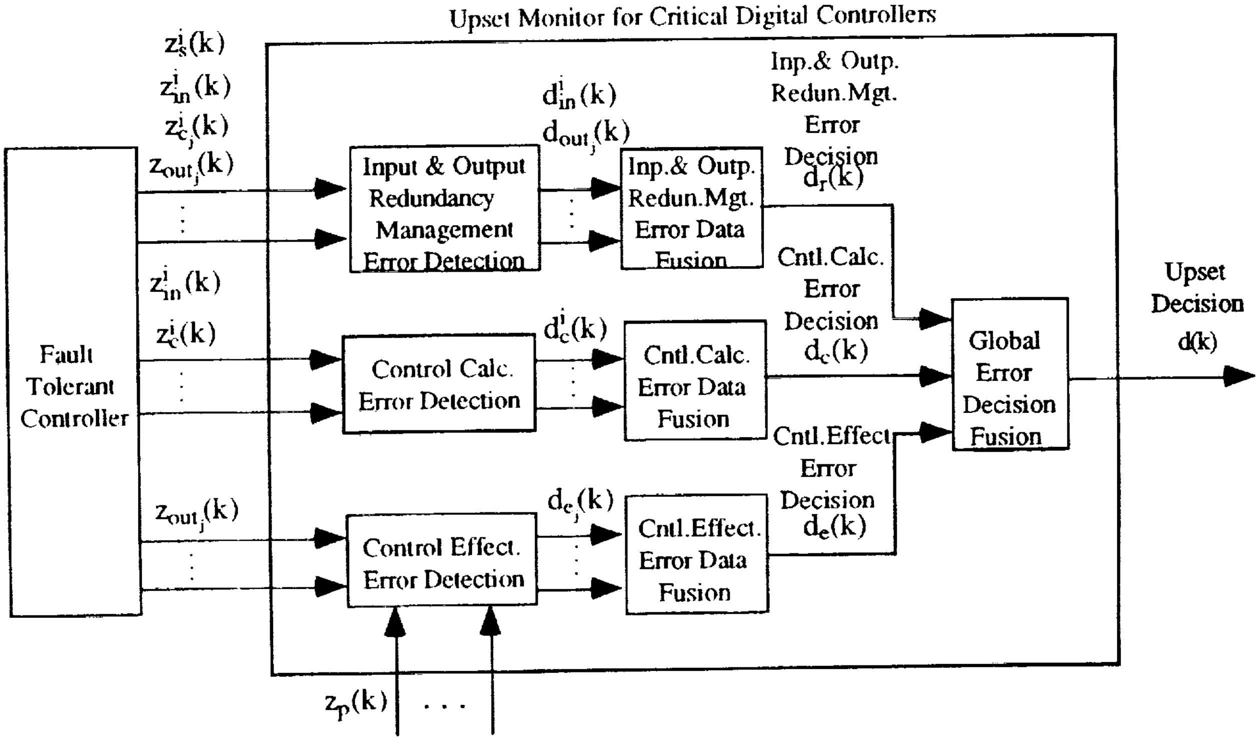
Upset Monitor for Critical Digital Controllers
$z_s^i(k)$
$z_{in}^i(k)$
$z_{c_j}^i(k)$
$z_{out_j}(k)$
Fault Tolerant Controller
Input & Output Redundancy Management Error Detection
$d_{in}^i(k)$
$d_{out_j}(k)$
Inp.& Outp. Redun.Mgt. Error Data Fusion
Inp.& Outp. Redun.Mgt. Error Decision $d_r(k)$
$z_{in}^i(k)$
$z_c^i(k)$
Control Calc. Error Detection
$d_c^i(k)$
Cntl.Calc. Error Data Fusion
Cntl.Calc. Error Decision $d_c(k)$
Global Error Decision Fusion
Upset Decision d(k)
Cntl.Effect Error Decision $d_e(k)$
$z_{out_j}(k)$
Control Effect. Error Detection
$d_{e_j}(k)$
Cntl.Effect. Error Data Fusion
$z_p(k)$
. . .

Figure 4: Upset Detection Concept for Critical Digital Systems

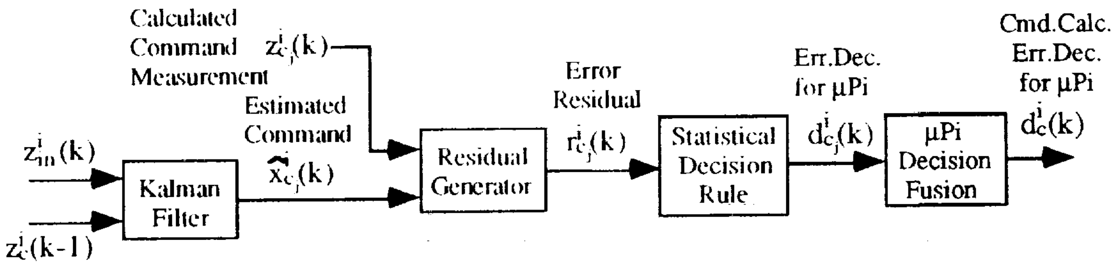

Figure 5: Strategy for Monitoring Control Law Integrity in Critical Controllers

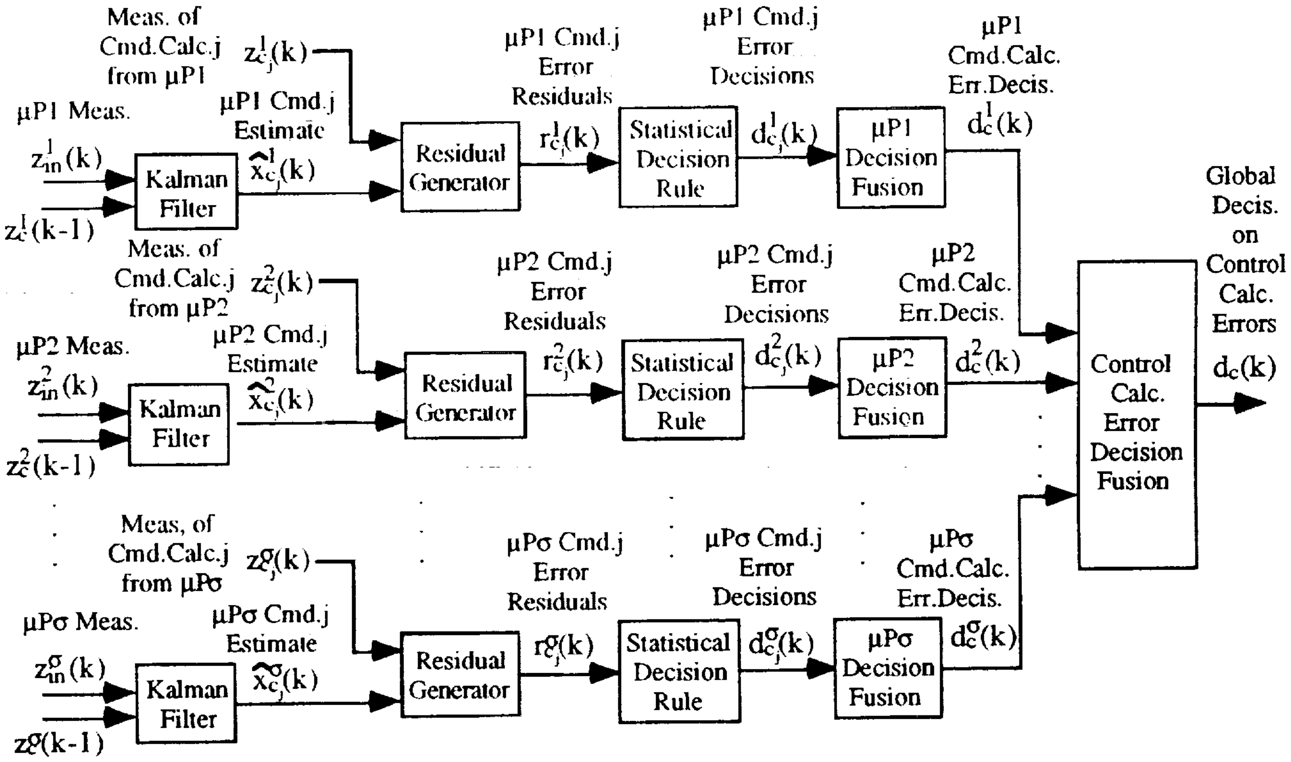

Figure 6: Approach for Dynamic Control Command Calculation Error Monitoring

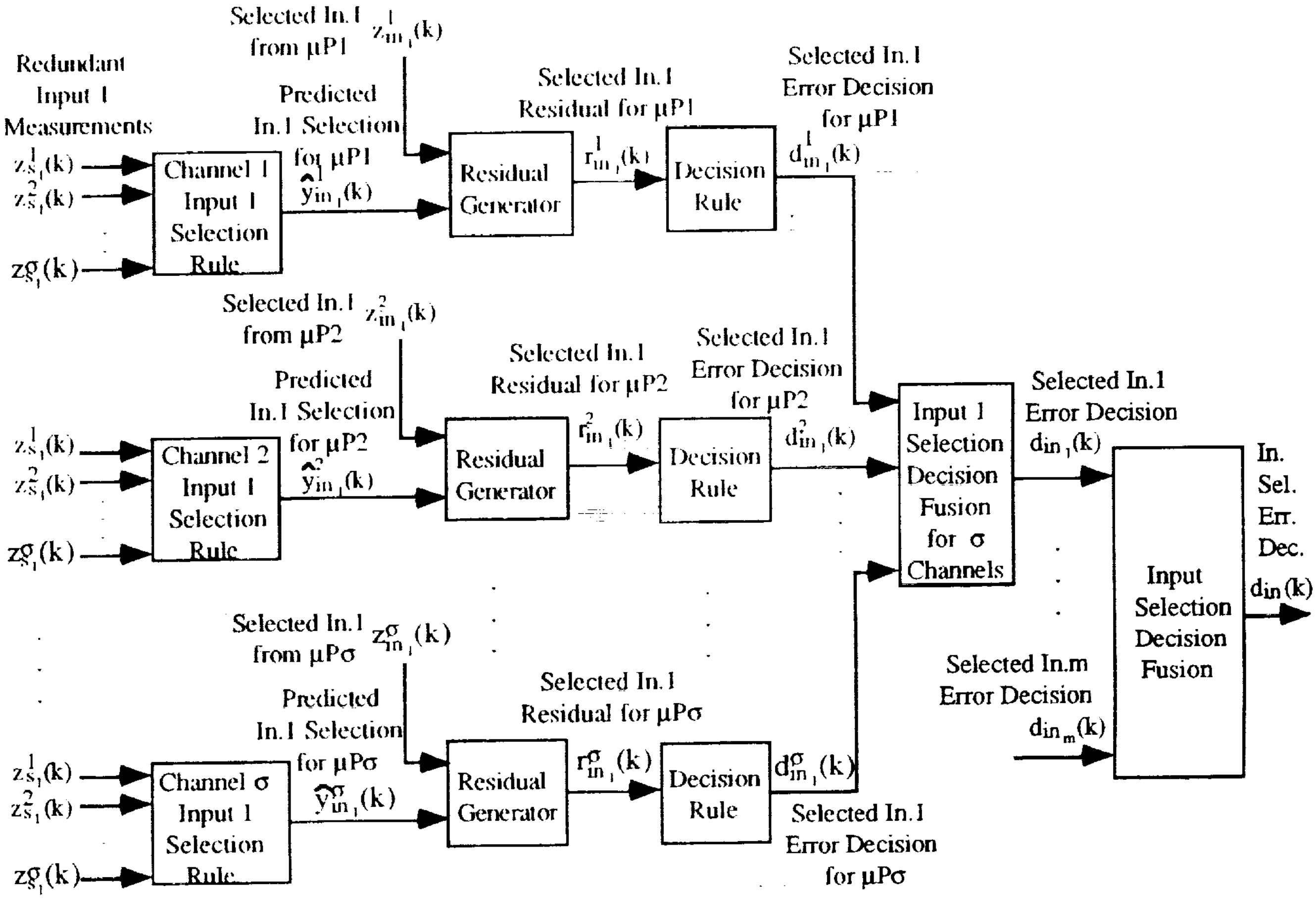
Redundant Input 1 Measurements
$z_{s_1}^1(k)$
$z_{s_1}^2(k)$
$z_{s_1}^{\sigma}(k)$
Channel 1 Input 1 Selection Rule
Selected In.1 from µP1
$z_{in_1}^1(k)$
Predicted In.1 Selection for µP1
$\hat{y}_{in_1}^1(k)$
Residual Generator
Selected In.1 Residual for µP1
$r_{in_1}^1(k)$
Decision Rule
Selected In.1 Error Decision for µP1
$d_{in_1}^1(k)$
Channel 2 Input 1 Selection Rule
Selected In.1 from µP2
$z_{in_1}^2(k)$
Predicted In.1 Selection for µP2
$\hat{y}_{in_1}^2(k)$
Residual Generator
Selected In.1 Residual for µP2
$r_{in_1}^2(k)$
Decision Rule
Selected In.1 Error Decision for µP2
$d_{in_1}^2(k)$
Channel σ Input 1 Selection Rule
Selected In.1 from µPσ
$z_{in_1}^{\sigma}(k)$
Predicted In.1 Selection for µPσ
$\hat{y}_{in_1}^{\sigma}(k)$
Residual Generator
Selected In.1 Residual for µPσ
$r_{in_1}^{\sigma}(k)$
Decision Rule
$d_{in_1}^{\sigma}(k)$
Selected In.1 Error Decision for µPσ
Input 1 Selection Decision Fusion for σ Channels
Selected In.1 Error Decision
$d_{in_1}(k)$
Selected In.m Error Decision
$d_{in_m}(k)$
Input Selection Decision Fusion
In. Sel. Err. Dec.
$d_{in}(k)$

Figure 7: Approach for Controller Input Selection Error Monitoring

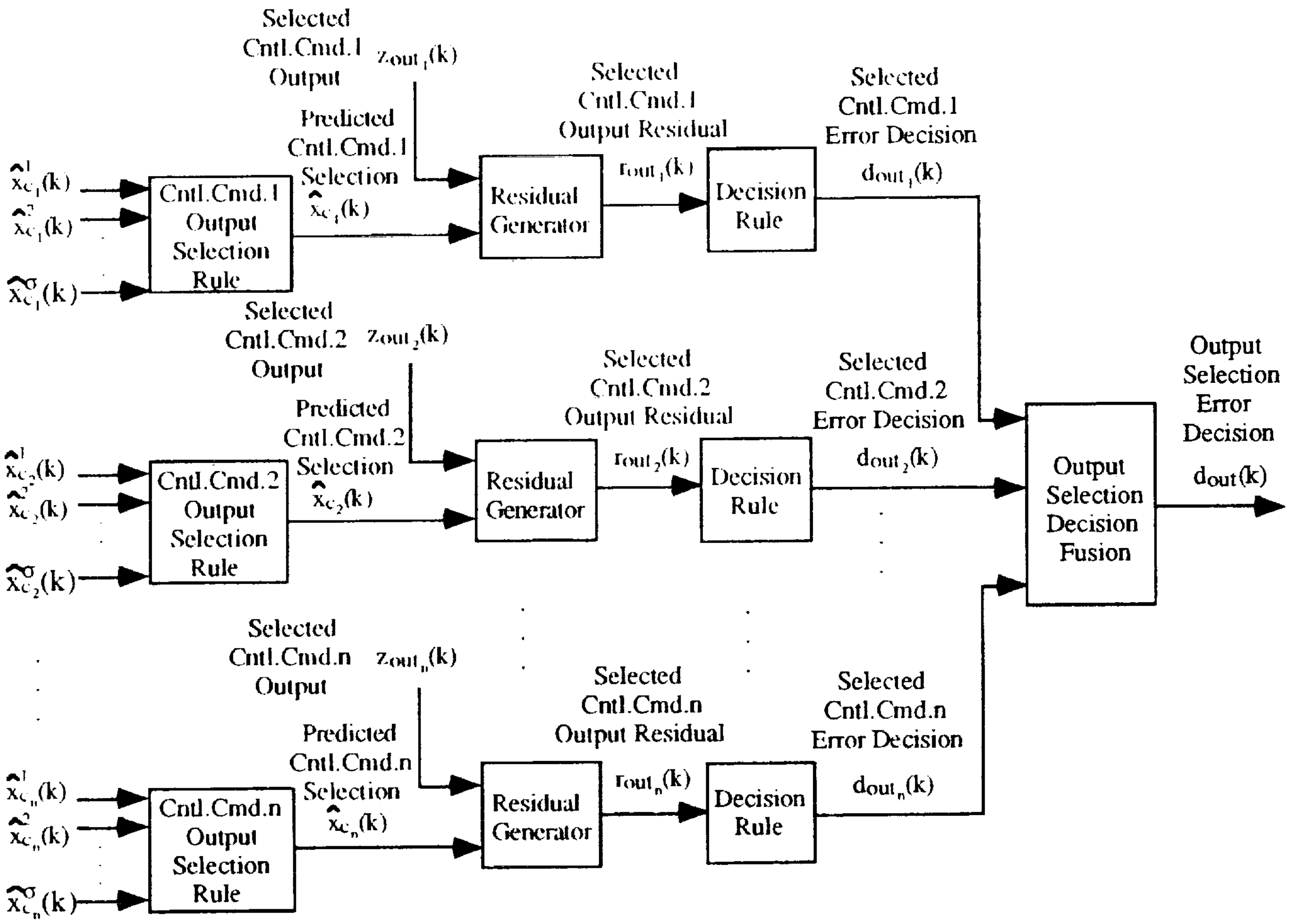
Selected Cntl.Cmd.1 Output
$z_{out_1}(k)$
Predicted Cntl.Cmd.1 Selection
$\hat{x}_{c_1}(k)$
$\hat{x}^1_{c_1}(k)$
$\hat{x}^2_{c_1}(k)$
$\hat{x}^{\sigma}_{c_1}(k)$
Cntl.Cmd.1 Output Selection Rule
Residual Generator
Selected Cntl.Cmd.1 Output Residual
$r_{out_1}(k)$
Decision Rule
Selected Cntl.Cmd.1 Error Decision
$d_{out_1}(k)$
Selected Cntl.Cmd.2 Output
$z_{out_2}(k)$
Predicted Cntl.Cmd.2 Selection
$\hat{x}_{c_2}(k)$
$\hat{x}^1_{c_2}(k)$
$\hat{x}^2_{c_2}(k)$
$\hat{x}^{\sigma}_{c_2}(k)$
Cntl.Cmd.2 Output Selection Rule
Residual Generator
Selected Cntl.Cmd.2 Output Residual
$r_{out_2}(k)$
Decision Rule
Selected Cntl.Cmd.2 Error Decision
$d_{out_2}(k)$
Selected Cntl.Cmd.n Output
$z_{out_n}(k)$
Predicted Cntl.Cmd.n Selection
$\hat{x}_{c_n}(k)$
$\hat{x}^1_{c_n}(k)$
$\hat{x}^2_{c_n}(k)$
$\hat{x}^{\sigma}_{c_n}(k)$
Cntl.Cmd.n Output Selection Rule
Residual Generator
Selected Cntl.Cmd.n Output Residual
$r_{out_n}(k)$
Decision Rule
Selected Cntl.Cmd.n Error Decision
$d_{out_n}(k)$
Output Selection Decision Fusion
Output Selection Error Decision
$d_{out}(k)$

Figure 8: Approach for Controller Output Selection Error Monitoring

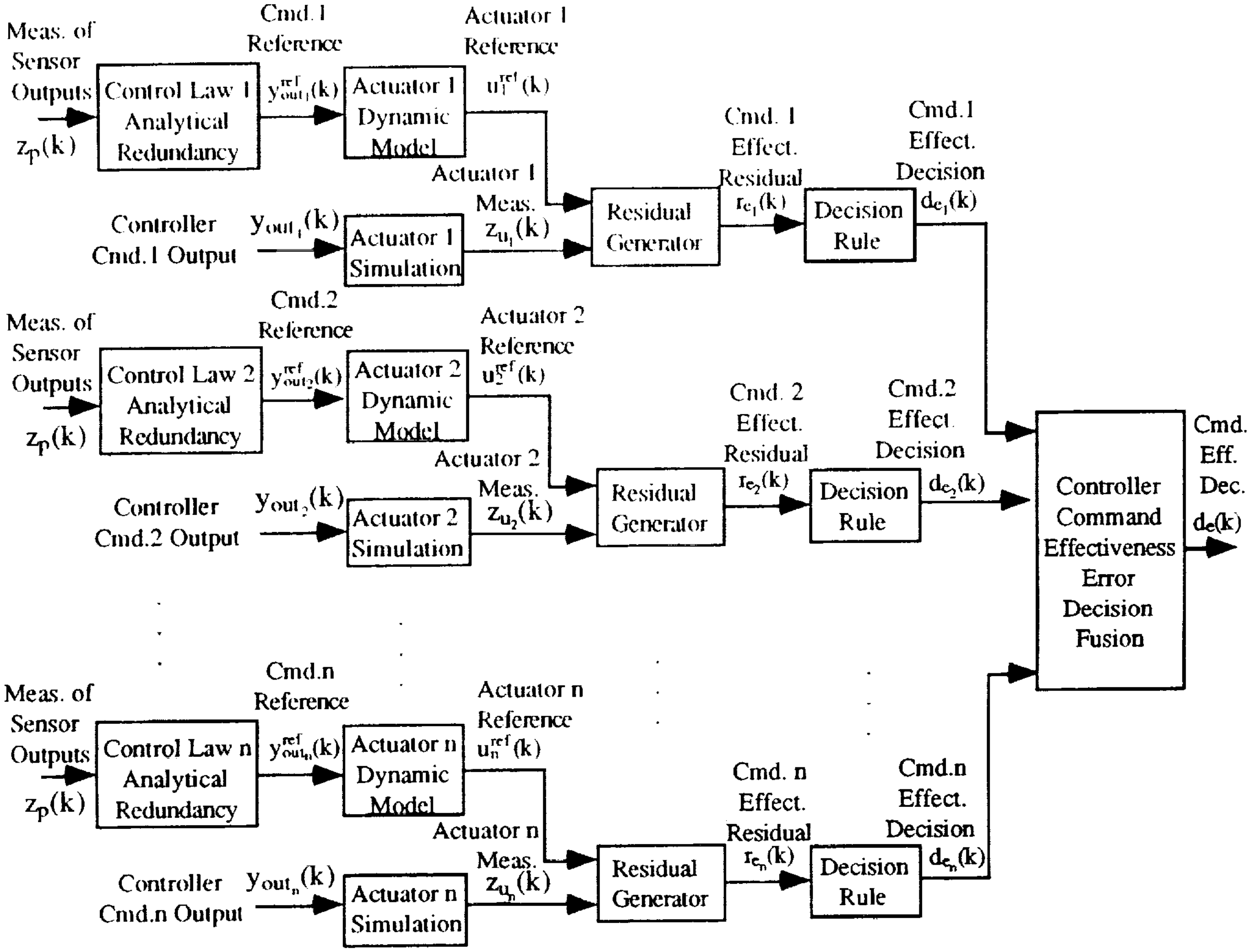

Figure 9: Approach for Controller Command Effectiveness Error Monitoring

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
November 1991

3. REPORT TYPE AND DATES COVERED
Technical Memorandum

4. TITLE AND SUBTITLE
Formulation of a Strategy for Monitoring Control Integrity in Critical Digital Control Systems

5. FUNDING NUMBERS
WU 505-64-10-10

6. AUTHOR(S)
Celeste M. Belcastro, Robert Fischl, and Moshe Kam

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23665-5225

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
NASA TM-104158

11. SUPPLEMENTARY NOTES
Fischl and Kam: Drexel University, Philadelphia, PA 19104.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Unclassified - Unlimited

Subject Category 08, 66, 33

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Advanced aircraft will require flight-critical computer systems for stability augmentation as well as guidance and control that must perform reliably in adverse, as well as nominal, operating environments. Digital system upset is a functional error mode that can occur in electromagnetically harsh environments, involves no component damage, can occur simultaneously in all channels of a redundant control computer, and is software dependent. This paper presents a strategy for dynamic upset detection to be used in the evaluation of critical digital controllers during the design and/or validation phases of development. The motivation for this work is the development of tools and techniques that can be used in the laboratory to validate and/or certify critical controllers operating in adverse environments that result from disturbances caused by an electromagnetic source such as lightning, High-Intensity Radiated Fields (HIRF), and Nuclear Electromagnetic Pulses (NEMP). The upset detection strategy presented in the paper provides dynamic monitoring of a given control computer for degraded functional integrity that can result from redundancy management errors and control command calculation errors that could occur in an electromagnetically harsh operating environment. In addition, analytical redundancy of the control laws provides a reference of the correct control command for the given dynamic mode of the plant. This reference command is used to determine the effectiveness of the control in the given dynamic situation. The paper discusses the use of Kalman filtering, data fusion, and decision theory in monitoring a given digital controller for control calculation errors, redundancy management errors, and control effectiveness.

14. SUBJECT TERMS
Digital upset; dynamic monitoring; Kalman filtering; statistical decision theory, data fusion

15. NUMBER OF PAGES
15

16. PRICE CODE
A03

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT

20. LIMITATION OF ABSTRACT