Proceedings of the 34th
Conference on Decision & Control
New Orleans, LA - December 1995

Incorporation of System Inertia into Reliability Evaluation of Real-Time Control Systems

Kang G. Shin and Lisa Guo

Real-Time Computing Laboratory
Department of Electrical Engineering and Computer Science
The University of Michigan
Ann Arbor, Michigan 48109–2122.
email: {kgshin,lguo}@eecs.umich.edu
Phone numbers: 313-763-0391 (voice); 313-763-4617 (fax)

Abstract – The control system inertia is characterized as the *control system deadline* (CSD). A computer controller may sometimes fail to produce correct and/or timely control signals due to massive component failures caused by external environmental interferences. However, the underlying control system does not necessarily crash immediately upon controller failure. The CSD is defined as the maximum time the control system can stay in its allowed state space without the computer controller's services in producing correct and/or timely control signals. Through the analysis and simulation of the Boeing 737 — a typical real-time control system — we characterized the CSD as a random variable. When evaluating the system reliability with the CSD knowledge, we need not derive the complete distribution of CSD, but need only the first and second moments, thus simplifying the necessary calculation. Finally, we applied the CSD knowledge to the system reliability evaluation, showing significant improvements in accuracy.

Key words: Real-time control systems, deadline, fault-tolerance, reliability models.

1 Introduction

Most existing control-system designs do not consider component failures during a given control mission. Consideration of possible component failures calls for the need of some form of fault-tolerant control. Adaptive control can be viewed as a faul-tolerant control option, because system parameters are estimated for every control cycle and the control law is adapted to the change in the parameters. There are many other fault-tolerant control algorithms that are widely discussed in the open literature. Willsky [1] surveyed the methods of detecting failures in a control system. To improve the reliability of a control system, we must resort to some form (time, space, or both) of redundancy. References [2, 4, 7, 8] are examples. These studies are based on one common assumption: the computer system can conduct all of detection and reconfiguration tasks even when other components of the control system fail.

The work reported in this paper was supported in part by the NASA under Grant NAG-1-1220 and the ONR under Grant No. N00014-91-J-1115. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of NASA or ONR.

Siljak [9] proposed a mathematical framework for analyzing redundant computer controllers, taking computer failure into consideration. But he assumed that computer failures are independent of one another. However, in some cases, computers located close to each other tend to be exposed to the same environmental interference, which may cause all the computers to fail at the same time. Even when computers do not provide correct control signals, the system may not crash immediately due to system inertia. If the fault can be removed within a certain time, the computer might be able to control the system back to normal operation. Shin *et al.* [10] proposed a general concept of the control system deadline (CSD) when the computer controller does not work as specified. Kim and Shin [11] studied in greater detail how to derive the CSD for linear and nonlinear systems. In this paper, we will consider the random behavior of CSD and incorporate this information into the reliability analysis of control systems. Section 2 introduces the definition of CSD and analyzes it as a function of some other variables for linear systems. Section 3 presents a numerical example to illustrate our idea of considering CSD as a random variable, not as a constant. Reliability analysis incorporating the CSD is presented in Section 4. The paper concludes with Section 5.

2 Analysis of Control System Deadlines

Shin *et al.* [10–12] proposed the concept of CSD and developed general methods for deriving it. For completeness, we first present a brief summary of their results and then analyze the CSD in depth for linear systems.

Let $\mathbf{x}(t)$ denote the state of the controlled process at time t, then state transitions can be characterized by a mapping ϕ: $\mathbf{T} \times \mathbf{T} \times \mathbf{X} \times \mathbf{U} \rightarrow \mathbf{X}$, where $\mathbf{T} \subset \mathbf{R}$ represents the time region, $\mathbf{X} \subset \mathbf{R}^n$ the state space, and $\mathbf{U} \subset \mathbf{R}^\ell$ the input space: $\mathbf{x}(t_1) = \phi(t_1, t_0, \mathbf{x}(t_0), \mathbf{u})$. More specifically, if we have a dynamic system

$$\dot{\mathbf{x}} = \mathbf{f}(t, \mathbf{x}, \mathbf{u}) \tag{2.1}$$

then ϕ can be considered as a solution to Eq. (2.1) given the initial condition $\mathbf{x}(t_0)$ at time t_0. Given a control

0-7803-2685-7/95 $4.00 © 1995 IEEE

law $\mathbf{u}$, the CSD is defined as

$$\tau(\mathbf{x}(t_0)) \equiv \sup\{\tau \ : \ \phi(t_0+\tau, t_0, \mathbf{x}(t_0), \mathbf{u}) \in \mathbf{X}_A\}$$

where $\mathbf{X}_A$ is the allowed state space. $\mathbf{X}_A$ is the intersection of two sets of states. The first set, denoted by $\mathbf{X}_A^1$, is the state space in which a system must stay in order to avoid immediate failure, e.g., a commercial airplane flying upside down. The second set, denoted by $\mathbf{X}_A^2$, is the state space where a system must stay in order to meet terminal constraints, e.g., airplane landing conditions.

Normally, a predesigned control law should not only keep the controlled process in the allowed state space, but also provide satisfactory performance. But if under external environmental interferences, a controller computer may fail to work properly, not only degrading the control system performance, but also possibly driving the system out of the allowed state space. If the controller computer failed at t_f, then the CSD is defined as the maximum time after t_f that the system can stay in the allowed state space under the erroneous control signals before the controller recovers from the failure and resumes the normal control function. In this paper, we focus on linear systems, because nonlinear systems are usually approximated by piecewise linear systems along a given nominal trajectory.

First, consider a single-variable system $\dot{x} = ax + bu$ with the control law $u = kx$, where a, b and k are constant. Let t_d denote the time period between t_f and the time when the controller computer is recovered from a failure. During this time, the control is not updated, but kept constant at u_{t_f}. In some cases, the controller computer may update the control signal "randomly" as opposed to just failing to update it. The control signal during t_d depends on the application's error handling mechanism. Here we will not discuss every possible case, but our discussion is general and applicable to other situations as well as the constant control signal during t_d.

Given the mission lifetime T, the terminal state is

$$x(T) = e^{(a+bk)(T-t_d)}\left\{e^{at_d} + \int_0^{t_d} e^{a(t_d-\tau)}d\tau bk\right\}x(0)$$

Let $M = e^{(a+bk)(T-t_d)}\left\{e^{at_d} + \int_0^{t_d} e^{a(t_d-\tau)}d\tau bk\right\}$. Note that M is not a function of t_f. From the terminal constraint $|x(T)| < \varepsilon$, we have $|M| < \frac{\varepsilon}{|x(0)|}$. The largest t_d which satisfies the above inequality is the CSD. It depends on the initial condition $x(0)$, the terminal constraint ε, mission lifetime T, and the feedback gain k. The shorter the mission time and the larger the difference between the initial condition and the terminal constraint, the smaller t_d gets.

Multivariable systems are more complicated due to the coupling between state variables. We should first choose the form of the terminal constraints. Unlike the single-variable case in which there is one obvious choice, there are several ways to specify the terminal constraints. One way is to have a constraint for each state variable, i.e., $|x_i(T)| < \varepsilon_i$. The problem with this method is that due to the coupling of state variables, the absolute value of each state is not necessarily monotone. In order to solve this problem, as the second approach, one may restrict the norm of the terminal state, i.e., $\| x_T \| < \varepsilon$. The norm of the state should decrease to 0 as T gets larger. The third approach is a more general than the second, taking a weighted sum of the state variables. We have chosen the second approach because the third approach requires knowledge of relative importance of each state variable, which is often unavailable and/or depends on the underlying application.

Consider a linear system $\dot{\mathbf{x}} = \mathbf{Ax} + \mathbf{Bu}$ with the control law $\mathbf{u} = \mathbf{Kx}$ where $\mathbf{x}$ and $\mathbf{u}$ are n- and p- dimensional vectors, respectively. $\mathbf{A}, \mathbf{B}$ and $\mathbf{K}$ are constant matrices with appropriate dimensions. The terminal state is then derived as:

$$\mathbf{x}(T) = e^{(\mathbf{A}+\mathbf{BK})(T-t_f-t_d)}\{e^{\mathbf{A}t_d} + (\int_0^{t_d} e^{\mathbf{A}(t_d-\tau)}d\tau)\mathbf{BK}\}e^{(\mathbf{A}+\mathbf{BK})t_f}\mathbf{x}(0) = \mathbf{M}\mathbf{x}(0).$$

Given the initial condition, terminal constraint, mission time, $\mathbf{M}$ is also a function of t_f (time when the controller computer fails), which is different from the single-variable case where the CSD is independent of t_f. To meet the terminal constraints, the following inequality should be satisfied:

$$\| \mathbf{M}\mathbf{x}(0) \| < \varepsilon \tag{2.2}$$

Inequality (2.2) indicates that the CSD not only depends on the norm of initial condition, but also the direction of the initial condition. Let $\overline{\sigma}(\mathbf{M})$ and $\underline{\sigma}(\mathbf{M})$ denote the maximum and minimum singular value of $\mathbf{M}$, then we have

$$\underline{\sigma}(\mathbf{M}) \| \mathbf{x}(0) \| \leq \| \mathbf{M}\mathbf{x}(0) \| \leq \overline{\sigma}(\mathbf{M}) \| \mathbf{x}(0) \|$$

The most conservative estimation of CSD would be the largest t_d which satisfies $\overline{\sigma}(\mathbf{M}) \| \mathbf{x}(0) \| < \varepsilon$. It guarantees the worst case since the CSD thus derived is a lower bound. When the condition number of matrix $\mathbf{M}$ is very large, the CSD can vary drastically for different initial conditions. One can see this from an example in Section 3. If we evaluate system reliability according to the most conservative estimate of CSD, the reliability is underestimated and the cost of fault tolerance will be much higher than necessary. Our solution to this problem is to consider the CSD as a random variable and derive its distribution for a particular application.

We will use a numerical example to illustrate the characteristics of the CSD of a linear control system.

3 A Numerical Example

We have chosen the Boeing 737 as our example control system, because it is a typical real-time control system and its detailed dynamics are readily available to us via the NASA Langley Research Center.

3.1 Overview of the Example Control System

The perturbation equation of the Boeing 737 is derived by linearizing its nonlinear dynamics along a trajectory during the landing phase, which consists of a constant path angle and a constant airspeed. The trim conditions are: forward speed UB=213.98627 ft/sec,

vertical speed WB=8.5686209 ft/sec, pitch attitude THETA=−0.012338403 rads, pitch rate QB=0. Control signals are: THRUST=8504.9006 lbs, ELEVATOR=2.723202 rads. The perturbation equation is $\dot{\mathbf{x}} = \mathbf{Ax} + \mathbf{Bu}$ where $\mathbf{x}$ = [UB, WB, THETA, QB]^T, $\mathbf{u}$ = [THRUST, ELEVATOR]^T, and

$$\mathbf{A} = \begin{bmatrix} -0.0377 & 0.1061 & -8.5649 & -32.1660 \\ -0.2785 & -0.7114 & 213.8900 & 0.4300 \\ -0.0002 & -0.0062 & -0.5235 & -0.0003 \\ 0 & 0 & 1.0000 & 0 \end{bmatrix}$$

$$\mathbf{B} = \begin{bmatrix} 0.3785 & 0.0065 \\ -0.0003 & -0.1621 \\ 0.0063 & -0.0212 \\ 0 & 0 \end{bmatrix}$$

The system is completely controllable. The goal of control is to keep the system at the trim condition *until* touchdown. The *control signal constraints* are: THRUST is between -7 and 13, ELEVATOR is between -15 and 15 degrees.

Whenever the real trajectory sways away from the nominal trajectory, the control system starts to pull the airplane back to the nominal trajectory. If it is in the middle of the mission, a slight deviation from the nominal trajectory will not do any harm. But after the airplane began the touchdown phase, it imposes very stringent constraints on its state.

The feedback matrix is

$$\mathbf{K} = \begin{bmatrix} -1.5644 & 3.1364 & -679.2176 & -197.0190 \\ -3.6333 & 3.2242 & -415.1189 & -212.5539 \end{bmatrix}$$

which makes the poles of the whole system: $2.2 \pm 2.2i$ and $0.14 \pm 0.14i$, and thus, the damping ratio of the system is 0.7.

3.2 Results

First, let's consider the situation where the deviation from the nominal trajectory starts at an altitude of 1000ft. Since we know that the vertical speed is 8.5686209ft/sec, the remaining mission time before touchdown is 116.7 seconds. We want to control the system so that when the aircraft approaches the end of the mission, the norm of the states is in the vicinity of zero (i.e., $\| \mathbf{x}(T) \| < \varepsilon$).

Simulation 1: We study the effect of the direction of terminal constraints. Let $\mathbf{x}(0) = [0, 10, 0, 0]^T$. First, consider the terminal constraint in terms of each state variable, i.e., $|x_i(T)| < \overline{x}_i(T)$, where x_i denotes the i-th element of $\mathbf{x}$. Figures 1 and 2 show the results when the terminal constraint (TC) $= \overline{x}_1 = \overline{x}_2 = \overline{x}_3 = 0.001$, $\overline{x}_4 = 0.002$, and TC $= \overline{x}_2 = \overline{x}_3 = \overline{x}_4 = 0.001$, $\overline{x}_1 = 0.002$, respectively. Comparing these two figures, we can find that the direction of terminal constraint has effects on the result. Figure 3 shows the result when the terminal constraint is $\| \overline{\mathbf{x}}(T) \| = 2.7 \times 10^{-4}$. The horizontal axis is t_f, and the vertical axis is the CSD.

Simulation 2: We study the effect of the direction of the initial condition. We would simply change the initial condition from $\mathbf{x}(0) = [0, 10, 0, 0]^T$ in the previous simulation to $\mathbf{x}(0) = [0, 0, 10, 0]^T$. The terminal constraint

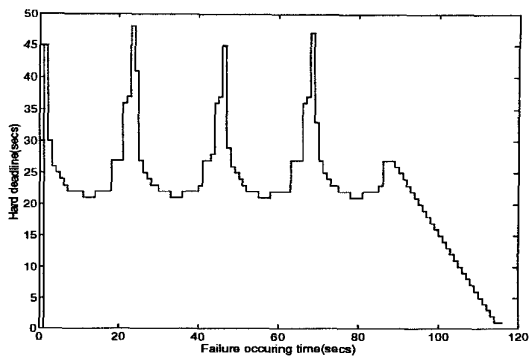

Figure 1: Initial condition: [0,10,0,0]; terminal constraints: [0.001, 0.001, 0.001, 0.002]

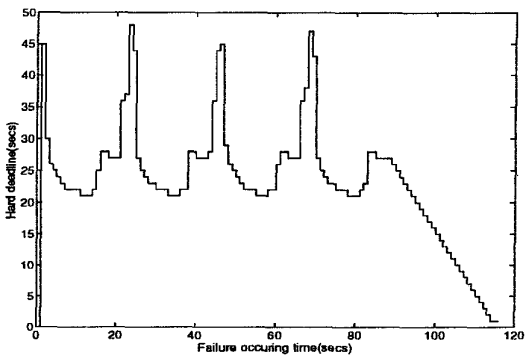

Figure 2: Initial condition: [0,10,0,0]; terminal constraints: [0.002, 0.001, 0.001, 0.001]

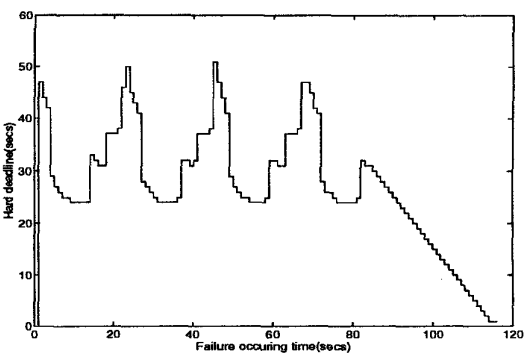

Figure 3: Initial condition: [0,10,0,0]; terminal constraints: $\| \overline{x}(T) \| = 2.7 \times 10^{-4}$; mission time: 116.7 seconds

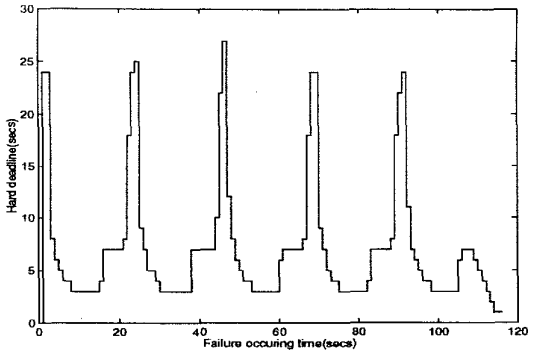

Figure 4: Initial condition: [0,0,10,0]; terminal constraints: $\| \overline{\mathbf{x}}(T) \| = 2.7 \times 10^{-4}$

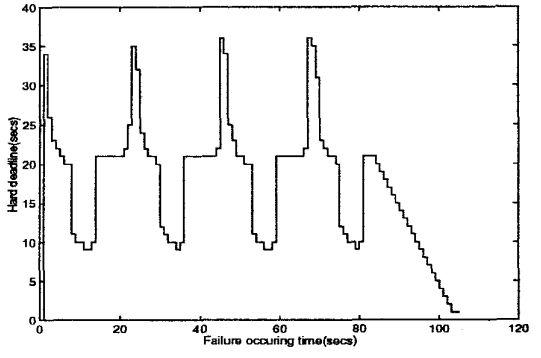

Figure 5: Mission time: 105 seconds

is in norm form. Figure 4 shows a much lower CSD as compared to Figure 3.

Simulation 3: We change the altitude from 1000ft to 900ft where the disturbance starts, i.e., changed the mission time from 116.7 seconds to 105 seconds. Figure 5 shows the relationship of the CSD versus the controller failure time when the mission time is 105 seconds. As expected, the CSD is much shorter compared to Figure 3.

Simulation 4: The last factor that will determine the CSD is the control law $\mathbf{K}$. Usually, the farther away the poles from the imaginary axis, the quicker the control response. But it is restricted by the control signal. Figure 6 shows the CSD when the poles of the system are moved from $0.14 \pm 0.14i$ to $0.2 \pm 0.2i$. As the control is more powerful in this case, the CSD can be much larger as compared to Figure 3.

3.3 Analysis

From the above simulation results, multivariable systems are found to be very complex. Even with the given initial condition, terminal constraint, mission time and control law, the CSD is not a monotonic function of t_f. What makes the analysis more complicated is that the initial condition itself is a random vector; so is the mission time because the disturbance can occur at any time with any magnitude and direction. We can use a random variable to capture the behavior of CSD. We

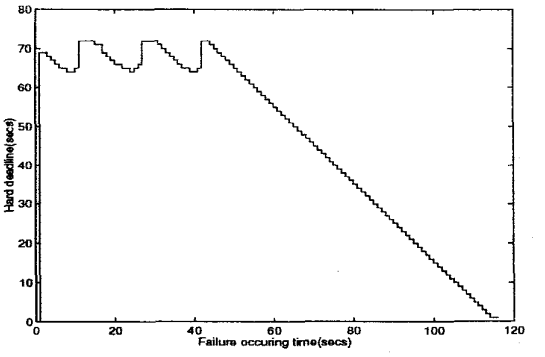

Figure 6: Changing control law

can also consider the initial condition and mission time as random variables whose distribution can be derived from field tests. Simulation can then be performed to derive the distribution of CSD corresponding to a fixed initial condition and mission time. The distribution can be described by the probability density function (pdf) or the moments (usually first and second, i.e., the expectation and the variance) of the random variable. The Chi-square test can be used to determine the fit of a distribution to the experimental and simulation data. We will see later that for some applications, only the mean and variance are required.

4 Reliability Analysis with CSD Knowledge

The CSD information can help us analyze the system reliability. Suppose we have n identical processors to run n copies of the same task and vote on these redundant results. If a majority of the processors produce correct results, then the system works correctly; otherwise, the system is in vulnerable state. Figure 7 shows our semi-Markov model for evaluating the system reliability.

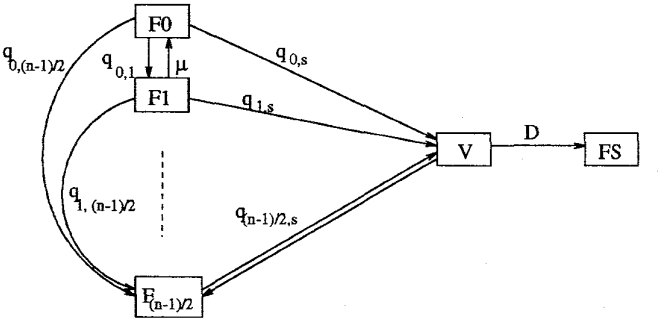

Figure 7: The NMR reliability model of a real-time control system

In this figure, F_i denotes the state that i processors produce erroneous results. V represents the *vulnerable* state when more than a half of the processors failed to produce correct results. Conventional reliability models do not include this vulnerable state. As soon as a majority of the processors fail, the whole system is considered to have failed. However, as we have seen in

the previous sections, this is not true for real-time control systems where "system inertia" protects the system from crashing immediately upon failure of a majority of processors. Incorporation of this inertia or CSD information into reliability analysis introduces a new state or vulnerable state.

FS is the state when the system actually crashed. Suppose the CSD is equal to D, and the sojourn time in state V is T. If $T > D$, the system moves from state V to state FS; otherwise, it moves from state V to safe state $F_{(n-1)/2}$.

The SURE package [13] is used in our reliability analysis. SURE is a reliability analysis tool for ultra-reliable systems. It uses a fast bounding theorem based on means and variances to compute the upper and lower bounds of system unreliability. Two types of transitions are identified in SURE. The first type is exponentially-distributed with a slow rate, which represents component failures. The second type is much faster but can have an arbitrary distribution. This type of transitions usually describes the recovery process. Since the transition from state "V" to state "FS" is much faster as compared to component failures (whether independent or correlated), it belongs to the second type. SURE requires that the recovery transitions be fast compared to the mission time and the inter-failure interval.

There are two ways to describe a fast transition, each based on a theorem. One theorem requires the information in terms of means and variances, and the other requires the information in terms of means and percentiles. So, when we derive the distribution from experimental data, we can just compute the required information instead of the exact distribution. The reasons for our choice SURE over other reliability modeling packages are that (1) the information it requires is easy to obtain; (2) it can handle complicated recovery mechanisms; (3) it does not depend on any particular modeling philosophy or structure.

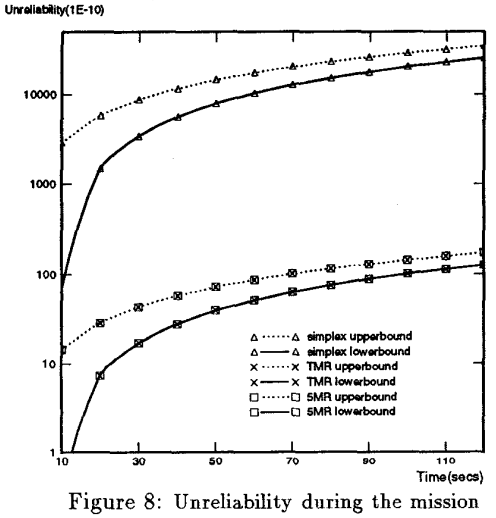

Figure 8: Unreliability during the mission

As an example, let's consider the B737 control system again. The mission time is 116.7 seconds for landing. Suppose the independent failure rate is 10^{-7}/second, the correlated failure rate is 10^{-9}/second. Suppose that when a common cause event occurs, there is an equal chance for a component to fail, or not to fail. The recovery rate is 0.5/second. From the simulation described in Section 3, we can obtain the mean and variance of CSD as 5 seconds, and 5 seconds^2, respectively.

The unreliability as a function of time is plotted in Figure 8. The Y axis is in logarithmic scale. From this figure, we can see that a simplex system is less reliable by more than 2 orders of magnitude than TMR and 5MR systems. On the other hand, there is almost no difference between TMR and 5MR for this example.

If we change the correlated failure rate to 10^{-6}, we get a different result as shown in Figure 9. In this example, a simplex system has a better lower bound than the redundant systems since the correlated failure rate is higher and the redundancy increases the possibility of more component failures in the system.

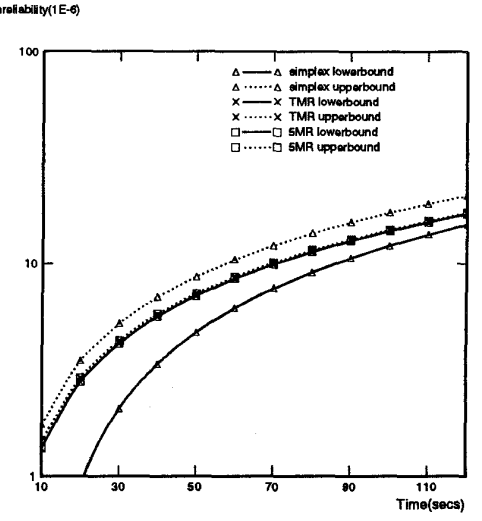

Figure 9: Unreliability during the mission with a different correlated failure rate

If we use the conventional reliability modeling technique without considering the effect of CSD, we would have gotten the TMR unreliability in Figure 10 (correlated failure rate=10^{-6}). We can see that our unreliability estimation is about one order of magnitude lower.

5 Conclusion

The main contribution of this paper is the treatment of CSD as a random variable and utilization of this information for more accurate modeling of system reliability.

Even when we treat the CSD as a random variable, we would like it to have a small variance around the mean. We tried to minimize the condition number of the system by applying an appropriate control law. Some work has been done on this subject. For example, Roppenecker [14] proposed a parametric expression for the controller gain matrix to make numerical analysis possible. Efforts have been made [15–17] to improve the performance of

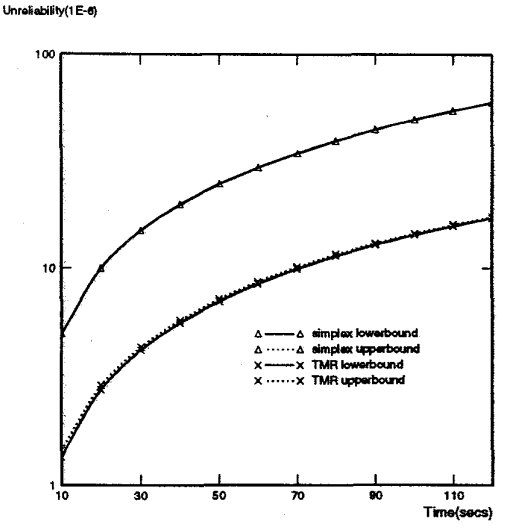

Figure 10: TMR unreliability during the mission

optimizing the feedback matrix gain and the condition number of a closed-loop system. But even with these methods, a highly-conditioned original system cannot have a low condition number through a constant matrix feedback. This is why a random variable has to be used to represent the CSD. For a system with a small condition number, the CSD would not depend on the initial condition very much. Thus, the field test for the distribution of initial condition is not needed.

In this paper, we did not address how to get the field data for the disturbance or how the engine control behaves when the computer controller fails. These are questions that are still under study. Shooman [18] surveyed EMI effects on airplanes. Since most of the data were derived from pilots' experiences, they were not very precise and most of the results were qualitative. Furthermore, no conclusion could be drawn on how the aircraft engines behave in the presence of an EMI. This needs to be studied further and is currently being explored at the NASA Langley Research Center.

Finally, we applied the CSD information to the evaluation of system reliability, showing significant improvements in accuracy.

Acknowledgement

The authors would like to thank Dick Hueschen and Celeste Belcastro of the NASA Langley Research Center for the information on the Boeing 737.

References

[1] A. S. Willsky, "A survey of design methods for failure detection in dynamic systems," *Automatica*, vol. 12, pp. 601–611, 1979.

[2] M. Mariton, "Detection delays, false alarm rates and the reconfiguration of control systems," *Int. J. Control*, vol. 49, no. 3, pp. 981–992, 1989.

[3] A. Emami-Naeini, M. M. Akhter, and S. M. Rock, "Effect of model uncertainty on failure detection: The threshold selector," *IEEE Trans. Automatic Control*, vol. 33, no. 12, pp. 1106–1115, December 1988.

[4] C.-C. Tsui, "A general failure detection, isolation and accommadation system with model uncertainty and measurement noise," *American Control Conference*, pp. 3123–3127, June 1993.

[5] T.-F. Hsieh and C.-A. Lin, "Stability conditions and controller design for systems with sensor and actuator failures," *American Control Conference*, pp. 3151–3152, 1993.

[6] T. E. Menke and P. S. Maybeck, "Sensor/actuator failure detection in the vista f-16 by multiple model adaptive estimation," *American Control Conference*, pp. 3135–3140, 1993.

[7] J. V. Medanic, "Design of reliable controllers using redundant control elements," *American Control Conference*, pp. 3130–3134, 93.

[8] P. R. Chandler, M. Pachter, and M. Mears, "Constrained linear regression for flight control system failure identification," *American Control Conference*, pp. 3141–3145, 1993.

[9] D. D. Siljak, "Reliable control using multiple control systems," *Int. J. Control*, vol. 31, no. 2, pp. 303–329, 1980.

[10] K. G. Shin, C. Krishna, and Y.-H. Lee, "A unified method for evaluating real-time computer controllers and its application," *IEEE Transactions on Automatic Control*, vol. 30, no. 4, pp. 357–366, April 1985.

[11] K. G. Shin and H. Kim, "Derivation and application of hard deadlines for real-time control systems," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 22, no. 6, pp. 1403–1413, November 1992.

[12] H. Kim and K. G. Shin, "On the maximum feedback delay in a linear/nonlinear control system with input disturbances caused by contrller-computer failures," *IEEE Transactions on Control System Technology*, vol. 2, no. 2, pp. 630–638, June 1994.

[13] R. W. Butler, "The SURE approach to reliability analysis," *IEEE Trans. Reliability*, vol. 41, no. 2, pp. 210–218, June 1992.

[14] G. Roppenecker, "On parametric state feedback design," *Int. J. Control*, vol. 43, no. 3, pp. 793–804, 1986.

[15] T. Owens and J. Marsh, "Some computational issues in optimal control by nonlinear programming," *Annals of Operations Research*, vol. 43, pp. 249–257, 1993.

[16] J. Kautsky, N. Nichols, and P. V. Dooren, "Robust pole assignment in linear state feedback," *Int. J. Control*, vol. 41, no. 5, pp. 1129–1155, 1985.

[17] R. Byers and S. G. Nash, "Approaches to robust pole assignment," *Int. J. Control*, vol. 49, no. 1, pp. 97–117, 1989.

[18] M. L. Shooman, "A study of occurrence rates of electromagnetic interference(EMI) to aircraft with a focus on hirf (external) high intensity radiated fields," Technical Report 194895, NASA, April 1994.