Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Reliability Monitoring of Fault Tolerant Control Systems [⋆]

Hongbin Li [*], **Qing Zhao** [*], **Zhenyu Yang** [**]

[*] *Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Alberta, Canada, T6G 2V4*
[**] *Department of Computer Science and Engineering, Aalborg University Esbjerg, Niels Bohrs Vej 8, 6700 Esbjerg, Denmark*

Abstract: This paper proposes a reliability monitoring scheme for active fault tolerant control systems using a stochastic modeling method. The reliability index is defined based on system dynamical responses and a safety region; the plant and controller are assumed to have a multiple regime model structure; and a semi-Markov model is built for reliability evaluation based on safety behavior of each regime model estimated by using Monte Carlo simulation. Moreover, the history data of fault detection & isolation decisions is used to update its transition characteristics and reliability model.

1. INTRODUCTION

New control techniques and design approaches have been developed to treat system component faults and to improve system reliability and availability, which are collectively called Fault Tolerant Control Systems (FTCS's). FTCS's usually employ Fault Detection and Isolation (FDI) schemes and reconfigurable controllers to accommodate fault effects, also known as active FTCS's. In these systems, faults and imperfect FDI results may degrade overall system performance thus corrupt designated reliability requirement. Therefore, it is necessary to validate the design of FTCS's from a reliability perspective.

The reliability of FTCS's has been investigated using various methods. The key problem is to establish appropriate reliability models with control objectives and safety requirements incorporated. Wu used serial-parallel block diagrams and Markov models for evaluation purpose, and defined a coverage concept to relate reliability and control actions (Wu [2004]). Walker proposed Markov and semi-Markov models to describe the transitions of fault and FDI modes, but without taking into account the control actions (Walker [1997]). In our previous work, we adopted static model-based control objectives and built a semi-Makov model from imperfect FDI and hard-deadline concepts (Li and Zhao [2005, 2006]). However, in many practical systems, the system safety and reliability are often assessed based on dynamic system responses. For instance, reliability in structural control is defined as the probability of system outputs outcrossing safety boundaries and evaluated by using Gaussian approximation (Song and Kiureghian [2006]). Also, an online reliability monitoring scheme using updated information may aid maintenance scheduling, provide pre-alarming, and avoid emergent overhauls. How to evaluate reliability when it is defined on system trajectory and how to implement an online-monitoring scheme are the main motivations of this work.

In this paper, first of all, a Steady State Test (SST) is proposed to reduce false alarms of FDI decisions. A stochastic model of such an FDI scheme is obtained based on which the transition characteristics of FDI modes can be described. A reliability evaluation scheme for FTCS's is then developed based on system dynamic responses and safety boundary. At last, online monitoring features are considered, such as estimation of FDI transition parameters based on history data and timely update of reliability index to reflect the changing system behavior. The remainder of this paper is organized as follows: The assumptions and system structure are given in Section 2; FDI scheme, modeling, and parameter estimation are discussed in Section 3; the determination of out-crossing failure rates and hard-deadlines are discussed in Section 4; and the reliability model construction is discussed in Section 5 followed by a demonstration example of an F-14 aircraft model in Section 6.

2. ASSUMPTIONS AND SYSTEM STRUCTURE

Assumption 1. The considered plant is assumed to have finite fault modes, and dynamics under each fault mode can be effectively represented by a linear system model.

Fault modes are represented by a set S with N integers; $\{\mathcal{M}_i : i \in S\}$ represents the set of dynamical plant models under various fault modes; and $\{\mathcal{K}_j : j \in S\}$ denotes a set of reconfigurable controllers in a switching structure. $\mathcal{K}_j$ is designed for fault mode j based on $\mathcal{M}_j$, $j \in S$. An FDI scheme is used to generate estimates of fault modes, which may deviate from true fault modes with error probabilities.

Assumption 2. FDI scheme is assumed to generate a fault estimate based on a batch of measurements and calculations for every fixed period T_c.

This assumption states a cyclic feature of FDI, such as statistical tests and Interactive Multiple Model (IMM) Kalman filters (Zhang and Li [1998]). FDI modes are represented by a discrete-time stochastic process $\eta_n \in S$, where $n \in \mathbb{N}$, the set of non-negative integers. The time duration between consecutive discrete indices is equal to FDI detection period T_c. $\mathcal{K}_j$ is put in use when $\eta_n = j$, $j \in S$. Corresponding to η_n, a discrete-time stochastic process ζ_n denotes true fault mode. In reliability engineering, constant failure rates are usually assumed for the main part of component life cycle. In such a case, ζ_n can be described as a Markov chain, and its transition probabilities are denoted as $G_{ij} = \Pr\{\zeta_{n+1} = j|\zeta_n = i\}$, $i, j \in S$.

Assumption 3. System performance is assumed to be represented by a vector signal $z(t)$. Safety region, denoted as Ω, is assumed to a fixed region in space of $z(t)$ bounded by its safety threshold. Failure is assumed to occur when $z(t)$ exceeds a safety region for the first time.

It is common in control systems to use a signal $z(t)$ to represent performance; and $z(t)$ is usually to be kept

[⋆] This work was supported in part by the Natural Sciences and Engineering Research Council of Canada.

at small values against influences from exogenous disturbances, model uncertainties, and model characteristic changes caused by faults. Safety region Ω is assumed to be fixed and known a priori. The scenario that $z(t)$ exceeds Ω represents lost of control or a failure. More discussions on this assumption can be found in Field and Bergman [1998].

Definition 4. For a time interval from 0 to t, the reliability function $R(t)$ is defined as the following probability:

$$R(t) = \Pr\{\forall 0 \leq \tau \leq t, \quad z(\tau) \in \Omega\}.$$

Mean Time To Failure (MTTF) is defined as the expected time of satisfactory operation:

$$\text{MTTF} = \int_0^\infty R(t)dt.$$

The MTTF herein represents the mean operational time without human intervention before failure.

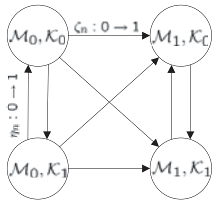
$\mathcal{M}_0, \mathcal{K}_0$
$\zeta_n : 0 \to 1$
$\mathcal{M}_1, \mathcal{K}_0$
$\eta_n : 0 \to 1$
$\mathcal{M}_0, \mathcal{K}_1$
$\mathcal{M}_1, \mathcal{K}_1$

Fig. 1. Transitions among regime models.

Compared with ζ_n and η_n, $z(t)$ is typically a fast-changing function determined by both continuous and discrete dynamics. As shown in Figure 1, ζ_n and η_n are two regime modes. When the modes $\zeta_n = i$ and $\eta_n = j$ are fixed, $z(t)$ evolves according to plant model $\mathcal{M}_i$ and controller $\mathcal{K}_j$ during the transitions among the regime models. As a result of this hybrid dynamics, directly evaluating $R(t)$ and MTTF is difficult. Therefore, a discrete-time semi-Markov chain X_n is constructed for reliability evaluation purpose. The main idea is: the hybrid system is decomposed into various regime models; each regime model is then evaluated for related safety characteristics; and X_n is constructed to integrate these characteristics with transition parameters of regime modes and its transition probabilities for reliability evaluation computed. The structure and main components of reliability monitoring scheme are illustrated in Figure 2.

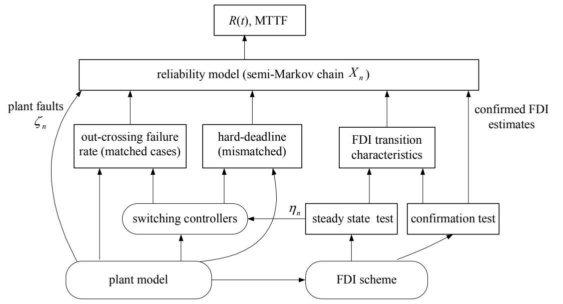

Fig. 2. System structure.

Semi-Markov reliability model X_n is the kernel component for calculating MTTF. It is constructed based on the following parameters: 1) the transition rates of ζ_n, called plant failure rates; 2) the estimates of ζ_n from FDI and confirmation test, called confirmed fault modes; 3) the parameters of η_n estimated from history data, called FDI transition characteristics; 4) the probability of $z(t)$ crossing safety boundary during an FDI cycle T_c when $\zeta_n = \eta_n$, called failure out-crossing rates. 5) the average number of periods before crossing safety boundary when $\zeta_n \neq \eta_n$, called hard-deadlines. Among these parameters, the second and third ones can be updated online.

3. FDI SCHEME AND ITS CHARACTERIZATION

3.1 Steady state tests

It is well-known that false alarm and missing detection rates are two conflicting quality criteria of FDI. One is usually improved at the cost of degrading the other. The general rules of adjusting FDI to balance these two criteria are often not known. Herein we focus on false alarm reduction. Considering that most false alarms last for short time only, an SST strategy is adopted for post-processing FDI decisions.

SST requires that, when FDI decision changes, new decision is accepted only when it stays the same for a minimum number of detection cycles. Let $T_{\text{SST}j}$ denote the required number of consistent cycles for FDI mode j, $j \in S$. The effectiveness of this SST strategy relies on the distribution of false alarm durations. For example, if a nonnegative discrete random variable λ_0 denotes the false alarm duration when system fault mode $\zeta_n = 0$, $T_{\text{SST}0}$ can be taken as $(1-\alpha)$-quantile of λ_0, $0 < \alpha < 1$, meaning

$$\Pr\{\lambda_0 > T_{\text{SST}0}\} \leq \alpha,$$

which implies that false alarm probability can be reduced by ratio α when accepting FDI decisions after $T_{\text{SST}0}$. The weakness of this method is additional detection time delay of $T_{\text{SST}j}$ when fault occurs. Detection decisions from SST are represented by η_n and used for controller reconfigurations. In Figure 2, the confirmation test is an SST with large test period to further reduce false alarm probability to a negligible level. It generates confirmed fault modes, which are used with FDI trajectories for updating transition parameters of η_n and reliability index.

3.2 Stochastic models

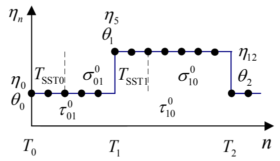

Fig. 3. A sample path of η_n.

A sample path of η_n is given in Figure 3. Let $\theta_m \in S$ and $T_m \in \mathbb{N}$ denote the FDI mode and cycle index respectively after the m-th transition of η_n, $m \in \mathbb{N}$. For example, in Figure 3, $\theta_1 = \eta_5$ and $T_2 = 5$. θ_m and T_m together determine FDI trajectory, and $\eta_n = \theta_{S_n}$, where $S_n = \sup\{m \in \mathbb{N} : T_m \leq n\}$ is the discrete-time counting process of the number of jumps in $[1, n]$. $(\theta, T) \triangleq \{\theta_m, T_m : m \in \mathbb{N}\}$ is called a discrete-time Markov renewal process if

$$\begin{aligned}\Pr\{\theta_{m+1} = j, T_{m+1} - T_m = l | \theta_0, \cdots, \theta_m; T_0, \cdots, T_m\} \\ = \Pr\{\theta_{m+1} = j, T_{m+1} - T_m = l | \theta_m\}\end{aligned} \tag{1}$$

holds for fixed $\zeta_{T_m} = \zeta_{T_m+1} = \cdots = \zeta_{T_{m+1}} = k$, $k, j \in S$, $l, m \in \mathbb{N}$. $\eta_n = \theta_m$ is then called the associated discrete-time semi-Markov chain of (θ, T). It can be shown that θ_m is a Markov chain, and its transition probability matrix is denoted by P^k.

Given $\zeta_{T_m} = \zeta_{T_m+1} \cdots = \zeta_{T_{m+1}} = k$, let $\tau_{ij}^k = T_{m+1} - T_m$ if $\theta_m = i$ and $\theta_{m+1} = j$, $i, j, k \in S$. τ_{ij}^k is the sojourn time of η_n between its transition to state i at T_m and the consecutive transition to j at T_{m+1}. If the transition destination state is not specified, let τ_i^k denote the sojourn time at state i.

As shown in Figure 3, τ_{ij}^k is the sum of two variables: a constant $T_{\mathrm{SST}i}$ for SST period and a random sojourn time σ_{ij}^k. Let $h_{ij}^k(l)$ and $g_{ij}^k(l)$ denote the discrete distribution functions of τ_{ij}^k and σ_{ij}^k respectively, which have the following relations:

$$h_{ij}^k(l) = \Pr\{\tau_{ij}^k = l\} = \begin{cases} 0, & l \le T_{\mathrm{SST}i}; \\ g_{ij}^k(l - T_{\mathrm{SST}i}), & l \le T_{\mathrm{SST}i}. \end{cases} \tag{2}$$

This semi-Markov description provides a general model on FDI mode transitions, but it involves a large number of parameters. The transition characteristics of η_n are jointly determined by P^k and h_{ij}^k (or g_{ij}^k). If S contains N fault modes, there are N transition probability matrices P^k and N^3 distribution functions h_{ij}^k. If each h_i^k follows geometric distribution, the description of η_n may degenerate to a hypothetical Markov model η_n'.

Markov chain can be considered as a special type of semi-Markov chain. If η_n can be modeled as a Markov chain with transition probability matrix denoted by H^k for $\zeta_n = k$, the following relations hold:

$$P_{ij}^k = \frac{H_{ij}^k}{1 - H_{ii}^k}, \tag{3}$$

$$h_{ij}^k(l) = (H_{ii}^k)^{l-1} H_{ij}^k, \tag{4}$$

$$h_i^k(l) = (H_{ii}^k)^{l-1}(1 - H_{ii}^k), \tag{5}$$

It is obvious that h_i^k is a geometric distribution. In fact, this is an essential property of Markov chain, as shown in the following Lemma.

Lemma 5. A discrete-time semi-Markov chain degenerates to a Markov chain if and only if the sojourn time at each state (when subsequent state is not specified) follows geometric distribution.

The proof is omitted for brevity. When T_{SST} is nonzero, the sojourn time of η_n does not follow geometric distribution owing to this deterministic constant, and Lemma 5 cannot be directly applied. However, as T_{SST} is known, a hypothetical process η_n' can be constructed by setting T_{SST} to zeros; if the sojourn time of η_n' is geometrically distributed, it can be described as a Markov chain; the original sojourn time of η_n can be recovered by adding T_{SST} to that of η_n'. This method may greatly reduce the number of parameters for characterizing FDI results.

3.3 Transition parameter estimation

FDI transition parameters can be estimated as an off-line test on FDI when both fault mode and FDI detection results are known. This estimation can also be carried out online using FDI history data and confirmed fault modes.

When η_n is modeled as a semi-Markov chain, P^k and h_{ij}^k (or g_{ij}^k) are parameters to be estimated. P^k can be estimated from the transition history of η_n. For example, when ζ_n is kept as a constant k, if there are M_{ij} transitions from i to j among all M transitions leaving i, the ij-th element of P^k can be estimated as $\hat{P}_{ij}^k = M_{ij}/M$. The estimation of sojourn time distribution g_{ij}^k can be completed in two steps: the histogram of sojourn time is firstly examined to select a standard distribution such that nonparametric estimation is converted to a parametric one; $\hat{g}_{ij}^k$ is then obtained by estimating unknown parameters in distribution functions.

If $\hat{g}_{ij}^k$ follows geometric distribution for all $i, j, k \in S$, η_n can be described as a hypothetical Markov chain η_n' under the hypothesis that $T_{\mathrm{SST}i} = 0$. As a result, transition probability H_{ij}^k from i to j and sojourn time τ_i^k at i have the following relation:

$$\Pr\{\tau_i^k = n\} = (H_{ii}^k)^{n-1}(1 - H_{ii}^k).$$

Therefore, $E(\tau_i^k) = \frac{1}{1-H_{ii}^k}$, and H_{ii}^k can be estimated by

$$\hat{H}_{ii}^k = \begin{cases} 1 - \dfrac{1}{\sum_{l=1}^M \tau_i^k(l)/M}, & \displaystyle\sum_{l=1}^M \tau_i^k(l)/M \neq 0, \\ 1, \quad \text{otherwise}, \end{cases} \tag{6}$$

where $\tau_i^k(l)$ denote M sojourn time samples at state i, $l = 1, \cdots, M$. H_{ij}^k can be estimated based on the transition frequency from state i to j:

$$\hat{H}_{ij}^k = (1 - \hat{H}_{ii}^k) w_{ij}^k / M, \tag{7}$$

where $1 - \hat{H}_{ii}^k$ is a normalization coefficient and w_{ij}^k represents the number of FDI transitions from i to j.

4. OUT-CROSSING FAILURE RATES AND HARD-DEADLINES

Owing to FDI delays or incorrect decisions, controller $\mathcal{K}_i$ may be used for its designated regime model $\mathcal{M}_i$ (namely, matched cases) and other model $\mathcal{M}_j$, $i \neq j$ (namely, mismatched cases). Matched cases usually account for major operation time, while mismatched cases often appear as temporary operation.

Definition 6. The out-crossing failure rate in matched cases is defined as

$$v_{ii} \triangleq \Pr\{\ \exists \tau,\ nT_{\mathrm{c}} < \tau \le (n+1)T_{\mathrm{c}},\ z(\tau) \notin \Omega | z(nT_{\mathrm{c}}) \in \Omega,$$
$$\zeta_n = \eta_n = i\},\ i \in S$$

Monte Carlo simulation can be used for estimating v_{ii}: Sample simulations are performed using generated sample uncertain plant model and sample disturbance input; the simulation time when system fails is called a sample time-to-failure. With a large number of time-to-failure samples obtained, v_{ii} can be estimated as the ratio between T_{c} and sample mean of time-to-failure. Mismatched cases are usually temporary operation caused by FDI false alarms or delays, and system may return to matched cases if $z(t)$ does not diverge to unsafe region. So, it is important to find out the average tolerable time before system failure. This time limit is called hard-deadline, denoted by $T_{\mathrm{hd}ij}$ for $\zeta_n = i$ and $\eta_n = j$. It can also be estimated by sample mean of time-to-failure using Monte Carlo simulations.

5. RELIABILITY MODEL CONSTRUCTION

The states of semi-Markov chain X_n for reliability evaluation are classified into two groups: one unique failure state, denoted by s_{F}, and multiple functional states, defined as state combinations of $\zeta_n = i$ and $\eta_n = j$, denoted as s_{ij}, $i, j \in S$. For example, if two types of faults are considered in the plant, ζ_n includes states of fault-free, fault type 1, fault type 2, and both fault 1 and 2, represented by $S = \{0, 1, 2, 3\}$, and X_n contains 17 states.

The semi-Markov kernel of X_n is denoted as $Q(\cdot, \cdot, n)$, representing the one-time transition probability in n steps. It is determined by the following parameters: 1) transition characteristics of fault and FDI modes; 2) outcrossing failure rate in state s_{ii} denoted by v_{ii}; 3) hard-deadline in state s_{ij} denoted by $T_{\mathrm{hd}ij}$; 4) FDI SST period denoted by $T_{\mathrm{SST}j}$ for FDI mode j.

Let us begin with the case that FDI mode can be described as a hypothetical Markov chain η_n' with transition probability denoted by H_{ij}^k. The calculation of Q is classified into the following cases:

Case 1: The transitions from functional states to themselves are not defined and the corresponding elements are assigned as zeros:

$$Q(s_{ii}, s_{ii}, m) = 0, \quad Q(s_{ij}, s_{ij}, m) = 0, i, j \in S.$$

Case 2: Failure state s_{F} is absorbing:

$$Q(s_{\mathrm{F}}, s_{\mathrm{F}}, m) = \begin{cases} 1, & m = 1; \\ 0, & m > 1. \end{cases}$$

Case 3: Matched states s_{ii}:

$$Q\ (\ s_{ii}, s_{\mathrm{F}}, m) = \begin{cases} (1 - v_{ii})^{m-1} G_{ii}^{m-1} v_{ii}, & m \le T_{\mathrm{SST}i}, \\ p_{ii}[(1 - v_{ii}) G_{ii} H_{ii}^i]^{(m - T_{\mathrm{SST}i-1})} v_{ii}, & m > T_{\mathrm{SST}i}, \end{cases}$$

$$Q\ (\ s_{ii}, s_{ji}, m) =$$
$$\begin{cases} (1 - v_{ii})^{m-1} G_{ii}^{m-1} (1 - v_{ii}) G_{ij}, & m \le T_{\mathrm{SST}i}, \\ p_{ii}[(1 - v_{ii}) G_{ii} H_{ii}^i]^{(m - T_{\mathrm{SST}i-1})} (1 - v_{ii}) G_{ij} H_{ii}^i, & m > T_{\mathrm{SST}i}, \end{cases}$$

$$Q\ (\ s_{ii}, s_{ij}, m) =$$
$$\begin{cases} 0, & m \le T_{\mathrm{SST}i}, \\ p_{ii}[(1 - v_{ii}) G_{ii} H_{ii}^i]^{(m - T_{\mathrm{SST}i-1})} (1 - v_{ii}) G_{ii} H_{ij}^i, & m > T_{\mathrm{SST}i}, \end{cases}$$

$$Q\ (\ s_{ii}, s_{kj}, m) =$$
$$\begin{cases} 0, & m \le T_{\mathrm{SST}i}, \\ p_{ii}[(1 - v_{ii}) G_{ii} H_{jj}^k]^{(m - T_{\mathrm{SST}i} - 1)} (1 - v_{ii}) G_{ik} H_{ij}^i, & m > T_{\mathrm{SST}i}, \end{cases}$$

where $p_{ii} = \Pr\{X_1 = X_2 = \cdots = X_{T_{\mathrm{SST}i}} = s_{ii} | X_0 = s_{ii}\} = (1 - v_{ii})^{T_{\mathrm{SST}i}} G_{ii}^{T_{\mathrm{SST}i}}$, $i \ne j$, $k \ne i$, $i, j, k \in S$.

The derivation of these equations are based on Markov transition probabilities and the decomposition of each event. For example,

$$\begin{aligned} & Q\ (s_{ii}, s_{\mathrm{F}}, m) \\ & = \Pr\{X_1 = X_2 = \cdots = X_{m-1} = s_{ii}, X_m = s_{\mathrm{F}} | X_0 = s_{ii}\} \\ & = \Pr\{X_1 = X_2 = \cdots = X_{m-1} = s_{ii} | X_0 = s_{ii}\} \Pr\{X_1 = s_{\mathrm{F}} | X_0 = s_{ii}\}. \end{aligned}$$

Considering steady state test of FDI, if $m \le T_{\mathrm{SST}i}$,

$$\Pr\{X_1 = X_2 = \cdots = X_{m-1} = s_{ii} | X_0 = s_{ii}\} = (1 - v_{ii})^{m-1} G_{ii}^{m-1};$$

If $m > T_{\mathrm{SST}i}$,

$$\begin{aligned} & \Pr\{X_1 = X_2 = \cdots = X_{m-1} = s_{ii} | X_0 = s_{ii}\} \\ & = \Pr\{X_1 = X_2 = \cdots = X_{T_{\mathrm{SST}i}} = s_{ii} | X_0 = s_{ii}\} \cdot \\ & \qquad [(1 - v_{ii}) G_{ii} H_{ii}^i]^{(m - T_{\mathrm{SST}i-1})}. \end{aligned}$$

$Q(s_{ii}, s_{\mathrm{F}}, m)$ can be obtained by combining these two probabilities with $\Pr\{X_1 = s_{\mathrm{F}} | X_0 = s_{ii}\} = v_{ii}$,

Case 4: Mismatched states: s_{ij}, $i \ne j$. When $m \le T_{\mathrm{SST}j}$, the transition probability of $X(t)$ to any other state is zero because of SST period. When $T_{\mathrm{SST}j} < m \le T_{\mathrm{hd}ij}$, the probability of $X(t)$ transiting to any other state is zero except to s_{ii}. The above reasoning is based on the facts that FDI rarely jumps to other false modes when current mode is incorrect, and mean fault occurrence time is in a much higher order compared with a short false FDI detection period. Therefore, when $T_{\mathrm{SST}j} < m \le T_{\mathrm{hd}ij}$,

$$\begin{aligned} & Q(s_{ij}, s_{\mathrm{F}}, m) = 0, \\ & Q(s_{ij}, s_{ii}, m) = (H_{jj}^i)^{m - T_{\mathrm{SST}j} - 1} H_{ji}^i, \quad j \ne l, \quad j, l \in S. \end{aligned}$$

When $m > T_{\mathrm{hd}ij} + 1$, X_n jumps to s_{F} at the earliest time $m = T_{\mathrm{hd}ij} + 1$ only:

$$\begin{aligned} Q(s_{ij}, s_{\mathrm{F}}, T_{\mathrm{SST}i} + 1) & = 1 - \sum_{k = T_{\mathrm{SST}i} + 1}^{T_{\mathrm{hd}ij}} Q(s_{ij}, s_{ii}, m) \\ & = 1 - \frac{1 - (H_{jj}^i)^{T_{ij} - T_{\mathrm{SST}j} + 1}}{1 - H_{jj}^i} H_{ji}^i. \end{aligned}$$

In the general cases, η_n is modeled as a semi-Markov chain, and the competition probabilities methods discussed in Li and Zhao [2006] can be utilized.

Definition 7. Given $\zeta_n = i$ and $\eta_n = j$, the combinational mode is denoted as (i, j), $i, j \in S$. Suppose $(\zeta_{n+1}, \eta_{n+1}) = \cdots = (\zeta_{n+m-1}, \eta_{n+m-1}) = (i, j)$ and the next combinational mode after the consequent transition of ζ_n or/and η_n at $n + m$ is $(\zeta_{n+m}, \eta_{n+m}) = (k, l)$, where $k \ne i$ or/and $l \ne j$, $k, j \in S$. The probability of this event is called the competition probability, denoted by $\rho_{(i,j) \rightarrowtail (k,l)}(m)$.

The calculation formulas of $\rho_{(i,j) \rightarrowtail (k,l)}(m)$ were derived in Section 3 of Li and Zhao [2006] and are omitted here for brevity. As the states of X_n is mainly defined as the state combinations of ζ_n and η_n, the calculation of the semi-Markov kernel of X_n is simplified when $\rho_{(i,j) \rightarrowtail (k,l)}(m)$ is available, as shown in the following listed formulas.

$$\begin{aligned} & Q(s_{ii}, s_{kl}, m) = (1 - v_{ii})^m \rho_{(i,i) \rightarrowtail (k,l)}(m), \\ & Q(s_{ii}, s_{\mathrm{F}}, m) = (1 - v_{ii})^{m-1} v_{ii}, \\ & Q(s_{ii}, s_{ii}, m) = 0, \\ & Q(s_{ij}, s_{kl}, m) = \begin{cases} \rho_{(i,j) \rightarrowtail (k,l)}(m), & m \le T_{\mathrm{hd}ij} \\ & \text{and } k = l = i, \\ 0, & \text{otherwise} \end{cases} \\ & Q(s_{ij}, s_{\mathrm{F}}, m) = \begin{cases} 0, & m \le T_{\mathrm{hd}ij}, \\ 1 - \sum_{m=1}^{T_{\mathrm{hd}ij}} Q(s_{ij}, s_{ii}, m), & m > T_{\mathrm{hd}ij}, \end{cases} \\ & Q(s_F, s_F, m) = \begin{cases} 1, & m = 1; \\ 0, & m > 1. \end{cases} \end{aligned}$$

Although these formulas appear to be simpler, both the parameter estimation and competition probability calculations need much more calculation burden than the first case when FDI decision is modeled as a hypothetical Markov chain. Once X_n is constructed, calculation of reliability function and MTTF are straightforward using available formulas given in Barbu et al. [2004].

6. DEMONSTRATION ON AN F-14 AIRCRAFT MODEL

6.1 Model description

A control problem of F-14 aircraft was presented in Balas et al. [1998], and also used as a demonstration example in MATLAB® Robust Control Toolbox [1]. This problem considers the design of a lateral-directional axis controller during powered approach to a carrier landing with two command inputs from the pilot: lateral stick and rudder

[1] MATLAB and Robust Control Toolbox are the trademarks of The MathWorks, Inc.

pedal. At an angle-of-attack of 10.5 degree and airspeed of 140 knots, the nominal linearized F-14 model has four states: lateral velocity, yaw rate, roll rate, and roll angle, denoted by v, r, p, and ϕ respectively; two control inputs, differential stabilizer deflection and rudder deflection, denoted by δ_{dstab} and δ_{rud} respectively; and four outputs: roll rate, yaw rate, lateral acceleration, and side-slip angle, denoted by p, r, y_{ac}, and β respectively. The system dynamics equations are ignored here, and can be loaded in MATLAB 7.1 using command 'load F14nominal'. An additional disturbance input is added to represent the wind gust effects.

The control objectives are to have handling quality (HQ) responses from lateral stick to roll rate p and from rudder pedal to side-slip angle β match ideal HQ models. Under fault free modes, the HQ models are $5\frac{2}{s+2}$ and $-2.5\frac{1.25^2}{s+2.5s+1.25^2}$; when fault occurs, HQ models degrade to $5\frac{1}{s+1}$ and $-2.5\frac{0.75^2}{s+1.5s+0.75^2}$ respectively.

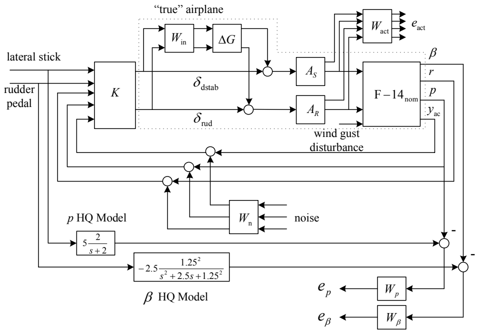

Fig. 4. Control design diagram for F-14 lateral axis (Courtesy of The MathWorks, Inc.)

The system block diagram is shown in Figure 4, where F-14_{nom} represents the nominal linearized F-14 model, and A_S and A_R the actuator models. e_p and e_β represent the weighted model matching errors. Actuator energy is described by e_{act}, and noise is added to the measured output after anti-aliasing filters.

The considered fault occurs in two actuators. Under fault-free mode, their transfer functions are:

$$A_S = A_R = \frac{25}{s+25}.$$

Two types of actuator faults are considered here: each has mean occurrence time 10^5 of FDI periods or its failure rate is 10^{-5}. Under fault type 1, the transfer function of A_S becomes

$$A_S' = 0.5\frac{15}{s+15}.$$

Under fault type 2, the transfer function of A_R becomes

$$A_R' = 0.5\frac{10}{s+10}.$$

These fault modes are described as the change of actuator gains and time constants. The set of fault modes is denoted by $S = \{0, 1, 2, 3\}$, representing fault-free, faut type 1, type 2, and simultaneous occurrence of both.

6.2 Simulation Results

Different H_∞ controllers are designed for each system mode to achieve nominal HQ control objectives under fault-free mode and degraded ones under fault modes. Typical output trajectories under fault-free mode are shown in Figure 5. The absolute minimal matching errors between the real responses and the ideal or degraded ones are shown in Figure 6. When these matching errors go over the safety limits, 30% of expected output, aircraft is considered as failed.

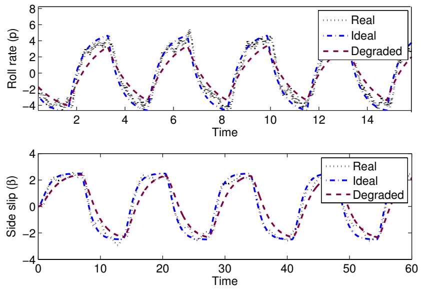

Fig. 5. Output trajectories.

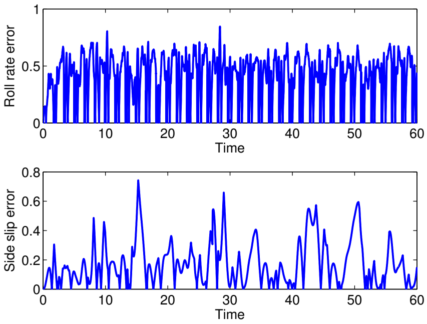

Fig. 6. The trajectories of matching errors.

An IMM FDI is constructed to detect fault occurrences. To reduce false alarms, a steady state test strategy is applied on FDI decisions with $T_{\text{SST}j} = 6$ for any FDI mode j. A typical FDI trajectory is shown in Figure 7. It is clear that the steady FDI mode is free of false alarms in the shown time period. But detection time delays are introduced when fault occurs at 20 and 50 seconds respectively.

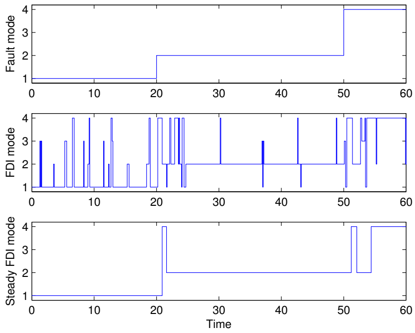

Fig. 7. FDI trajectory.

To represent FDI detection characteristics, a batch of fault and FDI history data is collected for statistical estimation. First, histograms of FDI delays are generated to check its distribution type. When there is no fault, the histogram of FDI sojourn time at fault-free mode is shown in Fig. 8. It clearly resembles a geometric distribution. Equation (6)-(7) are then used to estimate Markov transition probabilities, and those under fault-free mode are obtained as:

$$H^0 = \begin{bmatrix} 0.9990 & 0 & 0.0010 & 0.0000 \\ 1.0000 & 0 & 0 & 0 \\ 0.1330 & 0 & 0.8670 & 0 \\ 0.5000 & 0 & 0 & 0.5000 \end{bmatrix}.$$

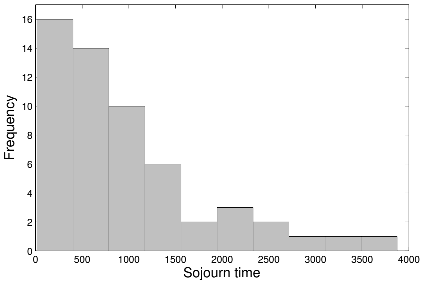

Fig. 8. Histogram of FDI sojourn time.

Note $H^0(2,1)$ represents the transition probability of FDI from decision mode 1 when fault mode is 0. It means that FDI is at false alarm state, and a properly designed FDI transits back to mode 0.

As a result of imperfect FDI results, controllers may be engaged for wrong fault modes. So, it is necessary to evaluate system behavior under all possible combinations of FDI and fault modes. Here, Monte Carlo simulations are adopted with the following settings: 1) command stick inputs are square waves with frequency as a random variable ranging from 0.2 to 2 Hertz; 2) wind gust disturbances and sensor measurement noises are assumed to be Gaussian processes; 3) actuator saturation effects limit control inputs to 20 and 30 respectively; 4) system failure is assumed to occur when model matching errors go over 30% of stick commands. For example, with fault mode 2 occurred and $\mathcal{K}_2$ engaged, mean time to system failure is 57403 seconds when controller K_2 is used, and 6 seconds when $\mathcal{K}_1$ is used. Considering the sampling period is 0.1 second for IMM FDI, the out-crossing failure rate and hard-deadline are: $v_{22} = 1/574030$, $T_{\text{hd}21} = 60$.

BY using MTTF as an objective, an optimization is performed on T_{SST}. It is found that MTTF will be improved from 27727 to 32605 seconds if $T_{\text{SST}j}$ is reduced from 6 to 1. A comparison of reliability functions before and after this optimization is shown in Figure 9. It is clearly shown that reliability index is improved. Comparisons on the transition probabilities between these two SST periods are shown in Figure 10, in which each sub-figure gives the transition probability curves from s_{00} to other states. For example, the sub-figure at the first row and second column shows the transition probabilities to s_{01} is increased from 0 to about 0.008. This is a natural result of increased false alarms when reducing $T_{\text{SST}j}$. In fact, when $T_{\text{SST}j} = 1$, new Markov transition parameters H'^0 becomes:

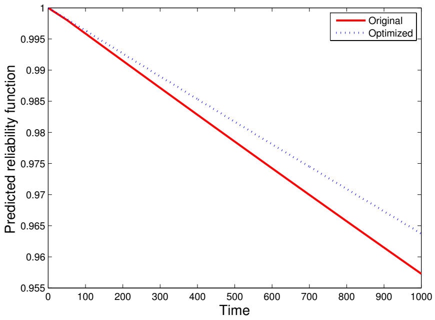

Fig. 9. Reliability functions comparison.

$$H'^0 = \begin{bmatrix} 0.9822 & 0.0017 & 0.0122 & 0.0038 \\ 0.2634 & 0.7366 & 0 & 0 \\ 0.1989 & 0 & 0.8011 & 0 \\ 0.3530 & 0 & 0 & 0.6470 \end{bmatrix}.$$

Compared with H^0, the element on the first row and second column is increased from 0 to 0.0017, a confirmation of increased false alarms. On the other hand, detection delays are reduced approximately from 6 to 1, and system stays less time under mis-matched fault and FDI cases. Overall, MTTF is improved.

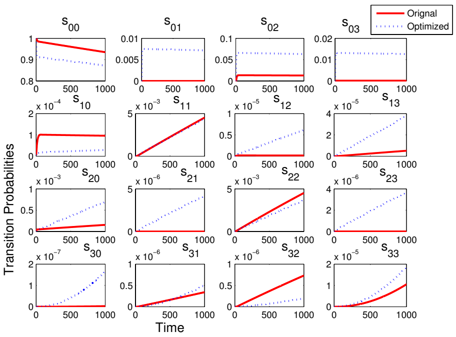

Fig. 10. Comparison of transition probabilities.

This evaluation procedure can be completed in an online manner. Estimated FDI transition parameters H and current mode of ζ_n provided by confirmed test on FDI can be used to provide updated MTTF based on this most recent information.

7. CONCLUSIONS

A reliability monitoring scheme for FTCS's is reported in this paper. The scheme contains two post-processing strategies on FDI results to provide estimated fault mode for control reconfiguration and confirmed mode for updating reliability. The stochastic transitions of FDI mode is represented by a semi-Markov chain with parameters estimated from history data. This scheme provides timely monitoring on the reliability index of FTCS's. However, as a weakness, the proposed scheme has large computation burden. In addition, it is necessary to study the sensitivity of the proposed scheme with respect to the uncertainties in transition parameters of the fault and FDI Markov chains, especially considering the implementation of the scheme to practical systems.

REFERENCES

G. Balas, A. Packard, J. Renfrow, C. Mullaney, & R. M'Closkey, Control of the F-14 aircraft lateral-directional axis during powered approach. *Journal of Guidance, Control, and Dynamics*, 21(6): 899-908, 1998.

V. Barbu, M. Boussemart, & N. Limnios, Discrete-time semi-Markov model for reliability and survival analysis, *Communications in Statistics Theory and Methods*, 33(11): 2833-2868, 2004.

R. Field Jr. & L. Bergman, Reliability-based approach to linear covariance control design, *Journal of Engineering Mechanics*, 124(2): 193-199, 1998.

H. Li & Q. Zhao, Reliability modeling of fault tolerant control systems, *Proc. Joint 44th IEEE Conf. Decision Contr. European Contr. Conf.*, Seville, Spain, page 2397-2402, Dec. 2005.

H. Li & Q. Zhao, Reliability evaluation of fault folerant control with a semi-Markov FDI model, *Proceedings of Mechnical Engineerings Part I - Journal of Systems and Control Engineering*, 220(I5): 329-338, 2006.

J. Song & A.D. Kiureghian, Joint first-passage probability and reliability of systems under stochastic excitation, *Journal of Engineering Mechanics*, 132(1): 65-77, 2006.

B. Walker, Fault tolerant control system reliability and performance prediction using semi-Markov models, Proceedings of Safeprocess, Kingston Upon Hull, UK, 1053-1064, 1997.

N.E. Wu, Coverage in fault-tolerant control, *Automatica*, 40(4): 537-548, 2004.

Y. Zhang & X.R. Li, Detection and diagnosis of sensor and actuator failures using IMM estimator, *IEEE Trans. Aerospace Electronic Systems*, 34(4), 1293-1313, 1998.