602436

Reliability of Fault Tolerant Control Systems: Part II[1]

N. Eva Wu

Department of Electrical Engineering, Binghamton University
Binghamton, NY 13902-6000, U.S.A.
Tel: 607-777-4375, Fax: 607-777-4464, Email:evawu@binghamton.edu

Abstract

This paper reports Part II of a two part effort that is intended to delineate the relationship between reliability and fault tolerant control in a quantitative manner. Reliability properties peculiar to fault-tolerant control systems are emphasized, such as the presence of analytic redundancy in high proportion, the dependence of failures on control performance, and high risks associated with decisions in redundancy management due to multiple sources of uncertainties and sometimes large processing requirements. As a consequence, coverage of failures through redundancy management can be severely limited. The paper proposes to formulate the fault tolerant control problem as an optimization problem that maximizes coverage of failures through redundancy management. Coverage modeling is attempted in a way that captures its dependence on the control performance and on the diagnostic resolution. Under the proposed redudnacy management policy, it is shown that an enhanced overall system reliability can be achieved with a control law of a superior robustness, with an estimator of a higher resolution, and with a control performance requirement of a lesser stringency.

1 Introduction

Highly reliable systems make use of redundancy to achieve fault tolerance, due to limited reliability of components or subsystems[8]. Utilization of analytic redundancy[9] that provided by static and dynamic relations among system variables, such as secondary functions of effectors, virtual measurements, projections, etc. can further reduce the probability of exhaustion of hardware in a cost-effective manner. Analytic redundancy management of complex control systems, however, involves considerable more risks in comparison with such schemes as majority voting, for decision making is often based on residual signals formed by the differences between noisy measurements and calculated values of output variables based on inaccurate models. Decision errors can be associated with uncertainties on whether there is a subsystem failure, which subsystem has failed, how severe is its effect, whether it is necessary to take a drastic corrective action, which action to take. In addition, the question may also arise on whether there is adequate control relevant redundancy[22] and authority to allow recovery from the effect of the failure. The dynamic and closed-loop nature, common to all control systems, is the source for additional difficulties, such as temporary mask of the effect of subsystem failures, the vagueness in the definition of a system level failure in the context of control performance, and the sometimes significant processing requirement in supporting the redundancy management.

There are many applications in which fault tolerance may be achieved by using one of the adaptive control[6, 1], or reliable control[18], or reconfigurable control[3] strategies. As the the control action becomes progressively more drastic, the lielihood of involving an explicit diagnostic process becomes higher, and decision making becomes riskier. Fault tolerant control in general is a subject too broad to be discussed in this paper. Instead, the discussion here will be confined to its relation to reliability and our inquiry on the control strategy will be kept at the conceptual level. The reader is referred to [17, 4, 5, 16] and references therein for a more complete view of the state of the art, issues, and methodologies in the field of fault tolerant control.

Definitions suggested in [14] on fault and failure are adopted with a slight modification. A fault is an unpermitted deviation of at least one characteristic property or variable of the system. A failure is a permanent interruption of a system's ability to perform a required function under specified operating conditions. Note that a failure can also be defined in the subsystem level. A fault may or may not lead to a failure. With-

[1]This work was supported in part by the NASA under Cooperative Agreement # NCC-1-336, in part by the NSF under Grant # ECS-9615956, and in part by the Xerox Corporation under Grant #IIE 1321-98. The author would also like to thank Prof. Y.-C. Ho of Harvard University for his suggestion on defining coverage of failures in fault tolerant control systems alternatively under the probabilistic formalization (rather than under the possibilistic formalization[19]), which allows the synergy with, and the direct utilization of the classical reliability theory and analysis tools.

out loss of generality, a subsystem failure is assumed to always lead to the system failure unless a successful management of redundancy ensues. Since this paper is concerned with closed-loop control systems to which occurrence of a failure depends on whether there is a loss of control performance, a properly defined control performance threshold will be introduced in the paper to quantify the acceptable system performance level. The threshold must encompass requirements in stability, and in transient as well as steady state control performance. It is assumed that no event or events would trigger a sequence of infinite reconfiguration actions in which case the stability problem of a different nature must be considered[7]. A system level failure is declared when faults or subsystem failures cause the control performance of the system to fall below the prescribed threshold. The performance threshold can be set at two (or more) different levels, each corresponding to a specific reliability requirement. In aviation, for example, one level can be set by the ability to carry out a normal mission (or mission abort in terms of failure probability), and another can be set by the ability to merely maintain the system stability needed for safe landing (loss of control in terms of failure probability). This paper will treat different reliability requirements in a unified manner.

Reliability is naturally a subjective concern in the analysis and design of fault-tolerant control systems. Reliability is rarely regarded as an objective criterion that guides a control system design in an integrated manner. This predicment is due to the difficulty in establishing a functional linkage between the over all system reliability, and the performance defined in the conventional sense at the bottom level for controls and for diagnosis. The paper is organized as follows. Section 2 models coverage in fault tolerant control systems, and delineates two important roles coverage plays one as a criterion for off-line integrated fault tolerant control system design and one as a criterion for on-line minimum-risk redundancy management. Finally, a functional linkage between reliability and control/diagnosis performance is established. Section 3 summarizes the findings of the paper.

2 Coverage in Fault Tolerant Control

This section focuses on coverage modeling and evaluation, through which reliability will be tied to the design and operation of fault tolerant control systems. The previous section emphasizes statistical analysis based on failure data, and attempts to infer from the sample of failure data to some representative behavior of the general population. It is possible in that case to assume a range of coverage values in assessing a system's reliability and determine what is the set of minimum coverage values required for a given overall system reliability requirement. The reliability issues are viewed from a different perspective in this section. The concern now is with how to achieve the set of required coverage values through proper designs of control and diagnostic modules. Some of the basic ideas presented in this section follow those presented in [19] where a possibilistic formalization is used. It is the first time rigorous arguments are given under a clearly defined redundancy manegement policy using a probabilistic formalization to confirm our intuitions on how control and diagnosis performance affect overall system reliability.

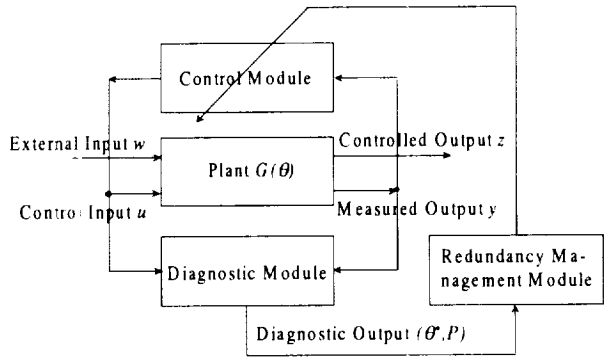

Fig.1 Schematic of fault tolerant control system

Since the design of both feedback control and diagnostic algorithm depends on the model of the plant to be controlled, the task of modeling of individual physical processes for which specific reliability goals are to be implemented must be first tackled. A model suitable for the fault tolerant control purpose should reflect the effects of failures and availability of redundancy. Suppose all such conditions enter the plant model in the form of parameters. The effort of fault parameterization in linear parameter varying (LPV) form[21], for example, is on going. A fault effect parameter space can then be defined as the Euclidean space of all parameters that change their values as the result of some fault occurrence. The prescribed range of variation of such parameters form a set in the parameter space. Let θ denote a vector in the space of dimension N, and Ω denote the set over which θ resides when fault occurs. Without loss of generality, Ω can be regarded as a hyper-rectangle

$$\Omega = \{\theta_{l,min} \leq \theta_l \leq \theta_{l,max},\ l = 1,\ ...,\ N\},$$

with $\theta = 0$ denoting the no-fault parameter vector.

Next, control performance will be defined over the fault effect domain. In the schematic diagram shown in Fig.1, $G(\theta)$ represents a model for the input to output mapping of the plant, including models of actuators and the sensors. The argument θ is made explicit to indicate that the model is dependent on the fault ef-

fect parameter vector. Vector w contains all external signals, including disturbances, sensor noises and reference signals. Controlled output z is an error vector, capturing the design specifications for the system; y is the vector of measured variables; u is the vector of control inputs. $1/\mu$[2] has been suggested and discussed as a measure of control perofrmance in [19], and the computability of this measure as a function of two control effectiveness factors, has been demonstrated[20].

Let J_{min} denote a prescribed control performance threshold to distinguish the normal from a failed operation for the controlled system, i.e., a failure is declared if

$$J_{U_i}(\theta) < J_{min}, \tag{1}$$

where subscript U_i denotes a particular control setting. Whenever (1) becomes the case, a control reconfiguration is becomes necessary. The essence of fault tolerant control lies with the management of the control relevant redundancy. Depending on the severity of anomaly, management of control relevant redundancy can be carried out via a control law robustification, or adaptation, or reconfiguration. As the control action becomes progressively more drastic, the likelihood of involving an explicit diagnostic process becomes higher, and decision making becomes riskier. Since successful redundancy management depends on the knowledge of fault effect parameter θ, the challenge facing us is to acquire, to represent, and to utilize the knowledge in the presence of uncertainties. Fault tolerance can be achieved only if sufficient redundant control authority exists in the system. The issue regarding the adequacy of control relevant redundancy is elaborated in [22]. The discussion on constraints that must be imposed when the set $\{U_i\}_{i=1}^{M}$ is constructed can be found in [19].

Let us now extend the dimension of the fault effect parameter space by one to form an $N+1$ parameter-performance (θ-J) space, as depicted in Fig.2. The horizontal plane in this figure is an abstract representation of the space of fault effect parameters. The distance of two fault effect parameter vectors is measured by the Euclidean norm. The vertical axis represents performance, a measure on how well the specified control objectives is achieved. A larger value along this axis corresponds to better achieved objectives.

A point (θ, J) in the θ-J space reflects the consequence of using a particular control law. Its projection on the horizontal plane specifies the corresponding fault parameter value, its vertical axis value indicates the level of performance achieved. For a given control law, different fault effect parameter vector would result in a different performance. Therefore, corresponding to each control law U_i, there is a surface, $J_{U_i}(\theta)$, as shown in Fig.2. Differently configured control laws produce different performance surfaces. The flat surface defines the performance threshold J_{min}, corresponding to a set of minimum objectives. Any point (θ, J) on the the i^{th} surface below this threshold corresponds to an underperformed control law U_i.

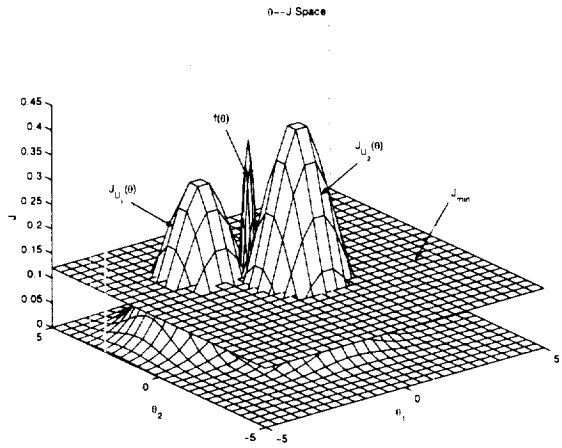

Fig.2 Graphical representation of a θ-J database, and its interaction with a diagnostic outcome

Definition 1. *Let*

$$S^A \equiv \{\theta \in \Omega | J_{U^A}(\theta) \geq J_{min}\}, \quad S^B \equiv \{\theta \in \Omega | J_{U^B}(\theta) \geq J_{min}\}. \tag{2}$$

With respect to any $\theta^* \in \Omega$, control law U^A is said to outperform control law U^B if and only if $\theta^* \in S^A, S^B$, and

$$S^A \supseteq S^B. \tag{3}$$

Similarly, with respect to any set $\Theta \subseteq \Omega$, control law U^A is said to outperform control law U^B if and only if $\Theta \subset S^A, S^B$, and

$$S^A \supseteq S^B. \tag{4}$$

In fact control laws that are robust and adaptive are designed to outperform coventional control laws in the sense defined above. This part of the study is conducted mostly during the off-line design phase and its thoroughness is judged by the extent of exploitation and utilization of existing redundancy, and completeness of coverage of the fault effect in the sense whenever possible. there should be at least one control law U_i that is not underperformed ($J_U(\theta) < J_{min}$) for every $\theta \in \Omega$. The outcome of such an investigation is a θ-J database, which is to be stored for on-line use. On-line data can supplement the database for use with on-line redesign. Such a database is apparently application specific.

The field of diagnosis of dynamic systems has matured over the past twenty years[10, 13, 15]. Diagnosis no doubt plays a crucial role in fault tolerant control. It provides information on the parameter values in the form of estimate $\bar{\theta}$. Since any $\bar{\theta}$ can be called an estimate, a description of the uncertainty associated with an estimate is needed for the estimate to be useful. First and second order statistics of an estimate can provide a reasonably prompt and accurate description of

the uncertainty. They can be obtained through empirical methods. An uncertainty description in the form of a probability density function $f(\hat{\theta})$ is shown in Fig.2. The spread of the density function describes the resolution or the performance of the diagnosis algorithm used. For a normal distribution with mean θ^* and covariance P, a hyper-ellipsoid can be formed as

$$\mathcal{E} \equiv \{\hat{\theta} | (\hat{\theta} - \theta^*)' P^{-1} (\hat{\theta} - \theta^*) \leq \kappa\},$$

where $\kappa > 0$ defines the level of a constant probability density which in turn determines the size of the N-dimensional hyper-ellipsoid. Since the volume of $\mathcal{E}$ is proportional to $\sqrt{\det(\kappa P)}$,

$$R_\kappa \equiv \frac{1}{det(\kappa P)}. \tag{5}$$

can be used as an indicator of the resolution for estimate $\hat{\theta}$. Since P is usually a function of time, so is R_κ.

Definition 2. *With respect to the same failure scenario, diagnostic algorithm A is said to outperform diagnostic algorithm B at time t if and only if*

$$R_\kappa^A(t) \geq R_\kappa^B(t), \ \forall \kappa \geq 0, \tag{6}$$

where R_κ is given by (5), and P is the second order central moment of $f(\hat{\theta})$.

For a given algorithm, $R_\kappa(t)$ is generally an increasing function of t, which reflects the speed/accuracy tradeoff commonly displayed. Due to the finite rate in data acquisition and processing, it is conceivable that a system with faster dynamics is more susceptible to the consequences of uncertainties at the time of decision making.

We now define the notion of coverage. Coverage has been used as a parameter to reflect the ability of a system to automatically recover from the occurrence of a fault during a normal system operation[12]:

$$Coverage \equiv Probability(System\ recovers | Fault\ occurs).$$

At a given time, there is one coverage value associated with each control law in use.

Definition 3. *Denote coverage associated with using control law U_i by $c_{U_i}(t)$. Denote the covered domain over which control law U_i provides an acceptable performance by $\Omega_i \subset \Omega$, i.e.,*

$$\Omega_i \equiv \{\theta \in \Omega | J_{U_i}(\theta) \geq J_{min}\}. \tag{7}$$

Then

$$c_{U_i}(t) = \int_{\Omega_i} f(\theta, t) d\theta. \tag{8}$$

The above integral should be understood as a combination of a multi-variable integral. It represents the probability that estimate $\hat{\theta}$ resides within set Ω_i over which U_i restores the system operation.

Theorem 1. *The optimal redundancy management policy is to select control law U_k that satisfies*

$$c_{U_k}(t_c) = \max_{i=1,2,\cdots} \{c_{U_i}(t_c)\}, \tag{9}$$

where t_c is the critical clearance time at which a corrective action must be taken, and c_{U_i} is given in (8).

Proof. Since an uncovered failure is associated with an exit state which is arrived at transition rate $(1 - c_{U_i}(t))\lambda_j$ for all i and some j, where λ_j is the transition rate out of state j to a non-exit state, The above transition rate enters only into the equation of exit state j in a Markov model and none of the other equations, i.e.,

$$\begin{aligned} & p_{jD}(t + \delta t) = p_{jD}(t) + \delta t(1 - c_{U_i}(t))\lambda_j p_j(t) \\ \Rightarrow \quad & \dot{p}_{jD}(t) = (1 - c_{U_i}(t))\lambda_j p_j(t). \end{aligned}$$

Selecting c_{U_k} that satisfies (9) leads to minimizing the amount of increase in the rate of change for the exit state probability. This probability contributes to the aggregated system death state probability as one of possibly many additive terms. Therefore this policy maximizes the overall system reliability. Critical clearance time t_c is used because it represents the longest time affordable for information acquisition and processing without jeopardizing the opportunity for performance restoration. □

Coverage is a dynamic quantity because $f(\hat{\theta}, t)$ changes with time. Typically, as more time is allowed to collect and process measured data, the resolution, as defined in (5), of the estimate increases and the value of coverage increases toward 1 as well, which is consistent with the classical speed/accuracy tradeoff. All the values of coverage used in part I of the paper are static coverage values. It is conceivable that in one application, a system may be able to afford to wait until sometime t_c when a prescribed static coverage value has been reached to make a decision for redundancy management, while in another application, critical time t_c is prescribed and a decision made at t_c must carry a high risk with the achieved static coverage.

It appears that the definition and the calculation of coverage must involve an explicit estimation algorithm. This is in fact not the case. Even for reliable control[18] where no estimation algorithm is involved at all, as long as there is a probabilistic description of the fault-effect parameter estimate (a uniform distribution over Ω in the case of total ignorance), and a database on control performance has been established, coverage is well defined.

From Definition 3 it can be seen that coverage is related to the performance of each individual control law J_{U_i}, to the system performance threshold J_{min}, and to the diagnostic resolution determined by $f(\hat{\theta})$. Therefore, in addition to its role as the criterion for optimal

redundancy management, coverage also plays a crucial role in providing guidelines for integrated designs of fault tolerant control systems. Since the above mentioned relation is uniquely and explicitly defined, the design guidelines are unambiguous and design results are measurable.

In the statement of the next three theorems, variable t is supressed for simplicity. This can also be regarded as confining our interest to only static coverage for some prescribed critical clearance time t_c.

Theorem 2. *Given a control performance threshold J_{min}, and an estimate $\hat{\theta} \in \Omega$ with a fixed distribution $f(\theta)$. Suppose U^A and U^B are two candidate control laws. Then $c_{U^A} \geq c_{U^B}$ if U_k^A outperforms U_k^B.*

Proof. Since U_k^A outperforms U_k^B, it follows by Definition 1 that

$$\Omega^A \equiv \{\theta \in \Omega | J_{U^A}(\theta) \geq J_{min}\} \supseteq \Omega^B \equiv \{\theta \in \Omega | J_{U^B}(\theta) \geq J_{min}\}.$$

Then by Definition 3

$$c_{U^A} - c_{U^B} = \int_{\Omega^A} f(\theta)d\theta - \int_{\Omega^B} f(\theta)d\theta = \int_{\Omega^A \cap \bar{\Omega}^B} f(\theta)d\theta \geq 0.$$

Therefore $c_{U^A} \geq c_{U^B}$. □

Based on Theorem 2, a robustified control law that has achieved an expansion of the covered domain leads to a higher coverage. Similarly, if an expansion of the covered domain has been achieved by making the control law adaptive, a higher coverage can be attained.

Theorem 3. *Given a control law U_i, and an estimate $\hat{\theta} \in \Omega$ with a fixed distribution $f(\theta)$. $J_{U_i}(\theta)$ is assuemd to be a single valued function over Ω. Suppose J_{min}^A and J_{min}^B are two control performance thresholds. Then $c_{U^A} \geq c_{U^B}$ if $J_{min}^A < J_{min}^B$.*

Proof. Since $J_{U_i}(\theta)$ is single valued over Ω, its α-cuts[?]

$$^{\alpha}J_{U_i}(\theta) \equiv \{\theta \in \Omega | J_{U_i}(\theta) \geq \alpha, \alpha \geq 0\}$$

form a nested sets

$$^{\alpha_i}J_{U_i}(\theta) \supseteq ^{\alpha_j}J_{U_i}(\theta), \quad \alpha_i \leq \alpha_j.$$

Let $\alpha = J_{min}^A$ and $\beta = J_{min}^B$. Then $J_{min}^A < J_{min}^B$ implies

$$^{\alpha}J_{U_i}(\theta) \supseteq ^{\beta}J_{U_i}(\theta).$$

From Definition 3

$$c_{U^A} - c_{U^B} = \int_{\alpha_{J_{U_i}(\theta)}} f(\theta)d\theta - \int_{\beta_{J_{U_i}(\theta)}} f(\theta)d\theta = \int_{\alpha_{J_{U_i}(\theta)} \cap \overline{\beta_{J_{U_i}(\theta)}}} f(\theta)d\theta \geq$$

Therefore $c_{U^A} \geq c_{U^B}$. □

Theorem 3 states that it is more difficult to achieve high coverage for a system with a more stringent control performance requirement.

Theorem 4. *Given a control law U_i, a control performance threshold J_{min}, and two estimates with distributions $N(\theta^*, P_A)$ and $N(\theta^*, P_B)$, respectively, where*

$$\theta^* \in \Omega_i \equiv \{\theta \in \Omega | J_{U_i}(\theta) \geq J_{min}\}$$

and $P_B = \chi P_A$, $\chi > 1$. In addition, assume $^{\alpha}J_{U_i}(\theta)$ is convex for all $\alpha \geq 0$. Then $c_{U^A} \geq c_{U^B}$.

Proof. Since $P_B = \chi P_A$, it follows from Definition 3 that

$$R_A^{\kappa} = \chi^N R_B^{\kappa} > R_B^{\kappa}, \quad \forall \kappa \geq 0.$$

Therefore diagnostic algorithm A outperforms algorithm B. Let $^{\alpha}f_A(\theta)$ and $^{\alpha}f_B(\theta)$ be the α-cuts of the two distributions over R^N, where $\alpha \geq 0$. Let α_0 be such that $^{\alpha_0}f_A(\theta) = ^{\alpha_0}f_B(\theta)$, and $\alpha_{max} = f_A(\theta^*) = 1/\sqrt{2\pi}^N det(P_A)$. The fact

$$\int_0^{\alpha_{max}} [^{\alpha}f_A(\theta)]d\alpha = \int_0^{\alpha_{max}} [^{\alpha}f_B(\theta)]d\alpha = 1$$

yields

$$\int_0^{\alpha_0} [^{\alpha}f_A(\theta) - ^{\alpha}f_B(\theta)]d\alpha + \int_{\alpha_0}^{\alpha_{max}} [^{\alpha}f_A(\theta) - ^{\alpha}f_B(\theta)]d\alpha = 0. \quad (10)$$

$P_A < P_B$ implies that the first integrand is non-positive for each θ and the second is non-negative for each θ. This still holds after restricting the α-cuts of the two distributions to the convex J_{min}-cut of $J_{U_i}(\theta)$. When the restriction to J_{min}-cut of $J_{U_i}(\theta)$ affects only the first term, the first term becomes less negative, and (10) becomes positive. In this case,

$$c_{U^A} - c_{U^B} = \int_{\Omega_i} [f_A(\theta) - f_B(\theta)]d\theta = \int_0^{\alpha_0} [^{\alpha}f_A(\theta) - ^{\alpha}f_B(\theta)]d\alpha +$$

$$+ \int_{\alpha_0}^{\alpha_{max}} [^{\alpha}f_A(\theta) - ^{\alpha}f_B(\theta)]d\alpha, \quad \theta \in \Omega_i \geq 0,$$

and therefore, $c_{U^A} \geq c_{U^B}$. For every θ at which the restriction to the J_{min}-cut of $J_{U_i}(\theta)$ affects the second term in (10), the first integrand vanishes because of the nested structure of the α-cuts. Since $\theta^* \in \Omega_i \subseteq J_{min}$-cut of $J_{U_i}(\theta)$, there will always be some set around θ^* over which the second term is nonzero. Therefore (10) remains non-negative, and $c_{U^A} \geq c_{U^B}$. □

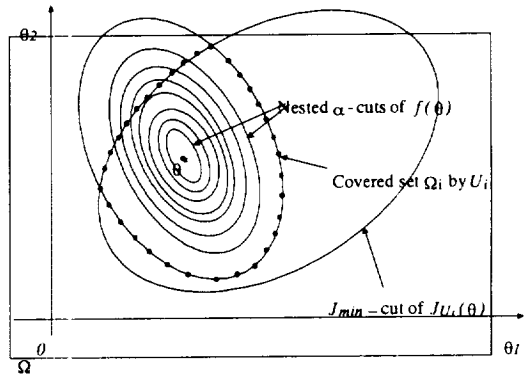

Fig.3 Nested-α-cuts of $f(\theta)$ and J_{min}-cut of J_{U_i} in the fault effect parameter space

Theorem 4 shows for a special case that a higher resolution leads to a higher system reliability with coverage defined in (8). It is possible to extend this result with relaxed assumptions on the distributions of the two estimates.

Due to the page limit, we will not be able to present any examples here. The reader is referred to [20] for an example of a small scale, proof-of-concept fault tolerant flight control system design where the bounds for coverage of a 75% loss of effectiveness of a control effector is ploted against local time (start at the onset of loss pf effectiveness), and the coverage at the critical clearance time is used for a control switch decision based on the minimum risk policy of Theorem 1.

3 Conclusions

The main contributions of the paper are presented in Definition 3, Theorems 1 through 4 and two corollaries in Section 2.

Theorem 1 establishes that maximizing the coverage of the form expressed in (8) optimizes the reliability of a given fault tolerant control system. Theorems 2, 3, and 4 establish that the robustification of a control law, relaxation of control performance requirement, and enhancement of diagnostic resolution help improve system reliability.

It is recognized that both field and test data crucial to reliability study but sensitive from a market-competition and liability viewpoints are difficult and also expensive to obtain, while published accident data alone are not sufficient. Given the situation, new reliability measure and assessment tools that can provide more accurate information under less stringent data requirements are yet to be defined and developed.

References

[1] Ahmed-Zaid, F., Ioannou, P., Gousman, K., and Rooney, R., Accommodation of failures in the F-16 aircraft using adaptive control, *IEEE Control Systems Magazine*, vol.11, pp.73-78, 1991.

[2] Balas, G.J., Doyle, J.C., Glover, K., Packard, A., and Smith, R., *μ-Analysis and Synthesis Toolbox* (for use with MATLAB), The Math Works, 1995.

[3] Banda, S.S., editor, Special issue on reconfigurable flight control, *International Journal of Robust and Nonlinear Control*, vol.9, pp.999-1115, 1999.

[4] Blalnke, M., Staroswiecki, M., and Wu, N.E., Concepts and methods in fault tolerant control, *Proc. American Control Conference*, 2001.

[5] Blanke, M., Izadi-Zamanabadi, R., Bogh, S.A., and Lunau, Z.P., Fault tolerant control systems-a historic review, *J. Control Engineering Practice*, vol.5, pp.693-702, 1997.

[6] Bodson, M., and Groszkiewicz, J., Multivariable adaptive algorithms for reconfigurable flight control, *IEEE Trans. Control System Technology*, vol.5, pp.217-229, 1997.

[7] Branicky, M.S., Multiple Lyapunov functions and other analysis tools for switched and hybrid systems, *IEEE Trans. Automatic Control*, vol.43, pp.475-482, 1998.

[8] R.W.Butler, The SURE approach to reliability analysis, *IEEE Trans. Reliability*,vol.41, pp 210-218, 1992.

[9] Chow. E.Y., and Willsky, A.S., Analytical redundancy and the design of robust detection systems, *IEEE Transaction on Automatic Control*, vol. 29, pp.603-614, 1984.

[10] Chen, J., and Patton, R., *Robust Model-Based Fault Diagnosis for Dynamic Systems*, Kluwer, 1998.

[11] Doyle, J.C., Glover, K., Khargonekar, P. P., and Francis, B.A., State-space solutions to standard H_2 and H_∞ control problems, *IEEE Trans. Automatic Control*, vol.34, 831-847, 1989.

[12] Dugan, and Trivedi, Coverage modeling for dependability analysis of fault tolerant systems, *IEEE Trans. Computers*, vol.38, pp 775-787, 1989.

[13] Gertler, J., *Fault Detection and Diagnosis in Engineering Systems*, Marcel Dekker, 1998.

[14] Isermann, R., and Balle, P., Trands in the application of model-based fault detection and diagnosis of technical processes, *Control Engineering Practices*, vol.5, pp.709-719, 1997.

[15] Mangoubi, R., *Robust Estimation and Failure Detection: A Concise Treatment* Springer-Verlag, 1998.

[16] Noura, H., Sauter, D., Hamelin, F., and Theilliol, D., Fault-tolerant control in Dynamic Systems: application to a winding machine, *IEEE Control Systems Magazine*, vol.20, pp.33-49, 2000.

[17] Reliability models for sensor fault detection with state-estimator schemes, Dirk van Shrick and Peter C. Muller, *Issues for fault diagnosis for dynamic systems*, (Patton, Frank, and Clark, Editors), Chapter 8, pp.219-244, Springer-Verlag, 2000.

[18] Veillette, R.J., Medanic, J.V., and Perkins, R.W., Design of reliable control systems, *IEEE Trans. Automatic Control*, vol.37, pp.290-304, 1992.

[19] Wu, N.E., and Klir, G.J., Optimal redundancy management in reconfigurable control systems based on normalized nonspecificity, *International Journal of Systems Science*, vol.31, pp.797-808, 2000.

[20] Wu, N.E., and Ju, J., Optimal management of redundant control authority for fault tolerance, *Proc. American Control Conference*, 2000.

[21] Wu, N.E., and Ju, J., Parametric modeling and fault tolerant control, *Proc. 19th Digital Avionics Systems Conference*, 2000.

[22] Wu, N.E, Zhou, K., and Salomon, G., Reconfigurability in linear time-invariant systems, *Automatica*, vol.36, pp.1767-1771, 2000.