Detecting Controller Malfunctions in Electromagnetic Environments: Part II – Design & Analysis of the Detector

Celeste M. Belcastro
NASA Langley Research Center
Mail Stop 130
Hampton, VA 23681
Phone: (757) 864-6182
Fax: (757) 864-4234
celeste.m.belcastro@larc.nasa.gov

Abstract

Verifying the integrity of control computers in adverse operating environments is a key issue in the development, validation, certification, and operation of critical control systems. Future commercial aircraft will necessitate flight-critical systems with high reliability requirements for stability augmentation, flutter suppression, and guidance and control. Operational integrity of such systems in adverse environments must be validated. This paper considers the problem of applying dynamic detection techniques to monitoring the integrity of fault tolerant control computers in critical applications. Specifically, this paper considers the detection of malfunctions in an aircraft flight control computer (FCC) that is subjected to electromagnetic environment (EME) disturbances during laboratory testing. A dynamic monitoring strategy is presented and demonstrated for the FCC from glideslope engaged until flare under clear air turbulence conditions using a detailed simulation of the B737 Autoland. The performance of the monitoring system is analyzed.

1. INTRODUCTION

Verifying the integrity of the control computer in adverse, as well as nominal, operating environments is a key issue in the development, certification, and operation of critical control systems. Future advanced aircraft will require systems for stability augmentation and flutter suppression, as well as guidance and control. Such systems will be flight-critical, since the flight of the aircraft will depend on reliable operation of these systems. Laboratory experiments show that control computers that are subjected to electromagnetic disturbances can malfunction and cause catastrophic departures in performance of the closed-loop system [1] – [2]. The integrity of fault tolerant control computers in critical applications can be viewed as the reliable system-level operation of controller functions such as redundancy management decisions, control law calculations, and input/output (I/O) rate and range checks [3]. This paper is concerned only with the design of a Control Law Calculation Malfunction (CLCM) detector. A design strategy for the CLCM was developed and analyzed in previous work [3] - [4]. In this time-varying model-based detection strategy, the threshold is scheduled with the models used to estimate the correct control command. This paper presents an improvement on previous work in the design of the detector threshold. The use of linear parameter varying models in the detector design was considered in [5], but will not be utilized in this paper. The problem formulation for the CLCM is reviewed in Section 2. The design of the improved CLCM detector is presented in Section 3. This design applies dynamic detection techniques to monitoring the integrity of a simulated control computer. Malfunctions in the controller are detected in terms of the residual between a measurement of the calculation (that may result from computer malfunctions) and an estimate of the correct calculation for the nominal (no malfunction) hypothesis. An extensive literature review on fault detection was conducted and has already been published [3]. These references are not repeated here. In Section 4, the monitoring strategy is demonstrated for the elevator command of a B737 Autoland flight controller from glideslope engaged until flare that resulted from a detailed closed-loop simulation. In the implementation of the time-varying dynamic detector, the threshold is scheduled with the models used to estimate the correct control command [6]. The performance of the dynamic monitoring strategy is analyzed in terms of

probability of false alarm and probability of a missed detection.

2. PROBLEM FORMULATION

The objective of this paper is the design of a Control Law Calculation Malfunction (CLCM) detector. The problem is formulated for the case of monitoring a fault tolerant controller with N processors that each calculates M control laws. A separate detector monitors each control law calculation from each processor, and is referred to as the "local detector". This paper considers the design of the local detector only. In terms of monitoring the integrity of the control law calculations, controller malfunction is defined as follows.

DEFINITION 1: The jth control law calculation of the ith processor is the result of a malfunction if:

$$\left|\Delta x_i^j(k)\right| > \varepsilon_i^j(k) \quad \text{for K time steps} \qquad (1)$$

$\Delta x_i^j(k)$ = change in the jth control law calculation of the ith processor due to malfunction

$\varepsilon_i^j(k)$ = maximum allowable variation of $x_i^j(k)$

$|\cdot|$ = absolute value

The change $\Delta x_i^j(k)$ in the calculation of the jth control law of the ith processor due to malfunction is defined as:

$$\Delta x_i^j(k) = x_i^j(k) - E\left[x_i^j(k) \mid X_i^{j^k}\right] \qquad (2)$$

$x_i^j(k)$ = actual jth control law calculation of the ith processor at time k, which may reflect a malfunction

$x_i^j(k)$ = correct (no malfunction) control law calculation j of the ith processor at k

$X_i^{j^k}$ = set of all $x_i^j(k)$ up to time k

$E\left[x_i^j(k) \mid X_i^{j^k}\right]$ = conditional expectation of correct (no malfunction) control calculation j at time step k given all $x_i^j(k)$ up to time k

The correct (no malfunction) command calculation, $x_i^j(k)$, in equation (2) is defined:

$$x_i^j(k+1) = \bar{F}_i^j x_i^j(k) + \bar{\vec{G}}_i^j \vec{u}_i^j(k) + \zeta_i^j w_i^j(k) \qquad (3)$$

$x_i^j(k)$ = correct (no malfunction) control law calculation j from the ith processor; i=1, 2, …, N; j = 1, …, M; $x_i^j(k) \in R$

$\vec{u}_i^j(k)$ = inputs to jth control law calculation of *processor i* from the plant simulation; $\vec{u}_i^j(k) \in R^L$

$w_i^j(k)$ = process noise for the jth control law calculation of *processor i*; $w_i^j(k) \in R$

$\bar{F}_i^j$ = system matrix for correct (no malfunction) control law calculation j of *processor i*

$\bar{\vec{G}}_i^j$ = input matrix for correct (no malfunction) control law calculation j of *processor i*

k = data frame during which all control laws are calculated

The system matrix $\bar{F}_i^j$ and input matrix $\bar{\vec{G}}_i^j$ are constant over an interval of interest. The process noise $w_i^j(k)$ in equation (3) accounts for modeling error, noise in the input vector $\vec{u}_i^j(k)$ from the aircraft sensors, and stochastic variations in the command that result from exogenous disturbances such as turbulence to the aircraft.

Command calculation j of the ith processor (which may reflect malfunction) is defined:

$$x_i^j(k+1) = F_i^j(k) x_i^j(k) + \vec{G}_i^j(k) \vec{u}_i^j(k) + \zeta_i^j w_i^j(k) \qquad (4)$$

$x_i^j(k)$ = jth control law calculation from processor i; i = 1, 2, …, N; j = 1, 2, …, M; $x_i^j(k) \in R$

$\vec{u}_i^j(k)$ = inputs to jth control law calculation of

processor i from the plant; $\vec{u}_i^j(k) \in R^L$

$w_i^j(k)$ = process noise for the jth control law calculation of *processor i*; $w_i^j(k) \in R$

The initial state of the jth command calculation of the ith processor is denoted as $x_i^j(k_0)$.

ASSUMPTION 1: The initial state $x_i^j(k_0)$ is a Gaussian random variable with mean $\bar{x}_i^j(k_0)$ and variance $P_i^j(k_0)$. The initial state of the calculations of the ith processor are independent.

ASSUMPTION 2: The process noise $w_i^j(k)$ is zero-mean, Gaussian, and white with variance Q_i^j. The process noise of the calculations of the ith processor are independent. Process noise $w_i^j(k)$ is independent of the initial state $x_i^j(k_0)$.

ASSUMPTION 3: Malfunction phenomena in the ith processor that result in errors in the jth control law calculation, modeled by equation (4), can be represented by parameter changes $\Delta F_i^j(k)$ and $\Delta \vec{G}_i^j(k)$ in the nominal values of matrices $F_i^j(k)$ and $\vec{G}_i^j(k)$, respectively, so that:

$$F_i^j(k) = \bar{F}_i^j + \Delta F_i^j(k) \tag{5}$$

$$\vec{G}_i^j(k) = \bar{\vec{G}}_i^j + \Delta \vec{G}_i^j(k) \tag{6}$$

The terms $\bar{F}_i^j$ and $\bar{\vec{G}}_i^j$ are the nominal values of the matrices $F_i^j(k)$ and $\vec{G}_i^j(k)$, respectively, are constant over each interval of interest, and are used in determining $x_i^j(k)$ for the reference signal. The time-varying terms $\Delta F_i^j(k)$ and $\Delta \vec{G}_i^j(k)$ reflect the perturbation in matrices $F_i^j(k)$ and $\vec{G}_i^j(k)$, respectively, that occur due to malfunction. Substituting equations (5) and (6) into equation (4) yields:

$$\begin{aligned} x_i^j(k+1) = &\left[\bar{F}_i^j + \Delta F_i^j(k)\right] x_i^j(k) + \\ &\left[\bar{\vec{G}}_i^j + \Delta \vec{G}_i^j(k)\right] \vec{u}_i^j(k) + \zeta_i^j w_i^j(k) \end{aligned} \tag{7}$$

Since the malfunction is uncertain, the perturbations $\Delta F_i^j(k)$ and $\Delta \vec{G}_i^j(k)$ are also uncertain.

ASSUMPTION 4: The perturbations $\Delta F_i^j(k)$ and $\Delta \vec{G}_i^j(k)$ are assumed to have the following characteristics: (1) Under nominal conditions (no malfunction), $\Delta F_i^j(k)$ and $\Delta \vec{G}_i^j(k)$ are zero; (2) Under malfunction conditions, the model of the random perturbations $\Delta F_i^j(k)$ and $\Delta \vec{G}_i^j(k)$ are generalized nonhomogeneous Poisson processes [7] with Gaussian coefficients [3]. Malfunctions affecting the control law calculations of *processor i* are independent.

Measurements from the processor that are input to the detector are:

$$z_i^j(k) = H_i^j x_i^j(k) + v_i^j(k) \tag{8}$$

$z_i^j(k)$ = measurement of jth control command from *processor i*; $z_i^j(k) \in R$; $i = 1, \ldots, N$; $j = 1, \ldots, M$

$x_i^j(k)$ = jth control command calculation from *processor i*, $x_i^j(k) \in R$

$v_i^j(k)$ = measurement noise for the jth control command of *processor i*, $v_i^j(k) \in R$

H_i^j = measurement weighting coefficient

ASSUMPTION 5: Measurement noise $v_i^j(k)$ is zero mean, Gaussian, and white with covariance matrix R_i^j. The measurement noise of the calculations of the ith processor are independent.

ASSUMPTION 6: Measurement noise $v_i^j(k)$ is assumed to be statistically independent of the initial state $x_i^j(k_0)$ and the process noise $w_i^j(k)$.

3. MONITOR DESIGN

The malfunctions to be detected are defined by Definition 1. Detection of the phenomenon in each of these definitions is binary and can, therefore, be defined in terms of the general hypotheses:

H_1 : Malfunction Condition

H_0 : Nominal (No Malfunction) Condition (9)

The calculations of the controller are observed via noisy measurements $\vec{z}_i(k)$ with probability density $p[\vec{z}_i(k) \mid H_i]$ from each of the processors.

The approach for detecting malfunctions in the control law calculations is shown in Figure 1:

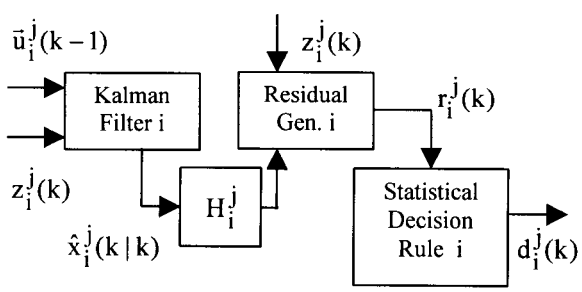

Fig. 1. Design Approach for Detecting Malfunctions in Control Law Calculation j of *Processor i*.

The control law calculation j of the ith processor is monitored using the residual:

$$r_i^j(k) = z_i^j(k) - H_i^j \hat{x}_i^j(k \mid k) \qquad (10)$$

where $z_i^j(k)$ and H_i^j are defined by equation (8), and $\hat{x}_i^j(k \mid k)$ is an estimate of $E\left[x_i^j(k) \mid X_i^{j^k}\right]$ defined in equation (2). The estimate $\hat{x}_i^j(k \mid k)$ can be produced using a Kalman filter. Under the stated assumptions and using a Gaussian approximation for the conditional density of the measurement under the malfunction hypothesis [3], the Bayesian decision rule can be shown to be:

$$r_i^j(k) \underset{d_i^j(k)=0}{\overset{d_i^j(k)=1}{\gtrless}} \lambda_i^j(k) \qquad (11)$$

where the threshold is defined for three cases.

Case 1: $P_{1i}^j(k) > P_{0i}^j(k)$

$$\lambda_i^j(k) = \left\{ \frac{\left[P_{0i}^j(k)\mu_{ri}^j(k)\right]^2}{\left[P_{1i}^j(k) - P_{0i}^j(k)\right]^2} + \frac{P_{0i}^j(k)\left[\mu_{ri}^j(k)\right]^2}{P_{1i}^j(k) - P_{0i}^j(k)} + \frac{2P_{1i}^j(k)P_{0i}^j(k)}{P_{1i}^j(k) - P_{0i}^j(k)} \ln \frac{\left[P_{1i}^j(k)\right]^{1/2} TH_i^j(k)}{\left[P_{0i}^j(k)\right]^{1/2}} \right\}^{1/2} - \frac{P_{0i}^j(k)\mu_{ri}^j(k)}{P_{1i}^j(k) - P_{0i}^j(k)} \qquad (12a)$$

$P_{0i}^j(k)$ = variance of the residual under hypothesis H_0

$P_{1i}^j(k)$ = variance of the residual under hypothesis H_1

$\mu_{ri}^j(k)$ = variance of the residual under hypothesis H_1

$TH_i^j(k)$ = Bayes Criterion

Case 2: $P_{1i}^j(k) < P_{0i}^j(k)$

$$\lambda_i^j(k) = \left\{ \frac{\left[P_{0i}^j(k)\mu_{ri}^j(k)\right]^2}{\left[P_{01i}^j(k) - P_{1i}^j(k)\right]^2} - \frac{P_{0i}^j(k)\left[\mu_{ri}^j(k)\right]^2}{P_{0i}^j(k) - P_{1i}^j(k)} - \frac{2P_{1i}^j(k)P_{0i}^j(k)}{P_{0i}^j(k) - P_{1i}^j(k)} \ln \frac{\left[P_{1i}^j(k)\right]^{1/2} TH_i^j(k)}{\left[P_{0i}^j(k)\right]^{1/2}} \right\}^{1/2} + \frac{P_{0i}^j(k)\mu_{ri}^j(k)}{P_{0i}^j(k) - P_{1i}^j(k)} \qquad (12b)$$

Note that for this case, the direction of the inequalities in equation (11) is reversed.

Case 3: $P_{1i}^{j}(k) = P_{0i}^{j}(k)$

$$\lambda_i^j(k) = \frac{\mu_{ri}^j(k)}{2} + \ln \frac{P_{0i}^j(k)\ln[TH_i^j(k)]}{\mu_{ri}^j(k)} \quad (12c)$$

The performance of the detector is determined by the probability of a false alarm and the probability of a missed detection. The probability of false alarm is:

$$\begin{aligned} Pf_i^j(k) &= P\left[d_i^j(k) = 1 \middle| H_0\right] \\ &= \int_{\lambda_i^j(k)}^{\infty} p_{H_0}\left[z_i^j(k) \middle| Z_i^{j^k}\right] dz_i^j(k) \end{aligned} \quad (13)$$

where $p_{H_0}\left[z_i^j(k) \middle| Z_i^{j^k}\right]$ is Gaussian [3] and $\lambda_i^j(k)$ is the threshold, given by equation (12a) - (12c), of the decision rule. The probability of a missed error detection in the jth calculation of the ith processor is:

$$\begin{aligned} Pm_i^j(k) &= 1 - P\left[d_i^j(k) = 1 \middle| H_1\right] \\ &= 1 - \int_{\lambda_i^j(k)}^{\infty} p_{H_1}\left[z_i^j(k) \middle| Z_i^{j^k}\right] dz_i^j(k) \end{aligned} \quad (14)$$

where $p_{H_1}\left[z_i^j(k) \middle| Z_i^{j^k}\right]$ is approximated by a Gaussian density [3] and $\lambda_i^j(k)$ is the threshold, given by equations (12a) - (12c) of the decision rule. It can be shown [3], that this approximation yields a conservative detector in the sense that the probability of a missed detection will be lower than that of the detector designed without the Gaussian approximation. However, the probability of false alarm will be higher in this detector.

4. SIMULATION EXAMPLE

The simulated controller calculates the control laws from a detailed closed-loop B737 Autoland Simulation. The implementation shown in this paper consists of the monitor for the elevator control law from a single processor. A Kalman filter estimates the correct calculation of the elevator control command. These estimates are used to generate residuals with the measured elevator command calculations. The elevator command calculation monitor performs a threshold test on the residual to make binary decisions on the occurrence of malfunction in the command calculation. The operating envelope for the simulated aircraft controller is from glideslope engaged until flare during the approach. During the landing, the aircraft is subjected to light clear air turbulence that consists of 20 kn. steady winds with 2 ft/s gusts.

Model parameters of equation (3) required for the Kalman filters are detailed in [6]. Since the elevator command is time-varying, it is modeled by a set of 27 linear models that are scheduled over the operating envelope from glideslope engaged until flare [6]. The interval over which each model is applied is referred to as the interval of interest for the detector associated with that model. Since the detector is model-based, it is scheduled with the model. Therefore, there are effectively 27 detectors that are scheduled over the operating envelope.

Analysis of data from laboratory experiments [1] – [2] is currently incomplete. Therefore, in this example, the mean and covariance of the residual under the malfunction hypothesis are postulated for illustration purposes. The mean and covariance of the disturbance are defined as follows for this simulation:

$$\mu_{ri}^j(k) \cong 2\left(\mu_{esterri}^j(k) + 3\sigma_{esterri}^j(k)\right) \quad (15)$$

$$P_{1i}^j(k) \cong P_{0i}^j(k) \quad (16)$$

where $\mu_{esterri}^j(k)$ is the mean of the estimation error under the nominal hypothesis and $\sigma_{esterri}^j(k)$ is the standard deviation of the estimation error under the nominal hypothesis over the interval of interest. In this simulation, the covariance under the malfunction hypothesis is set equal to that for the nominal hypothesis.

Since the *a priori* probabilities are unknown, the Bayes Criterion was determined by calculating the threshold of equation (12) over each interval

of interest with $TH_i^j(k)$ as the varying parameter. For this example, the value of the Bayes Criterion that optimized the tradeoff between probability of miss and probability of false alarm was determined to be the value at which these probabilities were equal. The Bayes Criteria that optimizes the performance of the detector over each interval of interest is shown in Figure 2.

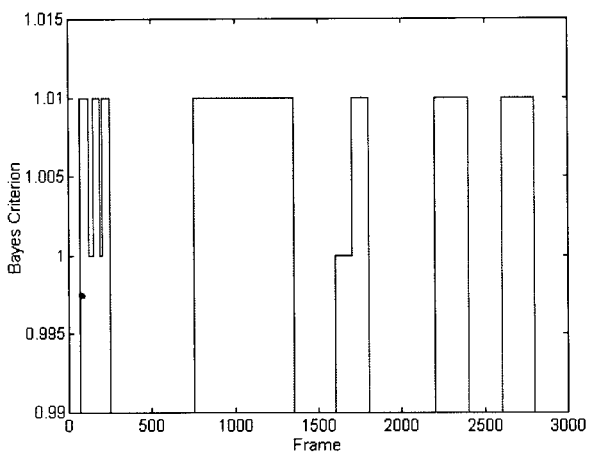

Figure 2: Optimal Bayes Criterion for the Detector Threshold of the Elevator Command Calculation Monitor from Glideslope Engaged until Flare

As seen in Figure 2, the optimal value of the Bayes Criterion for each interval of interest is a constant value between 0.99 and 1.01.

The threshold for the decision rule of equations (11) and (12) for the elevator command calculation monitor is shown in Figure 3.

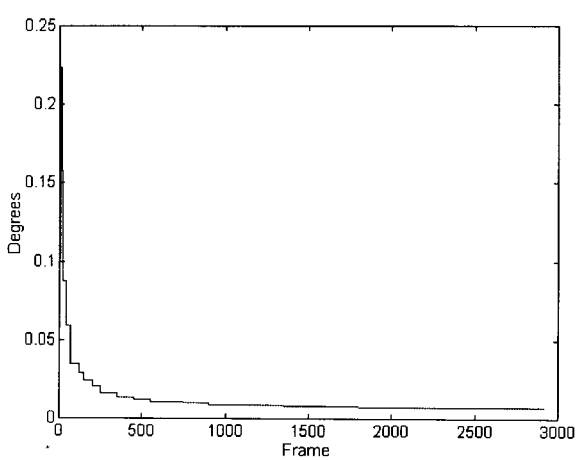

Figure 3: Detector Threshold for the Elevator Command Calculation Monitor from Glideslope Engaged until Flare

As seen in Figure 3, the thresholds for the first few intervals of interest are much larger than those for the rest of the operating envelope. This is because the first few intervals represent a mode switch to glideslope engaged. The model developed in [6] for this part of the operating envelope is more difficult to obtain and is not as accurate as those for the subsequent intervals. However, as seen in Figure 3, the threshold for the detector is less than 0.25 degrees everywhere in the operating envelope including the first few intervals. Therefore, elevator command calculation errors of very small magnitude can be detected. This is desirable since aircraft roll is fairly sensitive to changes in elevator position with the total elevator deflection being +/- 10 degrees.

The probability of false alarm for the elevator command monitor is shown in Figure 4.

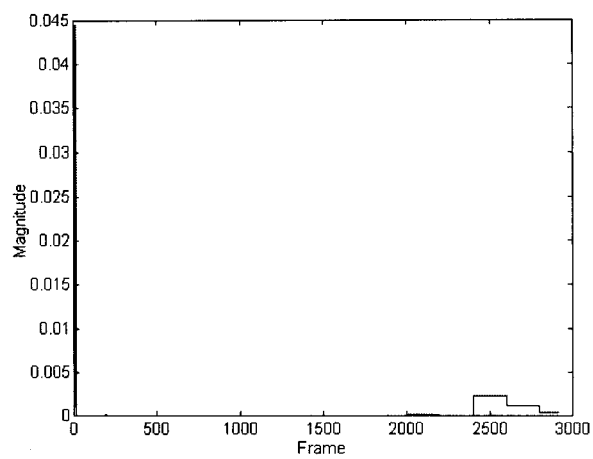

Figure 4: Probability of False Alarm for the Detector of the Elevator Command Calculation Monitor

As seen in Figure 4, the highest probability of a false alarm is in the first few intervals. However, even in these intervals, the probability of false alarm is less than 0.045. Everywhere else in the operating envelope, the probability of a false alarm is more than an order of magnitude less likely.

The probability of a missed detection for the Bayesian elevator command calculation monitor is shown in Figure 5.

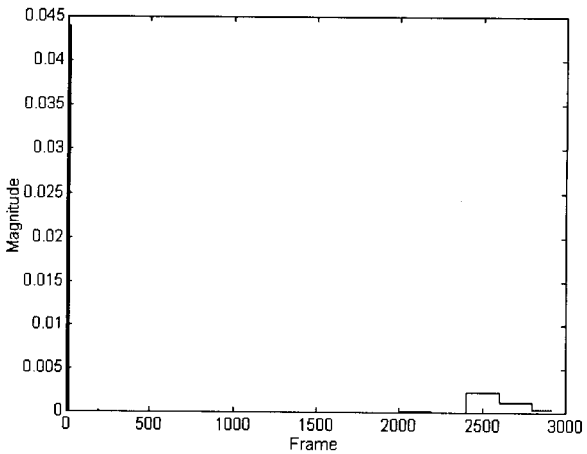

Figure 5: Probability of a Missed Detection for the Detector of the Elevator Command Calculation Monitor from Glideslope Engaged until Flare

As can be seen in Figure 5, the probability of a missed detection is less than 0.045 in the first few intervals and more than an order of magnitude less likely everywhere else in the operating envelope. Note that the probabilities of a missed detection and false alarm, shown in Figures 4 and 5, are essentially equal. This is because the Bayes Criterion used in the design of the threshold was selected such that these probabilities would be equal.

5.0 SUMMARY AND CONCLUSIONS

This paper presents an improved dynamic detection technique that can be applied to detect malfunctions in a fault tolerant control computer. Malfunction in the controller is detected by monitoring the control law calculations. The monitoring strategy was demonstrated for the elevator command of the B737 Autoland simulation under light clear air turbulence from glideslope engaged until flare. Detector performance was analyzed in terms of probability of false alarm and probability of a missed detection. These probabilities were determined to be less than 0.045, even under mode switching. The methodology for monitoring control integrity that was presented in this paper is limited by the stated assumptions. The Gaussian and independence assumptions for malfunctions in the control laws idealize conditions that could occur. Analysis of controller malfunction data obtained during laboratory experiments is in progress and may reveal the shortcomings of these assumptions. In the event that the assumptions are invalid, the design of the detector will be modified. Future work includes: i) assessment of the validity of assumptions made in the design of the detector using controller malfunction data obtained in laboratory experiments; ii) the removal of invalid assumptions for a redesign of the monitor to account for non-Gaussian densities and correlation between observations; and iii) implementation and demonstration of the monitor in the laboratory.

REFERENCES

1. Belcastro, C. M., "Closed-Loop HIRF Experiments Performed on a Fault Tolerant Flight Control Computer", Proceedings of the Digital Avionics Systems Conference, Irvine CA, October 1997
2. Belcastro, C. M., "Ensuring Control Integrity of Critical Systems Subjected to Electromagnetic Disturbances: Problem Overview", Proceedings of the American Control Conference", Philadelphia PA, June 1998
3. Belcastro, C. M., "Detecting Upset in Fault Tolerant Control Computers Using Data Fusion Techniques", Ph.D Dissertation, Drexel University, December 1994
4. Belcastro, C. M., Fischl, R. F., "Monitoring Functional Integrity in Fault Tolerant Aircraft Control Computers for Critical Applications", Proceedings of the International Federation of Automatic Control, San Francisco CA, June 1996
5. Belcastro, C. M., "Monitoring Functional Integrity in Critical Control Computers Subjected to Electromagnetic Disturbances", Proceedings of the American Control Conference, Philadelphia PA, June 1998
6. Weinstein, B., "Detecting Controller Malfunctions in EME: Part I – Modeling & Estimation of Nominal System Function", Proceedings of the Conference on Control Applications, Hawaii, 1999
7. Maybeck, P. S., Stochastic Models, Estimation, and Control, vol. 2., Academic Press, New York, 1982