Abstract—A performance model is introduced for estimating the tracking error of a Boeing 747 closed-loop digital flight control system implemented on a distributed recoverable computing platform, inspired by NASA’s ROBUS-2 communication system, when it is subjected to digital upsets. A methodology is then developed for computing a mean-square error tracking performance metric as a function of the number of processing elements used, the number of redundancy management units employed, and the level of upsets the system experiences.

I. INTRODUCTION

Under nominal operating conditions, the performance of a digital flight control system can be completely characterized by the dynamics of the aircraft, its systems (sensors and actuators) and the specific control law utilized. The computing platform on which the control system is implemented is largely irrelevant to the closed-loop system. But in a harsh environment, where certain fault-tolerant features of the computer architecture might be exercised beyond the fault assumptions, a degradation in control performance may be observed. The specific nature of this change in performance is a complex function of the environment, the physical implementation of the electronic systems, the digital design choices, the aircraft dynamics, and the control law. Digital electronics are affected, for example, by high intensity radiated fields (HIRF) [4]–[6], [12] and neutron radiation [20]–[22]. HIRF environments are known to trigger common-mode faults, affecting nearly-simultaneously multiple fault containment regions, and thereby reducing the benefits of n-modular redundancy, error correcting codes, and other fault-tolerant computing techniques [1], [2], [6], [8]. Thus, it is important to develop models which describe the integration of the embedded digital system, where the control law is implemented, and the dynamics of the closed-loop system. System designers and test engineers at all levels would benefit from the availability of such models for estimating the level of performance degradation in a given scenario.

In [7] a hybrid performance model was introduced for a Boeing 737 digital flight control system implemented on a distributed recoverable computing platform inspired largely by the NASA family of computer architectures known as SPIDER (Scalable Processor-Independent Design for Enhanced Reliability). The focus was on the SPIDER implementation which uses the computer communication system known as ROBUS-2 [10], [13], [14]. The primary goal was to develop a methodology for computing a mean-square error tracking performance metric as a function of the number of processing elements used, the number of redundancy management units employed, and the level of digital upsets the control system experienced. The analysis was accomplished largely using tools for jump-linear systems. The analysis presented, however, was not complete because the stochastic nature of the switching signal was not totally understood. The transition probabilities, for example, had to be estimated by Monte Carlo simulation. The present paper is a sequel to [7] in that a complete analytical treatment of the performance model is now possible given the recent theoretical advances reported in [3]. In addition, a higher fidelity Boeing 747 model is employed for the tracking performance analysis, one that has been validated against the full nonlinear aerodynamic models [9], [19]. Finally, a more complete treatment of correlated upsets in the redundancy management units is presented. This case turns out to be the most relevant for the ROBUS-2 system.

The paper is organized as follows. In the next section, the distributed computing system architecture under consideration is described, and, in parallel, its system level model developed in [7] is summarized. In Section III, the statistical nature of the model’s switching signal is completely characterized analytically and verified by simulation. In the subsequent section, the model’s tracking performance predictions are computed theoretically and compared against simulations. The final section summarizes the results of the paper and plans for future research.

II. CONTROLLER IMPLEMENTATION

The digital control system under consideration is assumed to be implemented on a distributed recoverable computational platform inspired by the ROBUS-2 communication system. It consists of \( N \) Processing Elements (PE’s) dedicated to calculating the updates of the control law at each sample period (\( T \)) and \( M \) Redundancy Management Units (RMU’s), which coordinate the communications between the PE’s by supplying full and reliable message transferring capability. The Bus Interface Units (BIU’s) are logical devices which provide the interfaces between the PE’s and the communication system. In the present application, an additional PE is employed as an input-output interface to the actuators. The processing units (PE’s and RMU’s) in the current prototype are all constructed from off-the-shelf devices. More details concerning the hardware implementation and the underlying theory on which the design is based can be found in [10], [13], [14]. An example of the specific interconnection topology under consideration for the distributed control system is shown in Fig. 1. Throughout this paper, the following assumptions will be in place:

A1) Each processing unit is recoverable within one sample period.
A2) The same control law is replicated in all $N$ PE’s.

A3) Each ROBUS-2 node (PE-BIU, RMU) is fail-silent. So a node stops transmitting data when an internal upset is detected. The fail-silent detection is assumed not to fail, i.e., it has 100% coverage.

A4) Each ROBUS-2 node forms an independent fault containment region.

A5) The state of each PE, say $z_i(k)$, is identically broadcast to the $i$-th channel of each RMU.

A6) The I/O PE is not subject to upset.

The model developed next is an abstraction from a control system point of view of how the information needed to compute control updates flows through the network. It is not a model of the actual digital layer of the communication system. The injected input disturbances, $\theta_i(k)$ and $\nu_{ij}(k)$, are random variables taking on the value ‘1’ when an upset is being injected and ‘0’ otherwise. The BIU outputs, $z_i(k)$, are binary random variables representing the state of their associated PE at time $k$. When $z_i(k)$ is ‘0’, the processor is functioning properly at time $k$ and will therefore provide the correct update to the control law at that instant. Otherwise, it is upset, and by assumption A3 it does not transmit a control law update. The state transition table for the PE with disturbance input $\theta_i(k)$ is given in Table I. The state of the $i$-th channel of the $j$-th RMU, namely $\tilde{z}_{ij}(k)$, is also subject to upset, specifically from the disturbance input $\nu_{ij}(k)$. When the output of a channel is ‘1’, it is not capable of reliably transmitting data from its associated PE to the I/O PE. The state transition table for the $i$-th channel of the $j$-th RMU is shown in Table II. It is basically identical to that for a PE. The output of the $ij$-th channel, $\tilde{y}_{ij}(k)$, is the logical OR of $\tilde{z}_{ij}(k)$ and $\tilde{z}_{ij}(k)$ signifying that a control update is not available on this channel at time $k$ if and only if the PE or the RMU are upset at this instant. The outputs of each communication channel are next fed to the I/O PE, in this case modeled as a logical AND. This sequential and combinatorial logic can be represented by a finite-state machine. If the I/O PE output $z_v(k) = 1$, then a control update is not possible for the closed-loop system, and it must operate in the upset mode until the next opportunity for an update at the $k+1$-th sample. Otherwise, the system operates in the nominal mode.

III. STATISTICAL NATURE OF THE I/O PE OUTPUT $z_v(k)$

It is known that when a finite-state machine is driven by an i.i.d. random process, its state process will be a homogeneous first-order Markov chain [11], [20]. The corresponding output process, however, need not be Markov of any order. Nevertheless, the output process $z_v(k)$ in the present application is particularly well behaved as described in the next theorem.

Theorem I: Consider an $N$ PE $\times M$ RMU network of the type shown in Fig. 1. Assume all the upset processes are mutually independent with the possible exception that the correlation coefficient between any two channel upsets in the same RMU is $r$. Then the I/O PE output process $z_v(k)$, $k \geq 1$ is an i.i.d. random process completely characterized by the stationary probability $p_1 := P\{z_v(k) = 1\}$ with

$$p_1 = (1 - (1 - p_\theta)(1 - p_{\nu}^M))^N$$

\[ (1) \]
TABLE III
THEORETICAL VALUES OF $p_1$ FOR DIFFERENT NUMBERS OF PE’S AND RMU’S WHEN $p_\theta = p_\nu = 0.05$ AND $r = 0.$

<table>
<thead>
<tr>
<th>PE’s</th>
<th>1 RMU</th>
<th>2 RMU’s</th>
<th>3 RMU’s</th>
<th>4 RMU’s</th>
<th>5 RMU’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9.7506e-002</td>
<td>5.2375e-002</td>
<td>5.0119e-002</td>
<td>5.0006e-002</td>
<td>5.0000e-002</td>
</tr>
<tr>
<td>2</td>
<td>1.5063e-003</td>
<td>2.7411e-003</td>
<td>2.5119e-003</td>
<td>2.5006e-003</td>
<td>2.5000e-003</td>
</tr>
<tr>
<td>3</td>
<td>9.2686e-004</td>
<td>1.4367e-004</td>
<td>1.2589e-004</td>
<td>1.2504e-004</td>
<td>1.2500e-004</td>
</tr>
<tr>
<td>5</td>
<td>8.8110e-006</td>
<td>3.1623e-007</td>
<td>3.1625e-007</td>
<td>3.1269e-007</td>
<td>3.1251e-007</td>
</tr>
</tbody>
</table>

TABLE IV
THEORETICAL VALUES OF $p_1$ FOR DIFFERENT NUMBERS OF PE’S AND RMU’S WHEN $p_\theta = p_\nu = 0.05$ AND $r = 1.$

<table>
<thead>
<tr>
<th>PE’s</th>
<th>1 RMU</th>
<th>2 RMU’s</th>
<th>3 RMU’s</th>
<th>4 RMU’s</th>
<th>5 RMU’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9.7506e-002</td>
<td>5.2375e-002</td>
<td>5.0119e-002</td>
<td>5.0006e-002</td>
<td>5.0000e-002</td>
</tr>
<tr>
<td>2</td>
<td>2.5375e-002</td>
<td>4.9937e-003</td>
<td>2.5606e-003</td>
<td>2.5006e-003</td>
<td>2.5000e-003</td>
</tr>
<tr>
<td>3</td>
<td>5.0119e-002</td>
<td>2.6247e-003</td>
<td>2.6247e-003</td>
<td>2.5125e-004</td>
<td>1.2531e-004</td>
</tr>
<tr>
<td>4</td>
<td>5.0606e-002</td>
<td>2.5062e-003</td>
<td>1.3125e-004</td>
<td>1.2506e-005</td>
<td>6.5625e-006</td>
</tr>
<tr>
<td>5</td>
<td>5.0000e-002</td>
<td>2.5003e-003</td>
<td>2.5125e-004</td>
<td>6.5625e-006</td>
<td>6.2500e-007</td>
</tr>
</tbody>
</table>

Fig. 2. Theoretically computed $\log_{10}(p_1)$ versus the number of PE’s and as a function of the number of RMU’s when $p_\theta = p_\nu = 0.05$ and $r = 0.$

when $r = 0$, and

$$p_1 = 1 - (1 - p_\theta^N)(1 - p_\nu^M) \quad (2)$$

when $r = 1$.

Proof: The assertion that $z_r(k)$, $k \geq 1$ is i.i.d. follows directly from the fact that the state processes $z(k)$ and $\tilde{z}(k)$ are i.i.d., since they are delayed versions of $\theta(k)$ and $\nu(k)$, respectively, and Lemma 7 in [3]. (The initial conditions $z(0)$ and $\tilde{z}(0)$ are always set to zero.) The identity (1) was proved in [7]. To verify (2), observe that $z_r(k) = 0$ exactly when at least one PE is not upset and one RMU is not upset, which are independent events since their respective disturbances are independent. The probability that all the PE’s are upset is $p_\theta^N$. Since $r = 1$, the probability that all the RMU’s are upset is $p_\nu^M$. Thus,

$$P\{z_r(k) = 0\} = (1 - p_\theta^N)(1 - p_\nu^M),$$

and the identity is proved.

Equation (1) is evaluated in Table III for various choices of $N$ and $M$ when $p_\theta = p_\nu = 0.05$, which is representative of ROBUS-2’s susceptibility in certain HIRF environments [15]–[17]. For comparison, (2) is evaluated in Table IV. In the special case where no RMU upsets occur, i.e., $p_\nu = 0$, observe that equations (1) and (2) both simplify to $p_1 = p_\theta^N$. The probability $p_1$ is plotted logarithmically as a function of $N$ and $M$ in Figs. 2 and 3 for $r = 0$ and $r = 1$, respectively. Of particular interest in the $r = 0$ case is the negligible difference between having no RMU upsets and having two or more RMU’s. For the disturbance level indicated, the benefit of having more than two RMU’s diminishes quickly. This is consistent with observations in reliability theory concerning parallel connections [18, p. 231]. The current implementation of ROBUS-2, however, is best modeled by the $r = 1$ case, since the entire RMU platform resets itself when any transmission error is detected. As the redundancy level is significantly reduced in this scenario, the saturation effect of adding more RMU’s is less pronounced as illustrated in...
modeled by a switched linear system of the form
\[ x(k+1) = A_{x_v(k)}x(k) + B_{x_v(k)}w(k), \]  \hspace{1cm} (3a)
\[ y(k) = C_{x_v(k)}x(k). \]  \hspace{1cm} (3b)

The nominal state space model \((A_0, B_0, C_0)\) was obtained using the linearization routine provided by FTLAB747 assuming straight and level flight (thus, \(r(k) = 0\), a cruising airspeed of 241 m/s and an altitude of 7000 m. The upset model \((A_1, B_1, C_1)\) was derived directly from the closed-loop model by setting the \(B\) matrix of the (default) \(H_{\infty}\) optimal control law equal to zero. Therefore, the control system could not process any new sensor data when computing the next control update. The state space models also include the Dryden turbulence spectral shaping filters. The white Gaussian noise input \(w(k)\) drives these shaping filters, which in turn inject the process noise \(v(k)\) into the control-loop. A sampled-data representation of each state space model was derived using a sampling frequency of 130 Hz. A comparison between the outputs of the continuous-time nonlinear and linear models is shown in Figs. 7 and 8 for the nominal closed-loop and upset closed-loop systems, respectively, under light turbulence conditions (1 m/s). Normally, the system will not operate in the upset mode for more than a second or two, so the upset model was judged to be sufficiently accurate.

In the event there are no upsets injected into the control computer, the nominal control system produces acceptable tracking performance. To quantify any degradation of performance in the presence of upsets, the error system shown in Fig. 9 was utilized. It consists of two copies of system (3)
having the same input $w(k)$. One system acts as a reference system and is never switched into the upset mode, while the other system is switched by the upset signal $z_u(k)$ to simulate digital upsets. The difference between their respective outputs produces the output error signal $y_e(k)$. The overall performance model is then a cascade of three subsystems as shown in Fig. 10. The performance index of interest is the mean power in the output tracking error

$$J_{w,e} = \lim_{k \to \infty} E\{\|y_e(k)\|^2\}.$$  

The limit will exist provided the error system is mean-square stable. The ultimate goal of this paper is to demonstrate how one can analytically compute $J_{w,e}$ as a function of the network topology and upset probabilities.

Theoretical values of the tracking error metric $J_{w,e}$ were determined using established theory for jump-linear systems. The specific approach summarized below is developed more extensively in [3]. Consider an arbitrary jump-linear system

$$x(k + 1) = A_{\rho(k)} x(k) + B_{\rho(k)} w(k), \quad x(0) = x_0$$

$$y(k) = C_{\rho(k)} x(k),$$

where the i.i.d. process $\rho(k)$ has states labeled by the symbols $\{\mu_l : l = 0, 1, \ldots, \ell - 1\}$. The following notion of stability is standard for this class of systems, as is the subsequent stability test.

**Definition 1:** The i.i.d. jump-linear system (4) is mean-square stable (MSS) if there exists a non-negative real number $\alpha$ such that $E\{\|x(k)\|^2\} \to \alpha$ as $k \to \infty$ for any initial condition $x_0$ with a finite second-order moment.

**Theorem 2:** The i.i.d. jump-linear system (4) is MSS if and only if $r_\rho(A) < 1$, where

$$A = \sum_{i=0}^{\ell-1} (A_i \otimes A_i)p_i,$$

$\otimes$ denotes the Kronecker product, $p_i = P\{\rho(k) = \mu_l\}$, and $r_\rho(\cdot)$ is the spectral radius.

**Theorem 3:** If the i.i.d. jump-linear system (4) is MSS when the distribution of $\rho(k)$ is $P = [p_0 \cdots p_{\ell-1}]$ for $k \geq 0$ then it follows that

$$J_w = \lim_{k \to \infty} E\{\|y(k)\|^2\} < \infty.$$ 

In particular,

$$J_w = \sum_{i=0}^{\ell-1} \text{tr}(C_i Q C_i^T)p_i,$$

where

$$Q = \sum_{i=0}^{\ell-1} (A_i A_i^T + B_i B_i^T)p_i = \text{vec}^{-1} ((I - A)^{-1} \text{vec}(B))$$

![Fig. 7. Continuous-time, nominal closed-loop linear (black) and nonlinear (gray) responses to light turbulence.](image)

![Fig. 8. Continuous-time, upset closed-loop linear (black) and nonlinear (gray) responses to light turbulence.](image)

![Fig. 9. The error system used for the tracking performance analysis.](image)

![Fig. 10. Performance model for the distributed recoverable Boeing 747 flight control system.](image)
with $\mathcal{A}$ defined in Theorem 2,
\[
B = \left( \sum_{i=0}^{L-1} B_i B_i^T p_i \right),
\]
and vec denotes the column stacking operator.

Theorem 3 is applied in the present context to the error system, which itself has two modes: $\mu_0 = 0$ (both subsystems are in the nominal mode) and $\mu_1 = 1$ (the switched system is in the upset mode). The corresponding spectral radius of $\mathcal{A}_e$ is shown in Figs. 11 and 12 for the $r = 0$ and $r = 1$ cases. For all typical upset probabilities, it is clear that the metric $J_{w,e}$ will be finite. In Figs. 13 and 14, the theoretical performance metrics are shown for each system output as a function of the upset probabilities assuming a 2 PE x 2 RMU control system implementation. From these plots one can directly determine whether the tracking performance is acceptable for any specified level of upsets. This system was also simulated by Monte Carlo methods. The values of $J_{w,e}$ estimated by simulation are given in Tables VI and VII for various configurations. They agree well with the theoretical values. A typical simulated tracking error response is shown in Fig. 15.

V. CONCLUSIONS AND FUTURE RESEARCH

In this paper, a performance model was employed to estimate the tracking error of a Boeing 747 control system implemented on a distributed recoverable computing platform, inspired by NASA’s ROBUS-2 communication system, when subject to digital upsets. In particular, a mean-square error tracking performance metric was computed as a function of the number of processing elements used, the number of redundancy management units employed, and the level of upsets the system experiences. Future work will include the


**TABLE VI**
A COMPARISON BETWEEN THEORY AND SIMULATION FOR VARIOUS DISTRIBUTED ARCHITECTURES WHEN \( r = 0 \).

<table>
<thead>
<tr>
<th>PE × RMU</th>
<th>( p_0 )</th>
<th>( p_0 )</th>
<th>( p_1 ) theory</th>
<th>( p_1 ) sim.</th>
<th>( J_{w,e} ) theory</th>
<th>( J_{w,e} ) sim.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 × 2</td>
<td>0.05</td>
<td>0.01</td>
<td>2.5095e-03</td>
<td>2.5026e-03</td>
<td>1.0305e-05</td>
<td>1.0304e-05</td>
</tr>
<tr>
<td>2 × 2</td>
<td>0.05</td>
<td>0.05</td>
<td>2.7431e-03</td>
<td>2.7350e-03</td>
<td>1.1284e-05</td>
<td>1.1298e-05</td>
</tr>
<tr>
<td>2 × 2</td>
<td>0.5</td>
<td>0.5</td>
<td>3.9063e-01</td>
<td>3.9059e-01</td>
<td>6.5020e-03</td>
<td>6.5208e-03</td>
</tr>
<tr>
<td>2 × 3</td>
<td>0.05</td>
<td>0.01</td>
<td>2.3001e-03</td>
<td>2.4984e-03</td>
<td>1.0276e-05</td>
<td>1.0305e-05</td>
</tr>
</tbody>
</table>

**TABLE VII**
A COMPARISON BETWEEN THEORY AND SIMULATION FOR VARIOUS DISTRIBUTED ARCHITECTURES WHEN \( r = 1 \).

<table>
<thead>
<tr>
<th>PE × RMU</th>
<th>( p_0 )</th>
<th>( p_0 )</th>
<th>( p_1 ) theory</th>
<th>( p_1 ) sim.</th>
<th>( J_{w,e} ) theory</th>
<th>( J_{w,e} ) sim.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 × 2</td>
<td>0.05</td>
<td>0.01</td>
<td>2.5095e-03</td>
<td>2.5010e-03</td>
<td>1.0280e-05</td>
<td>1.0257e-05</td>
</tr>
<tr>
<td>2 × 2</td>
<td>0.05</td>
<td>0.05</td>
<td>2.7431e-03</td>
<td>2.7350e-03</td>
<td>1.1284e-05</td>
<td>1.1298e-05</td>
</tr>
<tr>
<td>2 × 2</td>
<td>0.5</td>
<td>0.5</td>
<td>3.9063e-01</td>
<td>3.9059e-01</td>
<td>6.5020e-03</td>
<td>6.5208e-03</td>
</tr>
<tr>
<td>2 × 3</td>
<td>0.05</td>
<td>0.01</td>
<td>2.3001e-03</td>
<td>2.4984e-03</td>
<td>1.0276e-05</td>
<td>1.0305e-05</td>
</tr>
</tbody>
</table>

Fig. 15. Simulated tracking error \( E[\|p_e(kt)\|^2] \) (black) for a 2 PE × 2 RMU system when \( p_0 = p_0 = 0.5 \) and \( r = 0 \) compared to the theoretical limit \( J_{w,e} \) (gray).

development of an experimental testbed to provide a real world validation of the methodology.

**REFERENCES**


