JOURNAL OF GUIDANCE, CONTROL, AND DYNAMICS
Vol. 18, No. 1, January–February 1995

Impact of Near-Coincident Faults on Digital Flight Control Systems

Cristian Constantinescu*
Duke University, Durham, North Carolina 27708-0291

The effects of near-coincident faults must be taken into account in designing highly reliable digital flight control systems. In this paper closed-form solutions for permanent and transient near-coincident fault factors are derived, based on the behavioral decomposition/aggregation technique and Markov version of the CARE III coverage model. Parameters of the model are assumed to be exponentially distributed. The influence of fault detection rate, fault detectability, error production and propagation rates, error detectability, and transient fault/error transition rate on the near-coincident fault factors is discussed. Eventually, a homogeneous, continuous-time Markov chain is used for describing a triple modular redundant (TMR) system. The near-coincident fault factors are employed for analyzing the effect of the interfering faults on reliability of the TMR computer. System reliability and near-coincident fault unreliability are plotted as functions of mission time, fault detectability, and weight of permanent and transient fault/errors. The impact of near-coincident faults can be curbed by increasing fault detectability. That impact is also lower when the percentage of transients is higher.

Nomenclature

A = active fault state
A_D = active detected fault/error state
A_E = active error state
B = benign fault/error state
B_E = benign error state
B_D = benign detected error state
C_γ = probability of successful reconfiguration
$\hat{c}$ = probability of covered permanent faults
c_{p_γ} = probability of successful reconfiguration for permanent faults/errors
c_{tp_γ} = probability of successful reconfiguration for transient treated as permanent faults/errors
c_γ = probability that reconfiguration from a covered permanent or transient treated as permanent fault/error is completed before near-coincident fault occurs
DP = detected as permanent state
F = failure state, due to single-point faults
d = fault detectability
h_p = weight of permanent faults/errors
h_t = weight of transient faults/errors
N = failure state, due to near-coincident faults
N_γ = probability of near-coincident failure
r_{p_γ} = probability of successful recovery for permanent faults/errors
n_{t_γ} = transient near-coincident fault factor
n_γ = near-coincident fault factor
P_A = probability that fault/error detected in active state is diagnosed as permanent
P_B = probability that fault/error detected in benign state is diagnosed as permanent
$P_C(\tau)$ = time-dependent probability of covered permanent faults
$P_R(\tau)$ = time-dependent probability of covered transient faults
$P_S(\tau)$ = time-dependent probability of single-point failures
$\hat{r}$ = probability of covered transient faults
q = error detectability
n_{p_γ} = permanent near-coincident fault factor
r_{t_γ} = probability of successful recovery for transient faults/errors
r_γ = probability that recovery from transient fault/error is successful before near-coincident fault occurs
S_γ = probability of single-point failure
$\hat{s}$ = probability of single-point failures
s_{p_γ} = probability of single-point failures due to permanent faults/errors
s_{t_γ} = probability of single-point failures due to transient faults/errors
s_γ = probability of single-point failure in presence of near-coincident faults
α = transition rate of transient faults/errors from active to benign
β = transition rate of intermittent faults/errors from benign to active
λ = failure rate of processor module
γ = rate of interfering faults
δ = fault detection rate
ϵ = error propagation rate
ρ = error production rate

I. Introduction

REDUNDANT processing modules are employed for providing the high reliability currently required for computer-based flight control systems. Several authors have demonstrated that reliability of redundant systems is extremely sensitive to a special parameter, the coverage probability, defined as the probability of successful recovery given a fault occurs.[1–3] It has been shown that coverage depends on fault/error-detection, isolation, and recovery mechanisms, thus being a very difficult parameter to predict. Ng and Avizienis,[3] Stiffler,[4] and Dugan,[2] among others, have devised different models for computing the coverage probabilities. An impeding problem in reliability analysis is that, when the coverage models are included in the overall system model, the resulting model becomes extremely large and numerically stiff. Several analytical, simulation, and decomposition/aggregation techniques have been proposed for coping with this issue.[1,5–8] In the case of highly reliable systems the designer also has to consider the effect of a second fault,[7] frequently named near-coincident fault.[1,9]

The behavioral decomposition/aggregation method is employed in this paper for coping with the largeness and stiffness of the reliability model.[8] This approximation technique considers two independent models. The first one is the fault/error-handling model (FEHM). The FEHM deals with the fault/error detection, isolation, and recovery processes, providing the coverage probabilities. It is also referred to as the coverage model. The second model, called the fault occurrence rapair model (FORM), captures information on the system structure and the fault arrival process. The FORM uses the coverage probabilities computed by solving the FEHM. The

Received Aug. 26, 1993; revision received April 27, 1994; accepted for publication April 28, 1994.

*Research Associate, Electrical Engineering Department.

FEHM and FORM can be independently solved because fault/error detection and recovery times are in the range of seconds and fault occurrence times are in the range of thousands of hours.

For assessing the effect of near-coincident faults on flight control computers, we use the Markov version of the CARE III coverage model.[1,10] Closed-form solutions for near-coincident fault factors are derived in the case of permanent and transient faults. Those factors provide valuable information about the impact of near-coincident faults on the analyzed system, taking into account the parameters of the coverage model.

Several fault-tolerant machines have been developed for flight control applications, e.g., the software-implemented fault-tolerant computer (SIFT),[11] the fault-tolerant multiprocessor (FTMP),[12] the fault-tolerant processor (FTP),[13] the matrix voter based architecture (MVA),[14] and the brick wall redundancy (BWR).[15] These systems are based on the N modular redundant (NMR) concept; i.e., for N redundant modules, $N \geq 2f + 1$, the system is able to operate as long as the number of failed modules is less than or equal to f. NMR systems also employ majority voting for detecting the failed modules. The MVA, for instance, consists of several processor/local memory and system memory/input/output (I/O) interface modules that are interconnected through a matrix of buses and bus interface units. The voting operation is performed at the bus interface level. The BWR architecture represents an enhancement of the triple modular redundant (TMR) scheme. Each module of the triplex system consists of two independent processing units that compare their outputs. If a difference occurs, the whole module is shut down, before performing the majority voting. Both MVA and BWR systems have been designed to tolerate two faults and to shut down safely after the third one.

In this paper we discuss the effect of near-coincident faults on a simple TMR system. The rationale of this choice is twofold: first, the analysis is greatly simplified (e.g., the MVA Markov model requires thousands of states) and, second, the NMR structure (and its particular case, TMR) still represents an elementary building block for many modern flight control systems.

The paper is organized as follows: Section II provides closed-form solutions of the near-coincident fault factors. Influence of the parameters of the coverage model on the near-coincident fault factors is discussed in Sec. III. In Sec. IV the impact of interfering faults on a TMR computer is evaluated, taking into account the weight of permanent and transient faults/errors. Section V concludes this work.

II. Near-Coincident Fault Factors

The Markov version of the CARE III model for the particular case of exponentially distributed random variables is considered for analyzing the effect of near-coincident faults on a redundant computing system.[6] Figure 1 shows the state transition diagram of the model for permanent, transient, and intermittent faults. The model has one entry state, A, and three output states, B, DP, and F. State A is entered when a fault occurs or a benign intermittent fault becomes active. In that state the fault is both detectable and able to induce an error. State B is reached in the case of benign faults and faults/errors detected as transient. State B is an output state for transients only. Faults/errors detected as permanent lead to the DP state. A faulty module of the system is removed from service with probability P_A or P_B in the case of detected active or benign faults/errors, respectively. After detection the module can be returned to service with the complementary probability $1 - P_A$ or $1 - P_B$, as the dashed lines in Fig. 1 show. The single-point failure state F is entered if an error goes undetected. Details about the CARE III coverage model are available in the literature.[1,10]

In this paper it is assumed that faults/errors detected in the active state are permanent ($P_A = 1$), those detected in the benign state are transient ($P_B = 0$), and there are no intermittent faults/errors ($\beta = 0$). We also take into account that both A_D and B_D are zero holding time states. The fault detection capabilities of the self-test procedures are considered, according to the HARP implementation of the CARE III model.[1] Practically, this means that fault detection rate δ is multiplied by d. A fourth exit, N, is added to the coverage model. That exit is reached when the fault/error handling process is interrupted by an interfering event. The resulting coverage model is shown in Fig. 2.

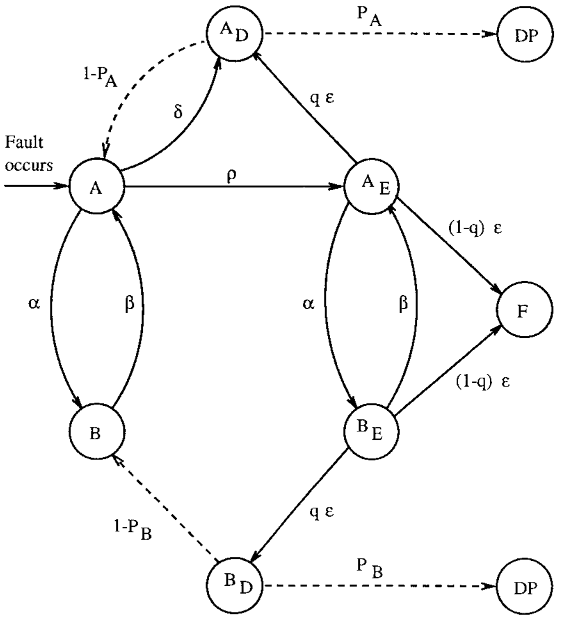

Fig. 1 CARE III coverage model.

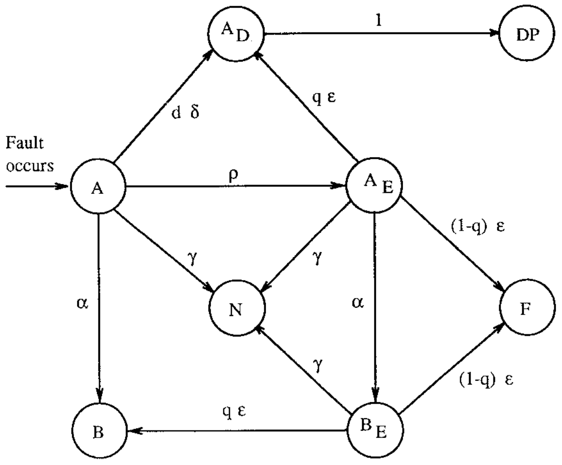

Fig. 2 Coverage model for permanent, transient, and near-coincident faults.

Let us consider that time between occurrences of the interfering faults is a random variable X with parameter γ characterized by the distribution

$$F_X = 1 - e^{-\gamma t}$$

The $\hat{c}$, $\hat{r}$, $\hat{s}$ probabilities are defined as[1]

$$\hat{c} = \lim_{\tau \to \infty} P_C(\tau)$$

$$\hat{r} = \lim_{\tau \to \infty} P_R(\tau)$$

$$\hat{s} = \lim_{\tau \to \infty} P_S(\tau)$$

Intuitively, $\hat{c}$, $\hat{r}$, and $\hat{s}$ represent the steady-state probabilities of covering permanent faults/errors, successfully restoring after transient faults/errors and failing due to undetected single-point faults/errors, respectively.

The c_γ, r_γ, and s_γ probabilities are defined for assessing the impact of a second fault, which occurs while the fault/error handling process is undergoing:

$$c_\gamma = \text{Prob[time to reconfigure system after permanent fault} < X]$$
$$= \int_0^\infty e^{-\gamma t}\, \mathrm{d}P_C(t) \qquad (1)$$

$$r_\gamma = \text{Prob[time to restore system after transient fault} < X]$$
$$= \int_0^\infty e^{-\gamma t}\, \mathrm{d}P_R(t) \qquad (2)$$

$$s_\gamma = \text{Prob[time to failure due to uncovered fault/error} < X]$$
$$= \int_0^\infty e^{-\gamma t}\, \mathrm{d}P_S(t) \qquad (3)$$

The near-coincident fault factor, which is the probability of reaching state N, is defined as

$$n_\gamma = 1 - (c_\gamma + r_\gamma + s_\gamma) \qquad (4)$$

The HARP tool employs extended stochastic Petri nets (ESPN) to solve the FEHM. For coping with stiffness of the FEHM (e.g., α can be three orders of magnitude higher than ρ), the coverage model is solved by simulation. Different distributions can be also associated with the timed transitions of the ESPN model. Expressions (1–3) are computed by means of Laplace-Stieltjes transforms and Taylor series expansions.[1]

Alternatively, we derive closed-form solutions for two near-coincident fault factors, independently solving the CARE III coverage model for permanent and transient faults/errors. We also take into account that expressions (1–3) are the Stieltjes integrals of $e^{-\gamma t}$ and the $P_C(t)$, $P_R(t)$, and $P_S(t)$ functions, respectively. The Stieltjes integrals are analytically computed for providing the reconfiguration, recovery, and failure probabilities.

In the case of permanent faults/errors ($\alpha = 0$) a reduced coverage model is obtained. It consists of states A, A_E, A_D, and F only. The probabilities of successful reconfiguration and single-point failure are derived by solving the reduced model for $P_C(t)$ and $P_S(t)$ and integrating by parts (1) and (3), respectively:

$$c_{p_\gamma} = \frac{\epsilon\rho q + \delta d(\epsilon + \gamma)}{(\gamma + \rho + \delta d)(\epsilon + \gamma)} \qquad (5)$$

$$s_{p_\gamma} = \frac{\epsilon\rho(1 - q)}{(\gamma + \rho + \delta d)(\epsilon + \gamma)} \qquad (6)$$

Taking into account that $r_{p_\gamma} = 0$, Eq. (4) becomes

$$n_{p_\gamma} = 1 - (c_{p_\gamma} + s_{p_\gamma}) \qquad (7)$$

The near-coincident fault factor for permanent faults/errors is derived by substituting Eqs. (5) and (6) into Eq. (7):

$$n_{p_\gamma} = \frac{\gamma(\epsilon + \gamma + \rho)}{(\gamma + \rho + \delta d)(\epsilon + \gamma)} \qquad (8)$$

In the case of transients $\alpha \neq 0$. The probability of successful reconfiguration for transients treated as permanent faults/errors is obtained by solving the CARE III model for $P_C(t)$ and integrating Eq. (1):

$$c_{tp_\gamma} = \frac{\epsilon\rho q + \delta d(\alpha + \epsilon + \gamma)}{(\alpha + \gamma + \rho + \delta d)(\alpha + \epsilon + \gamma)} \qquad (9)$$

The recovery probability after a transient fault/error is derived by substituting $P_R(t)$ and integrating Eq. (2):

$$r_{t_\gamma} = \frac{\alpha\epsilon\rho q + \alpha(\alpha + \epsilon + \gamma)(\epsilon + \gamma)}{(\alpha + \gamma + \rho + \delta d)(\alpha + \epsilon + \gamma)(\epsilon + \gamma)} \qquad (10)$$

Similarly, the probability of single-point failures due to transients is obtained by substituting $P_S(t)$ and integrating Eq. (3):

$$s_{t_\gamma} = \frac{\epsilon\rho(1 - q)}{(\alpha + \gamma + \rho + \delta d)(\epsilon + \gamma)} \qquad (11)$$

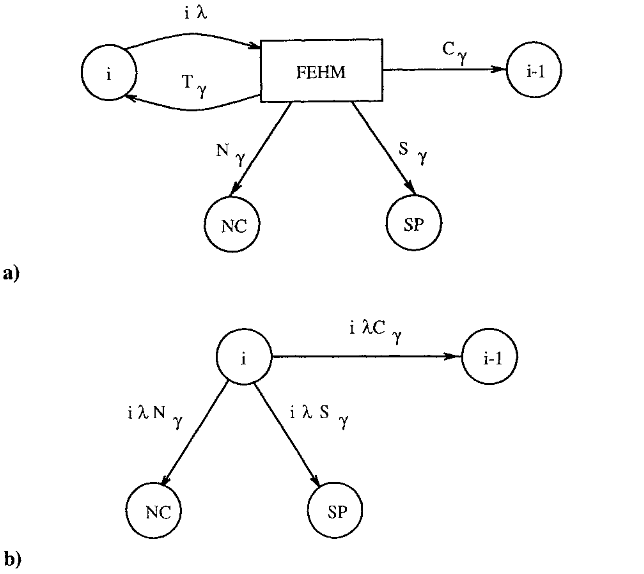

Fig. 3 a) incorporation of FEHM into FORM and b) equivalent Markov model.

Equation (4) is rewritten as

$$n_{t_\gamma} = 1 - \left(c_{tp_\gamma} + r_{t_\gamma} + s_{t_\gamma}\right) \qquad (12)$$

The closed-form solution of the near-coincident fault factor for transients is obtained by substituting Eqs. (9–11) into Eq. (12):

$$n_{t_\gamma} = \frac{\alpha\gamma\rho + \gamma(\alpha + \epsilon + \gamma + \rho)(\epsilon + \gamma)}{(\alpha + \gamma + \rho + \delta d)(\alpha + \epsilon + \gamma)(\epsilon + \gamma)} \qquad (13)$$

The probabilities of successful reconfiguration, single-point failure, and near-coincident failure, taking into account both the permanent and transient faults/errors, are

$$C_\gamma = h_p c_{p_\gamma} + h_t c_{tp_\gamma} \qquad (14)$$

$$S_\gamma = h_p s_{p_\gamma} + h_t s_{t_\gamma} \qquad (15)$$

$$N_\gamma = h_p n_{p_\gamma} + h_t n_{t_\gamma} \qquad (16)$$

The weights of the permanent and transient fault classes are defined as

$$h_p = \text{Prob[fault is permanent/fault occurs]}$$

$$h_t = \text{Prob[fault is transient/fault occurs]}$$

$$h_p + h_t = 1$$

Finally, Fig. 3a shows how the FEHM is incorporated into the FORM. The general case of i independent modules is considered. The failure of one module while the system is in state i leads to the entry state of the FEHM with rate $i\lambda$. If the fault is transient, the system returns to state i with probability T_γ, where $T_\gamma = 1 - (C_\gamma + S_\gamma + N_\gamma)$. The permanent and transient treated as permanent faults bring the system into the $i - 1$ state with probability C_γ. Transitions to the single-point and near-coincident failure states occur with probabilities S_γ and N_γ, respectively. Figure 3b depicts the equivalent Markov model.

III. Influence of Coverage Model Parameters on Near-Coincident Fault Factors

The direction and magnitude of the effect of varying the α-q parameters of the CARE III coverage model on the near-coincident fault factors are discussed in this section. Inspecting Eqs. (8) and (13) we notice that neither n_{p_γ} nor n_{t_γ} are functions of error detectability. Intuitively, this is explained as follows: The system is operational after an error has occurred with probability q. It reaches the failure

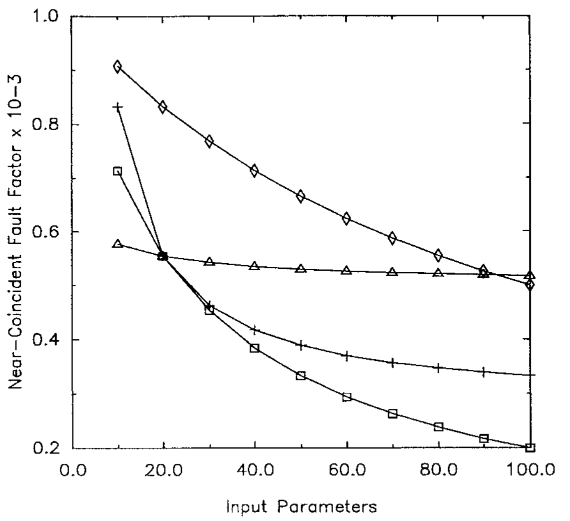

Fig. 4 Influence of coverage model parameters on n_{p_γ} ($\gamma = 0.01\,\mathrm{h}^{-1}$, $d = 0.1$–1.0): □, $n_{p_\gamma} = f(\delta)$; △, $n_{p_\gamma} = f(\rho)$; +, $n_{p_\gamma} = f(\epsilon)$; ◇, $n_{p_\gamma} = f(d)$.

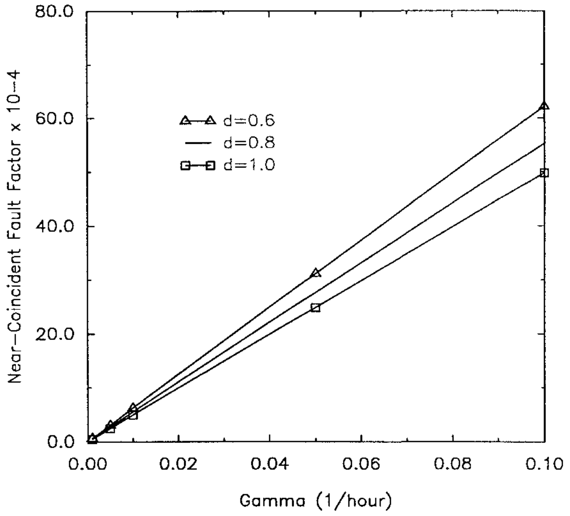

Fig. 5 Influence of γ on n_{p_γ} ($\delta = \epsilon = \rho = 20$).

state with probability $1 - q$. In the first case the interfering fault is handled as a new event, and in the second situation the fault has no effect because the system has already failed.

In the case of permanent faults/errors Fig. 4 shows that lower values for the n_{p_γ} factor are obtained by increasing d, δ, and ϵ. The δ and ϵ parameters have more effect at lower transition rates. The parameter ρ has negligible impact on n_{p_γ}.

Figure 5 provides information about the effect of γ on n_{p_γ} for three different fault detectability probabilities. Higher γ rates increase the near-coincident fault factor. The term n_{p_γ} can be reduced by increasing fault detectability. However, the near-coincident fault factor takes nonzero values even if d approaches 1.0, i.e., fault detectability is perfect.

In the case of transient faults/errors α, ρ, and ϵ have the strongest influence on n_{t_γ}, as is shown in Fig. 6. Higher α and ϵ values reduce the n_{t_γ} factor. The effect of these parameters is considerably higher for low transition rates. By contrast, the increase of ρ provides higher n_{t_γ} values over the range considered. The parameters δ and d slightly affect n_{t_γ}.

The effect of γ and d on the n_{t_γ} factor is depicted in Fig. 7. These parameters have a less significant influence, as compared to the case of permanent faults.

Eventually, it should be noted that fault detectability is the only parameter that can be practically modified during the design process for the purpose of blurring the effect of near-coincident faults. Henceforth we discuss the role of d for different weights of the permanent and transient faults/errors.

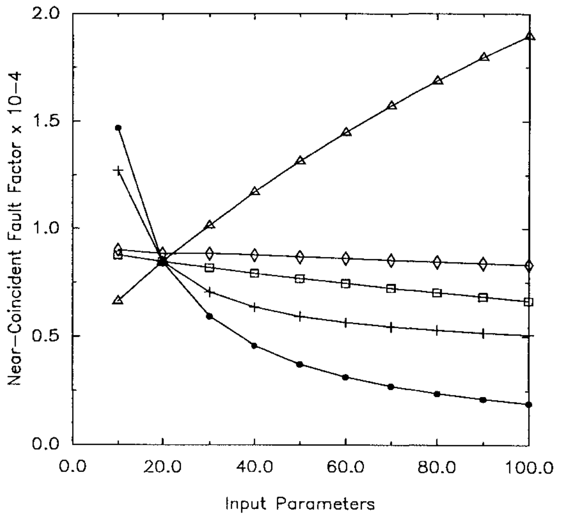

Fig. 6 Influence of coverage model parameters on n_{t_γ} ($\gamma = 0.01\,\mathrm{h}^{-1}$, $\alpha = 100$–1000, $d = 0.1$–1.0): ●, $n_{t_\gamma} = f(\alpha)$; □, $n_{t_\gamma} = f(\delta)$; △, $n_{t_\gamma} = f(\rho)$; +, $n_{t_\gamma} = f(\epsilon)$; ◇, $n_{t_\gamma} = f(d)$.

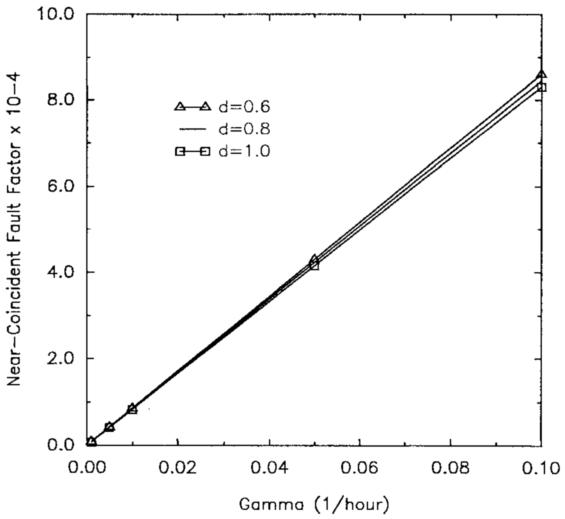

Fig. 7 Influence of γ on n_{t_γ} ($\alpha = 200$, $\delta = \epsilon = \rho = 20$).

IV. Effect of Near-Coincident Faults on Reliability of TMR Computer

A homogeneous, continuous-time Markov chain (CTMC) is employed for describing the behavior of a TMR system in the presence of interfering faults. For the sake of simplicity the model accounts for processor failures only. It can be extended, however, for taking into consideration the failures of the interprocessor communication and voting mechanisms.

The state transition diagram of the CTMC is shown in Fig. 8. The initial state of the model is labeled 3; i.e., three processing modules are operational when the system resides in that state. The other two operational states, labeled 2 and 1, correspond to the two and one operational modules, respectively. Two absorbing states, SP and NC, are also considered. The TMR system reaches the SP state in the case of single-point failures. Failures due to near-coincident faults bring the system into the NC state.

The CTMC transition rates are computed with the aid of Eqs. (14–16). For assessing the effect of near-coincident faults we need to know the rate at which the interfering events occur. In this work we assume that a second fault, which occurs in an operational module while the system is handling the first fault, results in entering the NC failure state. This assumption calls for using different γ rates in order to derive the transition rates associated with the outgoing arcs of the states labeled 3 and 2. When the system is in state 3, $\gamma = 2\lambda$, i.e., occurrence of a second fault in any of the two operational modules

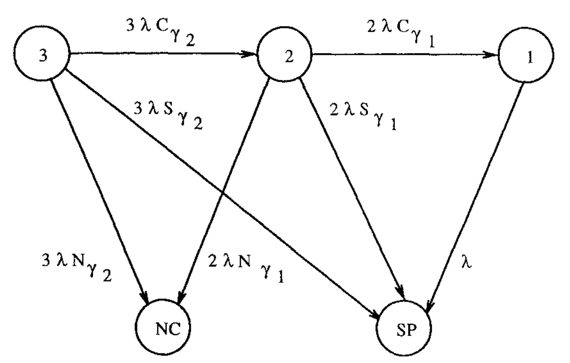

Fig. 8 Markov model of TMR system.

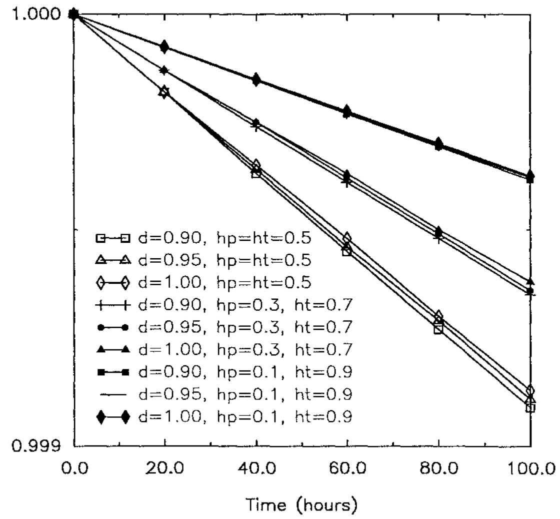

Fig. 9 System reliability as function of mission time, fault detectability, and weight of permanent and transient faults/errors ($\lambda = 0.0001$ h^{-1}, $\alpha = 200, \delta = \epsilon = \rho = 20, q = 0.9$).

while the TMR system handles the first fault, leads to a catastrophic failure. Similarly, $\gamma = \lambda$, in state 2, i.e., occurrence of a near-coincident fault in the only operational module during the processing of the previous fault brings the system into the NC failure state. The second subscript, associated with the C_γ, S_γ, and N_γ probabilities in Fig. 8, shows which γ rate is employed. For instance, C_{γ_2} is derived assuming $\gamma = 2\lambda$, and N_{γ_1} is computed for $\gamma = \lambda$.

More generally, if the model accounts for different constituent modules of the system, e.g., processors, memories, and buses, optimistic and conservative assumptions can be considered. Optimistically, it can be assumed that only interfering faults of the same module type bring the system into the failure state. For instance, when a memory fault/error is processed, a bus fault is not catastrophic. Conservatively, the system does fail due to a near-coincident fault in any module. For example, a processor fault/error is fatal if it occurs when an I/O fault is processed. The modeler also has a third choice: to explicitly account for the interaction among different modules during the fault/error handling process. Though this approach is tedious and requires a thorough knowledge of the system, it provides more accurate information about the influence of the near-coincident faults.

Reliability of the TMR system vs mission time for several fault detectability probabilities and weights of the permanent and transient faults/errors is shown in Fig. 9. As expected, higher values of d and h_t increase reliability. High fault detectability aids the TMR system to successfully reconfigure its structure. The high weight of the transients allows for system recovery with no degradation of the redundancy level.

Figure 10 answers the following questions:

1) How is near-coincident fault unreliability affected by fault detectability and the weight of permanent and transient faults/errors?

2) How much of the TMR system unreliability is due to near-coincident faults?

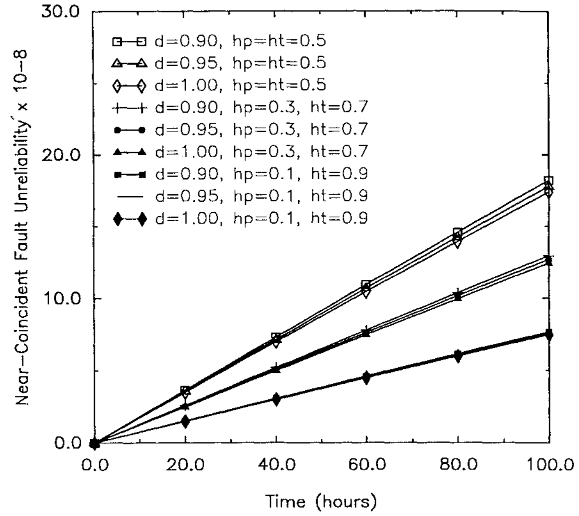

Fig. 10 System unreliability, due to near-coincident faults as function of mission time, fault detectability and weight of permanent and transient faults/errors ($\lambda = 0.0001$ h^{-1}, $\alpha = 200, \delta = \epsilon = \rho = 20, q = 0.9$).

Near-coincident fault unreliability is lower when d and/or h_t take higher values. High fault detectability allows the TMR system to successfully reconfigure before a second fault occurs. A high percentage of transient faults/errors also contributes to a low near-coincident fault unreliability. Usually, the active-to-benign transition rate for transients is at least 10 times higher than all other detection and propagation rates of the CARE III model. This allows for fast system recovery before the second fault occurs. It should be also stressed that, as the weight of transients is lower, the effect of fault detectability on near-coincident fault unreliability is more significant.

Finally, it is noticeable that the largest contribution of the near-coincident faults to the system unreliability is 18.2×10^{-8} for a 100-hour mission time, $d = 0.9$, and $h_p = h_t = 0.5$. Near-coincident unreliability is curbed to 7.5×10^{-8} for $d = 1.0$, $h_p = 0.1$, and $h_t = 0.9$.

V. Conclusions

In this paper a new approach is proposed for assessing the impact of near-coincident faults on the reliability of redundant flight control computers. The closed-form expressions of the near-coincident fault factors avoid stiffness of the coverage model and allow for fast parametric sensitivity analysis, providing valuable information about the effectiveness of different diagnostic and reconfiguration mechanisms. Closed-form solutions also are useful tools for verifying more general, numerical methods.

Reliability of a TMR system is analyzed as an application example. The contribution of near-coincident faults to the system unreliability is higher when the percentage of permanent faults is higher. That impact can be curbed by increasing fault detectability. The presented results also aid in understanding the fault/error handling process in the presence of interfering faults. However, it should be noted that assuming an exponential distribution for parameters of the coverage model represents the main limitation of this approach.

Acknowledgments

The comments and suggestions from the referees and the editor were very helpful in revision of the paper.

References

[1] Dugan, J. B., et al., "The Hybrid Automated Reliability Predictor," *Journal of Guidance, Control, and Dynamics*, Vol. 9, 1986, pp. 319–331.

[2] Dugan, J. B., and Trivedi, K. S., "Coverage Modeling for Dependability Analysis of Fault-Tolerant Systems," *IEEE Transactions on Computers*, Vol. 38, No. 6, 1989, pp. 775–787.

[3] Ng, Y., and Avizienis, A., "A Model for Transient and Permanent Fault Recovery in Closed Fault-Tolerant Systems," *Proceedings of the Sixth*

International Symposium on Fault-Tolerant Computing, 1976, pp. 182–187.

[4]Stiffler, J. J., "Computer Aided Reliability Estimation," *Proceedings of the AIAA/NASA/IEEE/ACM Computers in Aerospace Conference*, 1977, pp. 427–434.

[5]Boyd, M. A., and Bavuso, S. J., "Modeling a High Reliable Fault-Tolerant Guidance, Navigation and Control System for Long Duration Manned Spacecraft," *Proceedings of the IEEE/AIAA Digital Avionics Systems Conference*, 1992, pp. 464–469.

[6]Constantinescu, C., "Predicting Performability of a Fault-Tolerant Microcomputer for Process Control," *IEEE Transactions on Reliability*, Vol. 41, No. 4, 1992, pp. 558–564.

[7]McGough, J., Reibman, A., and Trivedi, K., "Markov Reliability Models for Digital Flight Control Systems," *Journal of Guidance, Control, and Dynamics*, Vol. 12, No. 2, 1989, pp. 209–219.

[8]Trivedi, K. S., and Geist, R. M., "Decomposition in Reliability Analysis of Fault-Tolerant Systems," *IEEE Transactions on Reliability*, Vol. R-32, 1983, pp. 463–468.

[9]McGough, J., "Effects of Near-Coincident Faults in Multiprocessor Systems," *Proceedings of the Fifth IEEE/AIAA Digital Avionics Systems Conference*, 1983, pp. 16.6.1–16.6.7.

[10]Rose, D. M., and Altschul, R. E., "Review and Verification of CARE III Mathematical Model and Code," NASA Contractor Rept. 166096, April 1983.

[11]Wensley, J. H., et al., "SIFT: Design and Analysis of a Fault-Tolerant Computer for Aircraft Control," *Proceedings of the IEEE*, Vol. 66, 1978, pp. 1240–1255.

[12]Hopkins, A. L., Smith, T. B., and Lala, J. H., "FTMP—A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft," *Proceedings of the IEEE*, Vol. 66, 1978, pp. 1221–1239.

[13]Lala, H. J., et al., "A Fault-Tolerant Processor to Meet Rigorous Failure Requirements," *Proceedings of the Seventh Annual Digital Avionics System Conference*, 1986, pp. 555–562.

[14]Somani, A. K., and Sarnaik, T. R., "Reliability Analysis Techniques for Complex Multiple Fault-Tolerant Computer Architectures," *IEEE Transactions on Reliability*, Vol. 39, No. 5, 1990, pp. 547–556.

[15]Eagle, K. H., and Agarwala, A. S., "Redundancy Design Philosophy for Catastrophic Loss Protection," *Proceedings of the Annual Reliability and Maintainability Symposium*, 1992, pp. 1–6.