Int. J. Appl. Math. Comput. Sci., 2007, Vol. 17, No. 4, 491–504
DOI: 10.2478/v10006-007-0041-0

amcs

RELIABILITY MODELING 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
e-mail: {hongbin,qingzhao}@ece.ualberta.ca

** Department of Computer Science and Engineering, Aalborg University Esbjerg
Niels Bohrs Vej 8, 6700 Esbjerg, Denmark
e-mail: yang@cs.aaue.dk

This paper proposes a novel approach to reliability evaluation for active Fault Tolerant Control Systems (FTCSs). By introducing a reliability index based on the control performance and hard deadline, a semi-Markov process model is proposed to describe system operation for reliability evaluation. The degraded performance of FTCSs in the presence of imperfect Fault Detection and Isolation (FDI) is reflected by semi-Markov states. The semi-Markov kernel, the key parameter of the process, is determined by four probabilistic parameters based on the Markovian model of FTCSs. Computed from the transition probabilities of the semi-Markov process, the reliability index incorporates control objectives, hard deadline, and the effects of imperfect FDI, a suitable quantitative measure of the overall performance.

Keywords: fault tolerant control, reliability evaluation, semi-Markov processes

1. Introduction

In order to meet high reliability requirements of safety-critical processes, major progress has been made in Fault Tolerant Control Systems (FTCSs) (Blanke *et al.*, 2001; Wu and Patton, 2003). FTCSs usually employ Fault Detection and Isolation (FDI) schemes and reconfigurable controllers to accommodate fault effects, also known as active FTCSs (Patton, 1997). As controllers are reconfigured based on FDI results, imperfect detection results caused by modeling uncertainties and disturbances may corrupt stability, performance, and therefore reliability (Mariton, 1989). Some works exist to restore the control performance when considering this FDI imperfectness. For example, Zhang and Jiang (2001) developed an integrated FDI and reconfigurable control approach based on Iteracting Multiple-Model (IMM) Kalman filters and eigenvalue assignments. This approach was then further improved to account for performance degradation under fault occurrences (Jiang and Zhang, 2006). However, it is unknown if the designed system satisfies critical reliability requirements. This is the main motivation behind the current paper.

A quantitative reliability analysis is required for FTCSs in order to verify safety requirements (Blanke, 1996). Moreover, this analysis is a prerequisite to reliability-based controller design. For example, in the reliability-based design of structural control, the key problem is to evaluate the failure probability, a complementary reliability index (Spencer *et al.*, 1994). For Fault Tolerant Control (FTC), improving the system reliability is considered to be the ultimate goal. Thus, the main objective of this paper is to develop a reliability index and its modeling method for active FTCSs.

The reliability of FTCSs has been investigated by using various methods. An ongoing research contribution is made by Wu (Wu, 2001; 2004; Wu and Patton, 2003). In her latest results, reliability was evaluated from a Markov process model built from serial-parallel block diagrams which describe functional relations among subsystems and components. Coverage was used as a link between reliability and control actions. A similar system configuration was deployed by Guenab *et al.* (2005), where reliability was evaluated from serial-parallel structures and optimization was conducted to find the best structure based on the reliability and cost. However, this framework is restricted to those FTCSs that can be described by serial-parallel block diagrams.

Other methods are based on Markov or semi-Markov

reliability modeling. For example, Walker (1997) proposed a semi-Markov model by defining semi-Markov states as the combinations of the status of faults and FDI schemes without considering dynamical relations and control objectives. Walker (1989) and Schrick and Müller (2000) used reliability evaluations from the Markov modeling of FDI to determine the residue threshold of FDI and to compare several sensor fault detection schemes, respectively. Harrison *et al.* (1981) established a similar discrete-time Markov model for a redundant navigator. However, in these Markov or semi-Markov models, the states are all simply defined as the combinations of fault modes and FDI results, in which the role of control in improving the system performance is not considered. Hence, a link between the reliability and the overall control performance of FTCSs is missing.

The latest progresses were reported in an invited session at the SAFEPROCESS conference in 2006, which presented various methods of improving FTCS analysis and design through an integrated reliability index. For example, Guenab *et al.* (2006) developed a reliability-based reconfiguration strategy according to an enumeration of finite system structures. Bonivento *et al.* (2006) proposed a reliability index for a hierarchic diagnostic system from its functional description. Patton *et al.* (2006) used a Monte Carlo simulation technique to design an FDI scheme with high reliability. Wu and Thavamani (2006) presented a simulation study to quantify the performance of a wireless network on the effects of the loop closure frequency and node storage capacity; Figueras *et al.* (2006) discussed a fault diagnosis system design using reliability analysis techniques with application to a practical problem. However, most of these methods are focused on either FDI or reconfigurable control only, while this paper takes into account the interaction effects between these two parts.

This paper proposes a new reliability index and its modeling method. The index incorporates the dynamical characteristics of FTCSs: control objectives, hard deadline, and the effects of imperfect FDI results. Based on the dynamical model of FTCSs, degrading control objectives are set for various fault scenarios, and the reliability is defined as the probability of satisfying degraded objectives, while a temporal violation within a hard deadline is allowed. To evaluate this index, a semi-Markov process is constructed to describe and to predict the control performance evolution due to fault occurrences and imperfect FDI results. The semi-Markov transition probabilities are computed to determine the reliability.

It is worthwhile to point out that this paper presents a part of the authors' work on the analysis and design of FTCSs based on a reliability criterion. The developed reliability index is essentially an off-line criterion and can be used for controller analysis and design. A controller design method was reported in (Li and Zhao, 2007), where a stabilizing controller parameterization and a randomized algorithm are integrated to design a state-feedback controller using the reliability index as an optimization objective. Another related work is an extended reliability analysis framework for a generalized semi-Markov FDI description reported in (Li and Zhao, 2006).

The remainder of this paper is organized as follows: A reliability index is defined in Section 2. The system model and assumptions are given in Section 3. A semi-Markov reliability model is presented in Section 4, and an example is given in Section 5, followed by conclusions in Section 6.

2. Reliability Index

Definition 1. The *reliability function* $R(t)$ of FTCSs is defined as the probability that, during the time interval $[0, t]$, FTCSs either satisfy presumed control objectives or violate them only temporarily for a short time no longer than the presumed hard deadline $T_{\rm hd}$.

A reliability index is introduced in Definition 1 to reflect the following dynamical characteristics of FTCSs:

• *Control objectives*. FTCSs are said to be functional if they satisfy given control objectives. A scalar function $J(t)$ is assumed to represent the control performance at time t, and a small value indicates a good performance. Assume that fault modes are finite, and the performance upper bound for the i-th fault mode is denoted as ρ_i. The control objective is to maintain $J(t) \leq \rho_i$ for each fault mode. More discussions are given in Section 3.2.

• *Hard deadline*. $J(t)$ may exceed ρ_i only temporarily for a short time because of imperfect FDI results and controller reconfigurations, which should be distinguished from a failure. The hard deadline concept proposed in a real-time system analysis is therefore used in Definition 1 (Shin and Kim, 1992). It is assumed that if the violation time is greater than a particular limit $T_{\rm hd}$, the system is generally unable to return to functional states. In this sense, $T_{\rm hd}$ is called the hard deadline of FTCSs.

Let $\zeta(t)$ represent the system fault mode at t. According to Definition 1, $R(t)$ is calculated as

$$R(t) = 1 - \Pr\Big\{\exists t_1, t_2 \in [0,t],\ t_2 - t_1 > T_{\rm hd},\ \forall \tau \in [t_1, t_2],\ J(\tau) > \rho_i,\ i = \zeta(\tau)\Big\}. \quad (1)$$

The reliability evaluation problem is then reduced to developing an approach to calculate $R(t)$. The main idea is to describe the evolution of $J(t)$ using a semi-Markov process and then to calculate $R(t)$ by solving the transition probabilities of the process.

Remark 1. As an overall performance criterion of FTCSs, the reliability function $R(t)$ gives the system survival probability for any operation period up to time t. The plot of calculated $R(t)$ can be deemed as a reliability prediction curve, which can be used to examine a

long-term system reliability behavior during an off-line analysis.

As a function criterion, $R(t)$ is not often used as an objective or a constraint in the design phase. An alternative scalar reliability index, Mean Time To Failure (MTTF), is usually preferable for a controller or a system design purpose, as shown in (Li and Zhao, 2007). It is defined as the expected lifetime of the satisfactory operation:

$$\text{MTTF} = \int_0^\infty R(t)\,\mathrm{d}t.$$

Both $R(t)$ and MTTF can be calculated from a semi-Markov process $X(t)$ constructed in the following sections. These criteria and the evaluation method lay the foundation for the system analysis and design from a reliability perspective.

3. System Modeling

3.1. Markovian Model. To address the effects of imperfect FDI results, Markovian models are used to study the reliability evaluation problem for given FTCSs. Although the Markovian modeling of FDI may be restrictive, the influence of FDI imperfectness is directly tackled in this model (Mariton, 1989; Srichander and Walker, 1993; Mahmoud *et al.*, 2003).

Consider the following nominal linear Markovian model of FTCSs:

$$\mathcal{M}: \begin{cases} \dot{x}(t) = A(\zeta(t))x(t) + B_1(\zeta(t))w(t) \\ \qquad\quad +B_2(\zeta(t))u(\eta(t),t), \\ z(t) = C_1(\zeta(t))x(t) + D_{11}(\zeta(t))w(t) \\ \qquad\quad +D_{12}(\zeta(t))u(\eta(t),t), \\ y(t) = C_2(\zeta(t))x(t) + D_{21}(\zeta(t))w(t) \\ \qquad\quad +D_{22}(\zeta(t))u(\eta(t),t), \end{cases} \tag{2}$$

where $x(t) \in \mathbb{R}^n, u(\eta(t),t) \in \mathbb{R}^m$, $w(t) \in \mathbb{R}^h$, $z(t) \in \mathbb{R}^p$, and $y(t) \in \mathbb{R}^l$ denote the system state, control input, exogenous input, controlled output, and measured output, respectively, and $\mathbb{R}^n$ denotes the n-dimensional real vector space. Here $\zeta(t)$ and $\eta(t)$ are assumed to be two separate continuous-time Markov processes. $A(\zeta(t))$, $B_1(\zeta(t))$, $B_2(\zeta(t))$, $C_1(\zeta(t))$, $C_2(\zeta(t))$, $D_{11}(\zeta(t))$, $D_{12}(\zeta(t))$, $D_{21}(\zeta(t))$, and $D_{22}(\zeta(t))$ are system matrices with compatible dimensions.

According to a probabilistic robustness analysis (Tempo *et al.*, 1997), the modeled uncertainties in (2) are assumed to have known probability distributions in bounded sets without specific structures. For example, they can be uncertain matrices additive to system matrices or uncertain transfer functions multiplicative to the nominal model.

The system in (2) can be viewed as a hybrid dynamical system including both continuous states and discrete modes (Mariton, 1989). The discrete modes, also referred to as system regimes, are represented by $\zeta(t)$ and $\eta(t)$ subjected to the stochastic evolution, and the dynamics of continuous-state $x(t)$ are described by linear state space equations, denoted by $\mathcal{M}(\zeta(t),\eta(t))$, for the corresponding system regimes.

Here $\zeta(t)$ is assumed to be a homogeneous Markov process with a finite state space $S_1 = \{0, 1, \ldots, N_1\}$ to describe system fault modes, $N_1 \in \mathbb{N}$. $\mathbb{N}$ denotes the set of nonnegative integers. The transition probability from mode i to j, $i, j \in S_1$, in the infinitesimal time interval of $\triangle t$ is given by

$$\zeta(t) : p_{ij}(\triangle t) = \begin{cases} \alpha_{ij}\triangle t + o(\triangle t), & i \neq j, \\ 1 - \alpha_{ii}\triangle t + o(\triangle t), & i = j, \end{cases}$$

where $\alpha_{ij},\ \alpha_{ii} \geq 0$ are the transition rates of $\zeta(t)$, and $o(\triangle t)$ denotes high order infinitesimal terms.

Moreover, $\eta(t)$ is assumed to be a conditionally Markov process with a finite state space $S_2 = \{0, 1, \ldots, N_2\}$ to describe FDI results, $N_2 \in \mathbb{N}$. When $\zeta(t) = k,\ k \in S_1$, the transition probability from mode i to j, $i, j \in S_2$, in $\triangle t$ is given by

$$\eta(t) : p_{ij}^k(\triangle t) = \begin{cases} \beta_{ij}^k\triangle t + o(\triangle t), & i \neq j, \\ 1 - \beta_{ii}^k\triangle t + o(\triangle t), & i = j, \end{cases}$$

where $\beta_{ij}^k,\ \beta_{ii}^k \geq 0$ represent the transition rates of $\eta(t)$ given $\zeta(t) = k$. These transition rates compose the generator matrices of $\zeta(t)$ and $\eta(t)$, denoted by, $G = [\pm\alpha_{ij}]_{N_1\times N_1}$ and $H^k = [\pm\beta_{ij}^k]_{N_2\times N_2}$, respectively, where the negative sign is taken when $i = j$.

In this Markovian model, the stochastic behaviors of FDI and fault modes are described by two Markov processes, and incorrect fault detection results are represented by mismatched modes between $\zeta(t)$ and $\eta(t)$. Therefore, the fault diagnosis quality can be obtained by examining the transition parameters of these two Markov processes, as demonstrated by the probabilistic parameters in Section 4.2.

3.2. Assumptions. The assumptions made in this paper are as follows:

Assumption 1. For fixed system regimes $\zeta(t)$ and $\eta(t)$, (2) is reduced to a linear system model $\mathcal{M}(\zeta(t),\eta(t))$. It is assumed that the control performance of $\mathcal{M}(\zeta(t),\eta(t))$ can be represented by a model-based static performance measure $\mu(\cdot)$.

"Static" means that $\mu(\cdot)$ depends on the system model only, but not on the system state trajectory $x(t)$, nor the output response $y(t)$. Essentially, this model-based static performance represents an average measure of how the system behaves in a particular regime. This

assumption is made mainly because of the fact that a reliability index mainly concerns a long-term behavior. An average performance measure is therefore more suitable for reliability analysis. For example, $\mu(\cdot)$ can be defined as $\|G_{zw}(\zeta(t), \eta(t), s)\|$, the system norm of the transfer function from w to z of the regime model, such as H_∞ and H_2 norms. With the development of robust and optimal control, system norms represent a widely-used static model-based index and have become a standard performance criterion. They can be used to describe general control objectives including trajectory tracking, disturbance attenuation, model matching, output variance when considering Gaussian disturbances, etc. As a practical example, Balas *et al.* (1998) used the H_∞ norm to describe a handling quality control problem in an aircraft. What is more, $\mu(\cdot)$ can also be defined as a stability criterion and other model-based control objectives.

In the design of active FTCSs, the performance index is often defined on system states or trajectories. For example, the performance measure is defined as a moving average of the norm of filter residual vectors in (Zhang and Jiang, 2001), and an average tracking error is used in (Jiang and Zhang, 2006). These criteria provide information for a reliable fault diagnosis and transient performance of the controller reconfiguration, which are suitable for the integrated design of FTCSs using IMM methods. In general, these time-varying control objectives depending on the system state or trajectory are not applicable to $\mu(\cdot)$, except for those that can be directly calculated based on a system model, such as the guaranteed cost control (Polyak and Tempo, 2001). If the time-varying control objectives are to maintain the system trajectory within a safety region under a Gaussian noise disturbance, the methods presented in Spencer *et al.* (1994) can be used instead to estimate the probabilistic performance for reliability evaluation. The performance value $J(t)$ is calculated as $\mu(\mathcal{M}(\zeta(t), \eta(t)))$. Based on Assumption 1, $\mu(\mathcal{M}(\zeta(t), \eta(t)))$ is a constant for fixed $\zeta(t)$ and $\eta(t)$. Abusing the notation, we use $J(\zeta(t), \eta(t)) \triangleq \mu(\mathcal{M}(\zeta(t), \eta(t)))$ to denote the dependence of this performance value on system regimes.

Assumption 2. The probability distribution of $\eta(t)$ can be approximated by its stationary distribution.

This assumption is a result of the limiting probability theory of Markov processes (Çinlar, 1975). Considering the meanings of $\zeta(t)$ and $\eta(t)$, the transition rates of $\eta(t)$ represent how fast FDI modes change for a particular fault mode while those of $\zeta(t)$ describe how frequently faults occur. As fault occurrences are often rare in practice, the transition rates of $\zeta(t)$ are usually in a smaller order than those of $\eta(t)$. Accordingly, the time for FDI to approach its stationary distribution is much shorter than the mean time of fault occurrences, and this assumption is therefore made.

4. Semi–Markov Process Model for Reliability Evaluation

A semi-Markov process, denoted by $X(t)$, is used as an intermediate model between FTCSs and the reliability index. It is constructed based on probabilistic parameters obtained from the dynamical model (2), and its transition probabilities are used to compute the reliability index $R(t)$ in (1).

4.1. State Definitions. Two state transition diagrams are shown in Fig. 1, where Fig. 1(a) is for the case of two fault modes $\{0,\ 1\}$, and Fig. 1(b) four fault modes $\{0,\ 1,\ 2,\ 3\}$ (in which the self-transitions of each state are not shown for the sake of brevity). $X(t)$ has five states in Fig. 1(a), denoted by $S_{\rm r} = \{0_{\rm N},\ 0_{\rm F},\ 1_{\rm N},\ 1_{\rm F},\ {\rm F}\}$, and nine states in Fig. 1(b): 'F' represents the unique absorbing failure state, and functional states are represented by a pair with a number and a letter in the subscript. The number represents a fault mode, the letter 'N' indicates a satisfactory performance, and 'F' an unsatisfactory performance but within the hard deadline. For $i \in S_1$, $i_{\rm N}$ and $i_{\rm F}$ are defined as

$$\begin{aligned} i_{\rm N}:\ &\{\zeta(t) = i,\ J(i,\ \eta(t)) \le \rho_i\},\\ i_{\rm F}:\ &\{\zeta(t) = i,\ J(i,\ \eta(t)) > \rho_i,\ \tau \le T_{\rm hd})\}, \end{aligned} \quad (3)$$

where τ denotes the sojourn time at $i_{\rm F}$. Each state of $X(t)$ indicates a fault mode and whether or not the control objective is satisfied. By studying the state transitions of $X(t)$, the performance evolution and reliability can be analyzed.

4.2. Probabilistic Parameters. Considering modeling uncertainties, the control performance can be given in terms of a classical worst-case measure for robustness but it may lead to a conservative result. In contrast, the probabilistic robustness analysis assumes a probability distribution of parametric uncertainties and evaluates the probability of satisfying a specific performance using randomized algorithms (Tempo *et al.*, 1997). This alternative criterion has a clear meaning in practice where the required performance objectives are always associated with certain minimum probability levels (Yaesh *et al.*, 2003). Based this idea, the following parameter is defined:

Definition 2. For a particular fault mode and FDI mode, the probability that the system is functional is defined as

$$\begin{aligned} \gamma_{ij} &\triangleq \Pr\{J(\zeta(t),\ \eta(t)) \le \rho_i | \zeta(t) = i,\ \eta(t) = j\}\\ &= \Pr\{J(i,j) \le \rho_i\} = \Pr\{\mu(\mathcal{M}(i,j)) \le \rho_i\},\\ &\qquad\qquad i \in S_1,\ \ j \in S_2. \end{aligned}$$

Here γ_{ij} is the probabilistic performance when the fault mode is i and the FDI mode is j. Based on Assumption 1, γ_{ij} can be estimated using a randomized algorithm

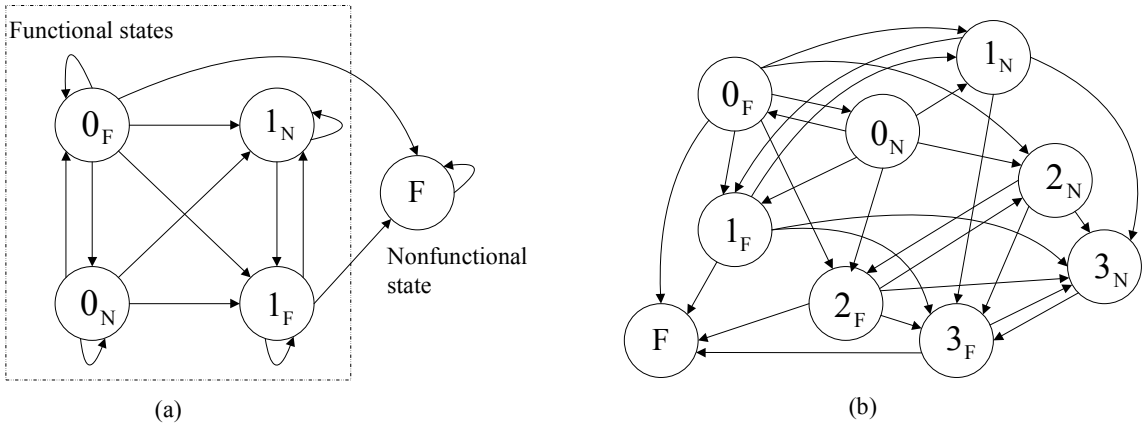

Fig. 1. State transition diagram of $X(t)$: (a) two fault modes; (b) four fault modes.

given by Tempo *et al.* (1997). This algorithm is essentially a Monte Carlo simulation, and γ_{ij} is estimated by an empirical probability. The estimation accuracy can be quantified based on the number of generated uncertainty samples.

Remark 2. Note that γ_{ij} is a key parameter relating the control performance of a particular system regime and the reliability of FTCSs. It demonstrates the influence of system dynamics and controllers on the reliability index $R(t)$.

Definition 3. For a particular fault mode, the *stationary distribution* of the FDI mode is defined as

$$\pi_j^i \triangleq \lim_{t\to\infty} \Pr\{\eta(t) = j|\zeta(t) = i\},\ \ i \in S_1,\ \ j \in S_2.$$

Here π_j^i can be calculated based on the generator matrix of $\eta(t)$ when $\zeta(t) = i$ (Çinlar, 1975, p. 265). Based on Assumption 2, π_j^i is used to approximate the following probability:

$$\Pr\{\eta(t) = j|\zeta(t) = i\} \approx \pi_j^i,\ \ i \in S_1,\ \ j \in S_2. \quad (4)$$

Remark 3. π_j^i reflects the detection precision of FDI and gives a probabilistic measure of its imperfectness. In the ideal case of a perfect FDI detection, $\pi_j^i = 0$ when $i \neq j$ and $\pi_i^i = 1$. Since π_j^i is the stationary distribution of the Markov process $\eta(t)$, it can be calculated by using a standard method in Markov theory, which involves only simple matrix operations on the generator of $\eta(t)$ (Çinlar, 1975, p. 265).

Definition 4. Given $X(t) = i_{\mathrm{N}}$, $i \in S_1$, the stationary probability that the FDI process equals a specific mode is defined as

$$w_j^i \triangleq \lim_{t\to\infty} \Pr\{\eta(t) = j|X(t) = i_{\mathrm{N}}\},\ \ i \in S_1,\ \ j \in S_2.$$

Here w_j^i can be computed based on Bayes' formula as shown below in the example of w_0^0 in the case of $S_2 = \{0,\ 1\}$. If γ_{00} and γ_{01} are not simultaneously zero, then w_0^0 is given by Eqn. (5).

Since all cases of $\eta(t) = k$ form a partition of the event space, $k \in S_2$, Bayes' formula is used in the second line of (5), where the conditional probability is converted to known mariginal and other conditional probabilities. If $\gamma_{00} = \gamma_{01} = 0$, w_0^0 is defined as π_0^0. The calculation procedures are similar for other values of i and j.

Definition 5. Given $X(t) = i_{\mathrm{F}}$, $i \in S_1$, the stationary probability that the FDI process equals a specific mode is defined as

$$v_j^i \triangleq \lim_{t\to\infty} \Pr\{\eta(t) = j|X(t) = i_{\mathrm{F}}\},\ \ i \in S_1,\ \ j \in S_2.$$

Note that v_j^i can be calculated in a much the same way as w_j^i.

Based on Assumption 2 and (4), w_j^i and v_j^i are used to approximate the following probabilities:

$$\begin{aligned}&\Pr\{\eta(t) = j|X(t) = i_{\mathrm{N}}\} \approx w_j^i,\\ &\Pr\{\eta(t) = j|X(t) = i_{\mathrm{F}}\} \approx v_j^i,\ \ i \in S_1,\ \ j \in S_2. \quad (6)\end{aligned}$$

Remark 4. Note that w_j^i and v_j^i are probabilistic estimates of FDI modes given the states of $X(t)$, and determined by the control performance of each system regime and FDI imperfectness parameters, represented by γ_{ij} and π_j^i, respectively.

4.3. Semi–Markov Kernel. The associated Markov-renewal process of $X(t)$ is denoted by $(Y_n,\ T_n,\ n \in \mathbb{N})$. Y_n denotes the so-called embedded Markov chain, which gives the state sequence visited by $X(t)$ consecutively, and T_n the transition time. The semi-Markov kernel of $X(t)$ is denoted by a matrix function Q, and its elements give one-step transition probabilities. For example,

$$
\begin{aligned}
w_0^0 &= \lim_{t\to\infty} \Pr\{\eta(t)=0|X(t)=0_{\mathrm{N}}\} \\
&= \lim_{t\to\infty} \Pr\{\eta(t)=0|\zeta(t)=0,\ J(0,\eta(t))\le\rho_0\} \\
&= \lim_{t\to\infty} \frac{\Pr\{J(t)\le\rho_0|\eta(t)=0,\ \zeta(t)=0\}\Pr\{\eta(t)=0,\ \zeta(t)=0\}}{\sum_{k\in S_2}\Pr\{J(t)\le\rho_0|\eta(t)=k,\ \zeta(t)=0\}\Pr\{\eta(t)=k,\ \zeta(t)=0\}} \\
&= \lim_{t\to\infty} \frac{\Pr\{J(0,\eta(t))\le\rho_0|\eta(t)=0\}\Pr\{\eta(t)=0|\zeta(t)=0\}\Pr\{\zeta(t)=0\}}{\sum_{k\in S_2}\Pr\{J(0,\eta(t))\le\rho_0|\eta(t)=k\}\Pr\{\eta(t)=k|\zeta(t)=0\}\Pr\{\zeta(t)=0\}} \\
&= \lim_{t\to\infty} \frac{\Pr\{J(t)\le\rho_0|\eta(t)=0,\ \zeta(t)=0\}\Pr\{\eta(t)=0|\zeta(t)=0\}}{\sum_{k\in S_2}\Pr\{J(t)\le\rho_0|\eta(t)=k,\ \zeta(t)=0\}\Pr\{\eta(t)=k|\zeta(t)=0\}} \\
&= \frac{\Pr\{J(0,0)\le\rho_0\}\lim_{t\to\infty}\Pr\{\eta(t)=0|\zeta(t)=0\}}{\sum_{k\in S_2}\Pr\{J(0,k)\le\rho_0\}\lim_{t\to\infty}\Pr\{\eta(t)=k|\zeta(t)=0\}} \\
&= \frac{\gamma_{00}\pi_0^0}{\gamma_{00}\pi_0^0+\gamma_{01}\pi_1^0}.
\end{aligned}
\tag{5}
$$

$Q(i_{\mathrm{N}},\ j_{\mathrm{N}},\ t)$ is defined by the following equation, where $i_{\mathrm{N}}, j_{\mathrm{N}} \in S_{\mathrm{r}}, t \in \mathbb{R}, t \ge 0$:

$$
\begin{aligned}
&Q(i_{\mathrm{N}},\ j_{\mathrm{N}},\ t) \\
&\quad \triangleq \Pr\Big\{Y_{n+1}=j_{\mathrm{N}},\ T_{n+1}-T_n\le t|Y_n=i_{\mathrm{N}}\Big\},
\end{aligned}
$$

which represents the probability of transiting from i_{N} to j_{N} in one step with sojourn time $T_{n+1}-T_n$ no greater than t (Çinlar, 1975).

According to Assumption 1, the state transitions of $X(t)$ are triggered by the mode changes of $\zeta(t)$ or $\eta(t)$, implying that faults, FDI decisions, and controller reconfigurations have major effects on the system performance and reliability. Hence the semi-Markov kernel Q is essential for reliability evaluation. By taking the transition of $X(t)$ from 0_{N} in Fig. 1(a) as an example, the main steps of calculating Q are listed as follows and illustrated in Fig. 2:

1) The FDI mode $\eta(t)$ before a transition is estimated using w_j^i or v_j^i based on the state of $X(t)$.

2) Competition between $\zeta(t)$ and $\eta(t)$. The process that jumps first determines possible transitional destination states. For example, if $\zeta(t)$ jumps before $\eta(t)$, the destination state is 1_{N} or 1_{F}; otherwise, 0_{N} or 0_{F}. This competition probability can be calculated using a property of exponential distributions.

3) The probability of satisfying control objectives at destination states is calculated by using γ_{ij}.

4) By combining previous steps, the transition probability is calculated using the total probability formula.

The property of exponential distributions mentioned in Step 2 is given as follows (Ross 2002, Chapter 5):

Let $X_1,\dots,X_n$ be independent random variables, with X_i following an exponential distribution with the parameter λ_i, $i = 1 \sim n$. Then the distribution of $\min(X_1,\dots,X_n)$ is still exponentially distributed with the parameter $(\lambda_1+\cdots+\lambda_n)$, and the probability of X_i being the minimum is $\lambda_i/(\lambda_1+\cdots+\lambda_n)$, $i = 1 \sim n$.

For example, suppose that $\zeta(t)=0$ and $\eta(t)=0$ before the transition. Let τ_ζ denote the sojourn time of $\zeta(t)$, and τ_η the sojourn time of $\eta(t)$. Because of Markov process theory, τ_ζ and τ_η are exponentially distributed with parameters given in the generator matrix:

$$
\begin{aligned}
\Pr\{\tau_\zeta\le t\} &= 1-e^{-\alpha_{00}t}, \\
\Pr\{\tau_\eta\le t\} &= 1-e^{-\beta_{00}^0 t}.
\end{aligned}
$$

Based on the above property,

$$
\begin{aligned}
\Pr\{\min(\tau_\zeta,\tau_\eta)\le t\} &= 1-e^{-(\alpha_{00}+\beta_{00}^0)t}, \\
\Pr\{\tau_\zeta<\tau_\eta\} &= \frac{\alpha_{00}}{\alpha_{00}+\beta_{00}^0}, \\
\Pr\{\tau_\eta<\tau_\zeta\} &= \frac{\beta_{00}^0}{\alpha_{00}+\beta_{00}^0}.
\end{aligned}
$$

The event $\tau_\zeta<\tau_\eta$ corresponds to $\zeta(t)$ transits before $\eta(t)$, and $\tau_\eta<\tau_\zeta$ means $\eta(t)$ transits first. This event appears to be a competition between two processes, and therefore the term competition probability is used. The above three probabilities determine the competition result and are used in calculating transition probabilities to different destination states, as shown in (15) in the proof of Theorem 1.

Following a similar idea shown in Fig. 2, the general results on calculating the semi-Markov kernel are given as follows:

Theorem 1. *The semi-Markov kernel of $X(t)$ can be calculated by the following equations:*

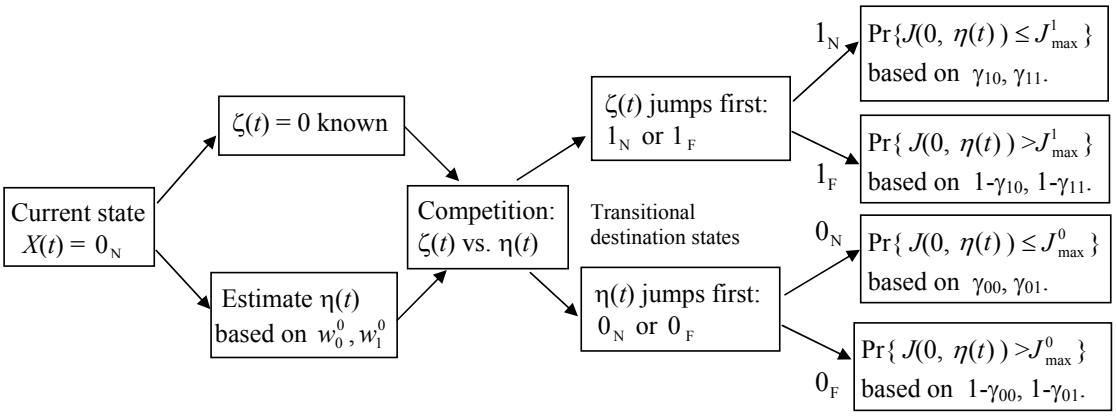

Fig. 2. Calculation procedure of the semi-Markov kernel.

$$Q(i_{\mathrm{N}},\, j_{\mathrm{N}},\, t) = \begin{cases} \sum\limits_{k\in S_2} w_k^i \sum\limits_{l\in S_2\backslash k} \dfrac{\beta_{kl}^i}{\alpha_{ii}+\beta_{kk}^i}(1-e^{-(\alpha_{ii}+\beta_{kk}^i)t})\gamma_{il}, \\ \qquad j=i, \\ \sum\limits_{k\in S_2} w_k^i \dfrac{\alpha_{ij}}{\alpha_{ii}+\beta_{kk}^i}(1-e^{-(\alpha_{ii}+\beta_{kk}^i)t})\gamma_{jk}, \\ \qquad j\in S_1\backslash i, \end{cases} \tag{7}$$

$$Q(i_{\mathrm{N}},\, j_{\mathrm{F}},\, t) = \begin{cases} \sum\limits_{k\in S_2} w_k^i \sum\limits_{l\in S_2\backslash k} \dfrac{\beta_{kl}^i}{\alpha_{ii}+\beta_{kk}^i}(1-e^{-(\alpha_{ii}+\beta_{kk}^i)t}) \\ \times(1-\gamma_{il}), \qquad j=i, \\ \sum\limits_{k\in S_2} w_k^i \dfrac{\alpha_{ij}}{\alpha_{ii}+\beta_{kk}^i}(1-e^{-(\alpha_{ii}+\beta_{kk}^i)t}) \\ \times(1-\gamma_{jk}), \qquad j\in S_1\backslash i, \end{cases} \tag{8}$$

$$Q(i_{\mathrm{F}},\, j_{\mathrm{N}},\, t) = \begin{cases} \sum\limits_{k\in S_2} v_k^i \sum\limits_{l\in S_2\backslash k} \dfrac{\beta_{kl}^i}{\alpha_{ii}+\beta_{kk}^i} \\ \times(1-e^{-(\alpha_{ii}+\beta_{kk}^i)\min(t,T_{\mathrm{hd}})})\gamma_{il}, \quad j=i, \\ \sum\limits_{k\in S_2} v_k^i \dfrac{\alpha_{ij}}{\alpha_{ii}+\beta_{kk}^i} \\ \times(1-e^{-(\alpha_{ii}+\beta_{kk}^i)\min(t,T_{\mathrm{hd}})})\gamma_{jk}, \quad j\in S_1\backslash i, \end{cases} \tag{9}$$

$$Q(i_{\mathrm{F}},\, j_{\mathrm{F}},\, t) = \begin{cases} \sum\limits_{k\in S_2} v_k^i \sum\limits_{l\in S_2\backslash k} \dfrac{\beta_{kl}^i}{\alpha_{ii}+\beta_{kk}^i} \\ \times(1-e^{-(\alpha_{ii}+\beta_{kk}^i)\min(t,T_{\mathrm{hd}})})(1-\gamma_{il}), \\ \qquad j=i, \\ \sum\limits_{k\in S_2} v_k^i \dfrac{\alpha_{ij}}{\alpha_{ii}+\beta_{kk}^i} \\ \quad \times(1-e^{-(\alpha_{ii}+\beta_{kk}^i)\min(t,T_{\mathrm{hd}})})(1-\gamma_{jk}), \\ \qquad j\in S_1\backslash i, \end{cases} \tag{10}$$

$$Q(i_{\mathrm{F}},\, \mathrm{F},\, t) = \mathbf{1}_{\{t>T_{\mathrm{hd}}\}}\Big(1-\sum_{j\in S_1}(Q(i_{\mathrm{F}},\, j_{\mathrm{N}},\, T_{\mathrm{hd}}) + Q(i_{\mathrm{F}},\, j_F,\, T_{\mathrm{hd}}))\Big), \tag{11}$$

$$Q(F,\, \mathrm{F},\, t) = 1,\ \ Q(F,\, j_N,\, t) = Q(F,\, j_F,\, t) = 0, \quad j\in S_1, \tag{12}$$

where $t>0$, $i,j\in S_1$, $S_2\backslash k \triangleq \{a|a\in S_2,\ a\neq k\}$, and $S_1\backslash i \triangleq \{b|b\in S_1,\ b\neq i\}$. S_1, S_2, and S_r denote the state spaces of $\zeta(t)$, $\eta(t)$, and $X(t)$, respectively. The indicator function $\mathbf{1}_{\{t>T_{\mathrm{hd}}\}}=1$ if $t>T_{\mathrm{hd}}$; otherwise, $\mathbf{1}_{\{t>T_{\mathrm{hd}}\}}=0$.

Proof. By applying the total probability formula and conditioning the probability on FDI modes, the first case of (7) can be decomposed into three parts as shown in the following equation, where (Y_n, T_n) denotes the associated Markov renewal process of $X(t)$:

$$\begin{aligned} &Q(i_{\mathrm{N}},\, i_{\mathrm{N}},\, t) \\ &\triangleq \Pr\{Y_{n+1}=i_{\mathrm{N}},\, T_{n+1}-T_n\le t|Y_n=i_{\mathrm{N}}\} \\ &=\sum_{k\in S_2}\Pr\{\eta(T_n)=k|Y_n=i_{\mathrm{N}}\} \\ &\quad\times\Pr\{Y_{n+1}=i_{\mathrm{N}},\, T_{n+1}-T_n\le t|Y_n=i_{\mathrm{N}},\, \eta(T_n)=k\} \\ &=\sum_{k\in S_2}\Pr\{\eta(T_n)=k|Y_n=i_{\mathrm{N}}\} \\ &\quad\times\Pr\{J(i,\eta(T_{n+1}))\le\rho_i,\, \zeta(T_{n+1})=i, \\ &T_{n+1}-T_n\le t|Y_n=i_{\mathrm{N}},\, \eta(T_n)=k\} \\ &=\sum_{k\in S_2}\Pr\{\eta(T_n)=k|Y_n=i_{\mathrm{N}}\}\sum_{l\in S_2\backslash k}\Pr\{\zeta(T_{n+1})=i, \\ &\eta(T_{n+1})=l, T_{n+1}-T_n\le t|Y_n=i_{\mathrm{N}}\,\eta(T_n)=k\}, \\ &\times\Pr\{J(i,\, \eta(T_{n+1}))\le\rho_i|\zeta(T_{n+1})=i,\, \eta(T_{n+1})=l, \\ &T_{n+1}-T_n\le t, Y_n=i_{\mathrm{N}},\, \eta(T_n)=k\} \\ &=\sum_{k\in S_2}\Pr\{\eta(T_n)=k|Y_n=i_{\mathrm{N}}\} \\ &\quad\sum_{l\in S_2\backslash k}\Pr\{\zeta(T_{n+1})=i,\eta(T_{n+1})=l, \end{aligned}$$

$$T_{n+1} - T_n \le t | \zeta(T_n) = i,\ \eta(T_n) = k\}$$
$$\times \Pr\{J(i,\ l) \le \rho_i\}. \quad (13)$$

The first and last terms in (13) can be approximated by the corresponding stationary probabilities:

$$\Pr\{\eta(T_n) = k | Y_n = i_{\rm N}\} \approx w_k^i,$$
$$\Pr\{J(i,\ l) \le \rho_i\} \approx \gamma_{il}. \quad (14)$$

The second term in (13) is equal to the competition probability:

$$\Pr\Big\{\zeta(T_{n+1}) = i,\ \eta(T_{n+1}) = l,$$
$$T_{n+1} - T_n \le t | \zeta(T_n) = i,\ \eta(T_n) = k\Big\}$$
$$= \frac{\beta_{kl}^i}{\alpha_{ii} + \beta_{kk}^i}(1 - e^{-(\alpha_{ii}+\beta_{kk}^i)t}). \quad (15)$$

Substitute (14) and (15) into (13), and the first case of (7) follows. The second case of (7) can be proved in a similar procedure considering that the mode of $\zeta(t)$ changes instead and the derivation is given as follows:

$$\begin{aligned}
&Q(i_{\rm N},\ j_{\rm N},\ t)\\
&\triangleq \Pr\{Y_{n+1} = j_{\rm N},\ T_{n+1} - T_n \le t | Y_n = i_{\rm N}\}\\
&= \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\rm N}\}\\
&\quad \times \Pr\{J(j, \eta(T_{n+1})) \le \rho_j,\ \zeta(T_{n+1}) = j,\\
&\qquad T_{n+1} - T_n \le t | Y_n = i_{\rm N}, \eta(T_n) = k\}\\
&= \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\rm N}\} \Pr\{\zeta(T_{n+1}) = j,\\
&\quad \eta(T_{n+1}) = k,\ T_{n+1} - T_n \le t | Y_n = i_{\rm N},\ \eta(T_n) = k\}\\
&\quad \times \Pr\{J(j,\ \eta(T_{n+1})) \le \rho_j | \zeta(T_{n+1}) = j,\\
&\quad \eta(T_{n+1}) = k, T_{n+1} - T_n \le t,\ Y_n = i_{\rm N},\ \eta(T_n) = k\}\\
&= \sum_{k \in S_2} \Pr\{\eta(T_n) = k | Y_n = i_{\rm N}\} \Pr\{\zeta(T_{n+1}) = j,\\
&\quad \eta(T_{n+1}) = k,\ T_{n+1} - T_n \le t | \zeta(T_n) = i_{\rm N},\\
&\quad \eta(T_n) = k\} \Pr\{J(j,\ k) \le \rho_j\}\\
&= \sum_{k \in S_2} w_k^i \frac{\alpha_{ij}}{\alpha_{ii} + \beta_{kk}^i}(1 - e^{-(\alpha_{ii}+\beta_{kk}^i)t})\gamma_{jk},\\
&\qquad\qquad j \in S_1 \backslash i. \quad (16)
\end{aligned}$$

The proof of (8) is similar and the details are omitted.

For (9) and (11), $X(t)$ transits from $i_{\rm F}$, and these probabilities depend on $T_{\rm hd}$. If $t \le T_{\rm hd}$, they can be calculated in a similar way as in the case of $i_{\rm N}$. If $t > T_{\rm hd}$, $Q(i_{\rm F},\ j_{\rm N},\ t)$ and $Q(i_{\rm F},\ j_{\rm F},\ t)$ maintain the constant values of $Q(i_{\rm F},\ j_{\rm N},\ T_{\rm hd})$ and $Q(i_{\rm F},\ j_{\rm F},\ T_{\rm hd})$, respectively, while $X(t)$ transits to F. Therefore, (9) and (10) have similar expressions to (7) and (8) with t replaced by $\min(t, T_{\rm hd})$ (Ciardo *et al.*, 1990). $Q(i_{\rm F},\ {\rm F},\ t)$ becomes nonzero only if $t > T_{\rm hd}$, and it is complementary to the transition probability from $i_{\rm F}$ to other states within $T_{\rm hd}$. The indicator function $\mathbf{1}_{\{t>T_{\rm hd}\}}$ describes this behavior, and (11) follows. (12) is obvious considering that F is absorbing. ■

In the above derivation, each element of the semi-Markov kernel is decomposed into three parts: FDI mode estimation, competition probability, and probabilistic performance estimation, and each part can be approximated or calculated using the probabilistic parameters. The effects of the hard deadline are described by $\min(t, T_{\rm hd})$ and $\mathbf{1}_{\{t>T_{\rm hd}\}}$.

Once the semi-Markov kernel is established, $R(t)$ and other reliability criteria, such as MTTF, are readily computed (Limnios and Oprisan, 2001). Since the state F is absorbing, if the initial state is $0_{\rm N}$, the reliability function $R(t) = 1 - P(0_{\rm N},\ {\rm F},\ t)$, where the transition probability function from $0_{\rm N}$ to F is denoted by $P(0_{\rm N},\ {\rm F},\ t) \triangleq \Pr\{X(t) = {\rm F} | X(0) = 0_{\rm N}\}$. Compared with $Q(0_{\rm N},\ {\rm F},\ t)$, $P(0_{\rm N},\ {\rm F},\ t)$ may involve multiple transitions but $Q(0_{\rm N},\ {\rm F},\ t)$ is for one transition only.

The main procedure of evaluating the reliability for FTCSs is summarized as follows:

1) Given the Markovian model (2) of FTCSs, the states of $X(t)$ are defined as in Section 4.1.

2) Continuous-state dynamics analysis. For fixed $\zeta(t)$ and $\eta(t)$, the system in (2) is reduced to $\mathcal{M}(\zeta(t), \eta(t))$, and the robust control performance of this regime model under probabilistic uncertainties is represented by a probabilistic parameter γ_{ij} in Definition 2.

3) Discrete-mode dynamics analysis. FDI imperfectness and its relations with the states of $X(t)$ are described by the probabilistic parameters in Definitions 3–5.

4) The continuous-state and discrete-mode dynamics are combined to construct the semi-Markov kernel of $X(t)$ using Theorem 1, and $R(t)$ is calculated by solving the transition probabilities of $X(t)$.

5. Illustrative Example

A control problem of an F-14 aircraft was presented by Balas *et al.* (1998), and also used as a demonstration example in the MATLAB® Robust Control Toolbox[1]. This problem concerns the design of a lateral-directional axis controller during a powered approach to a carrier landing with two command inputs from the pilot: a lateral stick and a rudder pedal. At an angle-of-attack of 10.5 degrees and an airspeed of 140 knots, the nominal linearized F-14 model has four states: lateral velocity, yaw rate, roll

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

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. These variables are related by the following state-space equations:

$$\dot{x}_{\text{F14}} = A_{\text{F14}}x_{\text{F14}} + B_{\text{F14}}u_{\text{F14}},$$
$$y_{\text{F14}} = C_{\text{F14}}x_{\text{F14}} + D_{\text{F14}}u_{\text{F14}},$$

where $x_{\text{F14}} = [v\ r\ p\ \phi]^T,\ u_{\text{F14}} = [\delta_{\text{dstab}}\ \delta_{\text{rud}}]^T,\ y_{\text{F14}} = [\beta\ p\ r\ y_{\text{ac}}]^T$, and numerical values are given by (17).

The control objectives are to have handling quality (HQ) responses from the lateral stick to the roll rate p and from the rudder pedal to the side-slip angle θ match the first- and second-order responses

$$5\frac{2}{s+2}, \quad -2.5\frac{1.25^2}{s+2.5s+1.25^2},$$

respectively.

The system block diagram is shown in Fig. 3, where F-14_{nom} represents the nominal linearized F-14 model, and A_S and A_R actuator models. Here e_p and e_β represent the weighted model matching errors. The actuator energy is described by e_{act}, and noise is added to the measured output after anti-aliasing filters. ΔG and W_{in} represent the multiplicative uncertainty and its weighting function, respectively. The transfer function ΔG is assumed to be stable and unknown, except for being uniformly distributed within the norm-bounded set of $\|\Delta G\|_\infty \le 1$.

By incorporating performance weighting functions, W_{act}, W_n, W_p, and W_β, a generalized plant with the 26th order can be constructed from Fig. 3, corresponding to the nominal fault-free regime model $\mathcal{M}(\zeta(t),\ \eta(t))$ in (2) for $\zeta(t) = \eta(t) = 0$. The control objectives are converted to the closed-loop H_∞ norm, $\|G_{zw}(\zeta(t), \eta(t), s)\|_\infty$, where w is the vector of the lateral stick and the rudder pedal, and $z = [e_p^T\ e_\beta^T\ e_{\text{act}}^T]^T$. An H_∞ controller $K_0(s)$ is designed for the nominal fault-free model, which achieves the H_∞ norm of 0.6671. For brevity, the parameters of the generalized plant and controller are not given here, see (Balas *et al.*, 1998) for details of the design procedure.

Consider two fault scenarios where the effectiveness of two actuators is reduced by half, denoted by

$$B_{\text{F14}}^{\text{f1}} = B_{\text{F14}}\begin{bmatrix}0.5 & 0\\ 0 & 1\end{bmatrix}, \quad B_{\text{F14}}^{\text{f2}} = B_{\text{F14}}\begin{bmatrix}1 & 0\\ 0 & 0.5\end{bmatrix},$$

respectively, where $B_{\text{F14}}^{\text{f1}}$ and $B_{\text{F14}}^{\text{f2}}$ denote the values of B_{F14} under faults.

Following a similar procedure as the fault-free mode, the generalized plants under faults can be derived, corresponding to the faulty regime models in (2). The other two controllers, $K_1(s)$ and $K_2(s)$, are designed accordingly for the plant under two actuator faults which achieve the H_∞ norms of 1.0558 and 0.7021, respectively.

The performance evaluation function is defined as

$$J(\zeta(t),\ \eta(t)) = \mu(\mathcal{M}(\zeta(t),\ \eta(t)) = \begin{cases} 1, \text{if internally unstable at } t,\\ \dfrac{\|G_{zw}(\zeta(t),\eta(t),s)\|_\infty}{1+\|G_{zw}(\zeta(t),\eta(t),s)\|_\infty},\\ \quad \text{if internally stable at } t,\end{cases}$$

and $\rho_0 = 0.5455,\ \rho_1 = \rho_2 = 0.6000$. Note that the performance degradation has been considered since ρ_1 and ρ_2 are greater than ρ_0. The hard deadline T_{hd} is arbitrarily assumed to be 1 minute in this example. Detailed discussions on determining the hard deadline can be found in (Shin and Kim, 1992).

Here $\zeta(t)$ and $\eta(t)$ take values from $S_1 = S_2 = \{0,\ 1,\ 2\}$ in which the three modes denote the fault-free mode and the loss of effectiveness in the first and second actuator, respectively. The generator matrices of these Markov processes to describe fault occurrences and FDI results are given as follows:

$$G = \begin{bmatrix}-0.003 & 0.001 & 0.002\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix},$$

$$H^0 = \begin{bmatrix}-0.02 & 0.01 & 0.01\\ 2 & -2.01 & 0.01\\ 2 & 0.01 & -2.01\end{bmatrix},$$

$$H^1 = \begin{bmatrix}-2.01 & 2 & 0.01\\ 0.01 & -0.02 & 0.01\\ 0.01 & 2 & -2.01\end{bmatrix},$$

$$H^2 = \begin{bmatrix}-2.01 & 0.01 & 2\\ 0.01 & -2.01 & 2\\ 0.01 & 0.01 & -0.02\end{bmatrix}.$$

The time unit of transition rates is selected as 1 minute. According to G, the mean occurrence time is 1000 minutes for the first fault mode and 500 minutes for the second fault, and both fault modes are absorbing. For FDI modes, according to the first row of H^0, when the aircraft is in fault-free mode, the mean time of false alarms is 100 minutes. According to its second row, the mean time to return to correct detection after a false alarm is 0.5 minutes. H^1 and H^2 can be interpreted similarly.

Following the definitions given in Section 4.2, four probabilistic parameters are calculated as follows:

$$\gamma \triangleq \begin{bmatrix}\gamma_{00} & \gamma_{01} & \gamma_{02}\\ \gamma_{10} & \gamma_{11} & \gamma_{12}\\ \gamma_{20} & \gamma_{21} & \gamma_{22}\end{bmatrix} = \begin{bmatrix}0.8600 & 0 & 0\\ 0 & 0.7000 & 0\\ 0 & 0 & 0.9600\end{bmatrix},$$

$$\left[\begin{array}{c|c} A_{\mathrm{F14}} & B_{\mathrm{F14}} \\ \hline C_{\mathrm{F14}} & D_{\mathrm{F14}} \end{array}\right] = \left[\begin{array}{cccc|cc} -0.1160 & -227.2806 & 43.0223 & 31.6347 & 0.0622 & 0.1013 \\ 0.0027 & -0.2590 & -0.1445 & 0 & -0.0053 & -0.0112 \\ -0.0211 & 0.6703 & -1.3649 & 0 & -0.0467 & 0.0036 \\ 0 & 0.1853 & 1.0000 & 0 & 0 & 0 \\ \hline 0.2469 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 57.2958 & 0 & 0 & 0 \\ 0 & 57.2958 & 0 & 0 & 0 & 0 \\ -0.0028 & -0.0079 & 0.0511 & 0 & 0.0029 & 0.0023 \end{array}\right]. \tag{17}$$

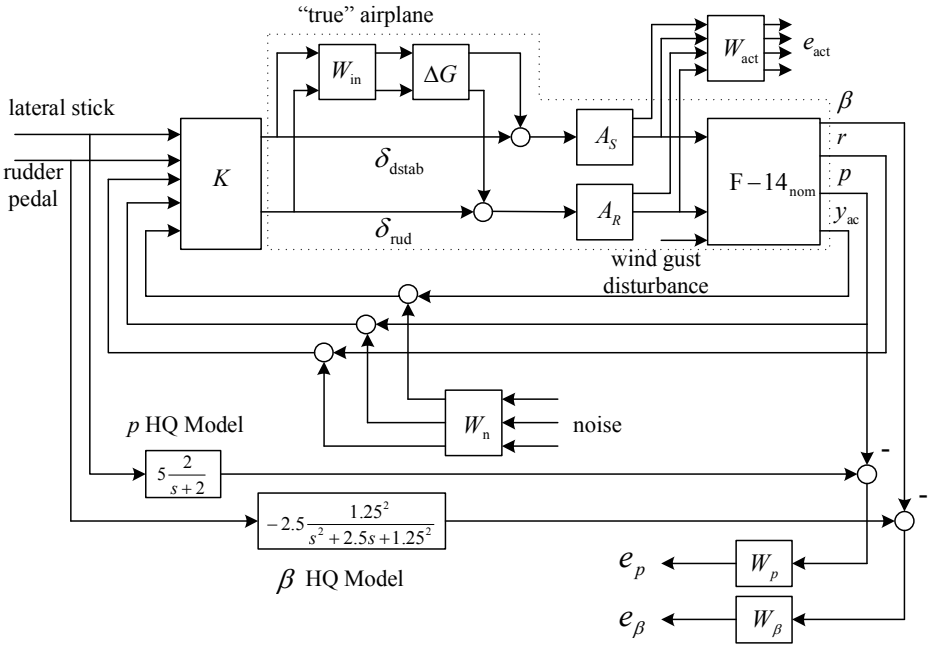

Fig. 3. Control design diagram for the F-14 lateral axis (courtesy of The MathWorks, Inc.).

$$\pi \triangleq \begin{bmatrix} \pi_0^0 & \pi_1^0 & \pi_2^0 \\ \pi_0^1 & \pi_1^1 & \pi_2^1 \\ \pi_0^2 & \pi_1^2 & \pi_2^2 \end{bmatrix} = \begin{bmatrix} 0.9901 & 0.0050 & 0.0050 \\ 0.0050 & 0.9901 & 0.0050 \\ 0.0050 & 0.0050 & 0.9901 \end{bmatrix},$$

$$w \triangleq \begin{bmatrix} w_0^0 & w_1^0 & w_2^0 \\ w_0^1 & w_1^1 & w_2^1 \\ w_0^2 & w_1^2 & w_2^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$v \triangleq \begin{bmatrix} v_0^0 & v_1^0 & v_2^0 \\ v_0^1 & v_1^1 & v_2^1 \\ v_0^2 & v_1^2 & v_2^2 \end{bmatrix} = \begin{bmatrix} 0.9333 & 0.0333 & 0.0333 \\ 0.0161 & 0.9677 & 0.0161 \\ 0.1000 & 0.1000 & 0.8000 \end{bmatrix}.$$

γ is calculated based on the closed-loop plant regime models of this F-14 aircraft and the H_∞ norm objective by using a randomized algorithm and taking random samples of ΔG within its bounded set (Tempo *et al.*, 1998). According to γ, the probability of satisfying the bounds of the H_∞ norm under each mode is 0.86, 0.7, and 0.9, respectively, if FDI gives a correct detection. According to π, the stationary probability of a correct detection is 0.9901. According to w, when the bounds of the H_∞ norm are satisfied, the probability that the FDI gives a correct detection are 1, but FDI may have given wrong estimates of fault modes when the bounds of the H_∞ norm are not satisfied according to v.

The state space of $X(t)$ contains seven states for this system: $S_{\mathrm{r}} = \{0_{\mathrm{N}},\ 0_{\mathrm{F}},\ 1_{\mathrm{N}},\ 1_{\mathrm{F}},\ 2_{\mathrm{N}},\ 2_{\mathrm{F}},\ \mathrm{F}\}$. With the above probabilistic parameters calculated from the F-14 aircraft model, the semi-Markov kernel of $X(t)$ for reliability evaluation is obtained by following the procedure in Section 4.3. The transition probabilities and reliability curve are then calculated as shown in Fig. 4.

Each transition probability curve in Fig. 4 gives the probability that $X(t)$ is in each state at t starting from the initial state 0_{N}. From the curves of reliability and the transition probability to the state F, it is clear that system failure probability remains at 0 within T_{hd}, a finding consistent with our reliability definition as temporal violation of control objectives is not deemed as a failure. We also

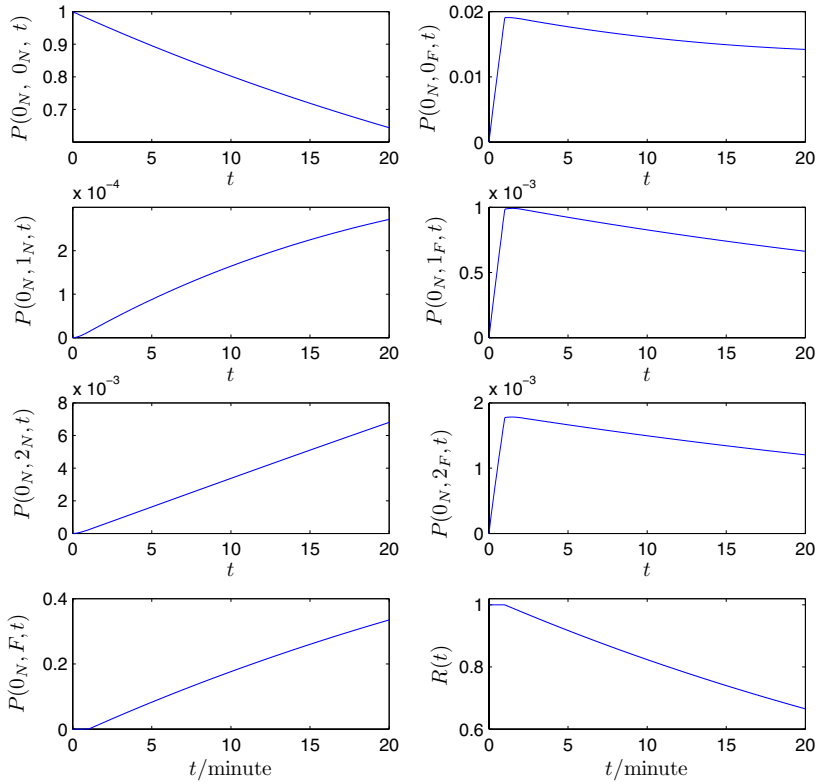

Fig. 4. Transition probability and reliability function.

find that $P(0_{\mathrm{N}}, 2_{\mathrm{N}}, t)$ is much larger than $P(0_{\mathrm{N}}, 1_{\mathrm{N}}, t)$, a finding consistent with $G(1,3) > G(1,2)$ and $\gamma_{22} > \gamma_{11}$.

According to Fig. 4, the probability of transiting to the state 0_{F} is much higher than in the case of 1_{F} and 2_{F}. So $X(t)$ transits to F mainly from 0_{F}. This implies that the false alarm of FDI at the fault-free mode is more likely the reason for a system failure than fault occurrences themselves, a finding useful for a system reliability improvement. To verify this finding, the false alarm rate for $\zeta(t) = 0$ is reduced by half by setting $H^0(1,2) = H^0(1,3) = 0.005$ and $H^0(1,1) = -0.01$. The transition probability and reliability curves for the system after reducing false alarms are shown in Fig. 5. As we expected, $P(0_{\mathrm{N}}, 0_{\mathrm{F}}, t)$ is reduced, and $R(t)$ is improved. We may also calculate and compare the MTTF of both cases: the MTTF of FTCSs before reducing FDI false alarms is 47.3415 minutes while the MTTF after reducing false alarms is 80.9144 minutes.

On the other hand, the sensitivity of the reliability index with respect to the control performance can also be demonstrated. Let probabilistic parameters be improved to $\gamma_{00} = \gamma_{11} = \gamma_{22} = 0.99$. Based on the definitions of i_{N} in (3) and γ_{ij} in (4), we expect increases in transition probabilities to i_{N}, $i \in S_1$. The transition probability and reliability curves for FTCSs with the improved control performance are shown in Fig. 6. Compared with Fig. 4, $P(0_{\mathrm{N}}, 0_{\mathrm{N}}, t)$, $P(0_{\mathrm{N}}, 1_{\mathrm{N}}, t)$, and $P(0_{\mathrm{N}}, 2_{\mathrm{N}}, t)$ are clearly improved. As a result, the reliability curve is also improved and the MTTF increases to 76.7722 minutes compared with the original MTTF of 47.3415 minutes. Consequently, the transition probability of $X(t)$ not only offers a reliability evaluation, but also help us to find an effective solution to improve the reliability.

6. Conclusions

A semi-Markov reliability model for the reliability analysis of FTCSs has been presented. The index reflects the characteristics of FTCSs, including a model-based control performance and a hard deadline concept. Based on four probabilistic parameters, the semi-Markov model was constructed, and the reliability could be thereby calculated. The semi-Markov transition probabilities and the reliability function provide valuable information on the long-term safety behavior of FTCSs. Moreover, the effects of FDI and the control performance on the reliability were demonstrated in an illustrative example. With this reliability index and the modeling method available, a reliability-based controller can be designed to optimize the overall system reliability.

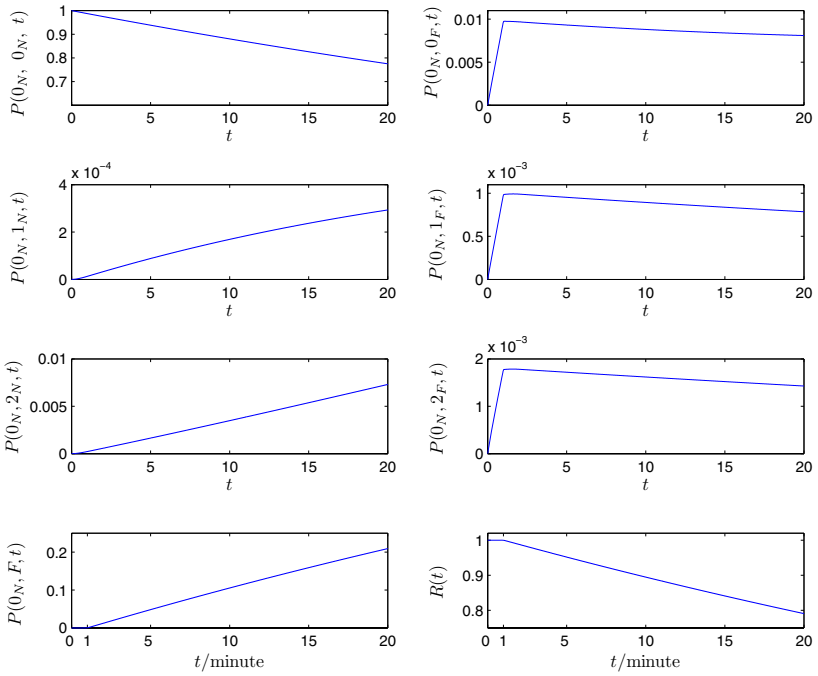

Fig. 5. Transition probability and reliability function after reducing FDI false alarms.

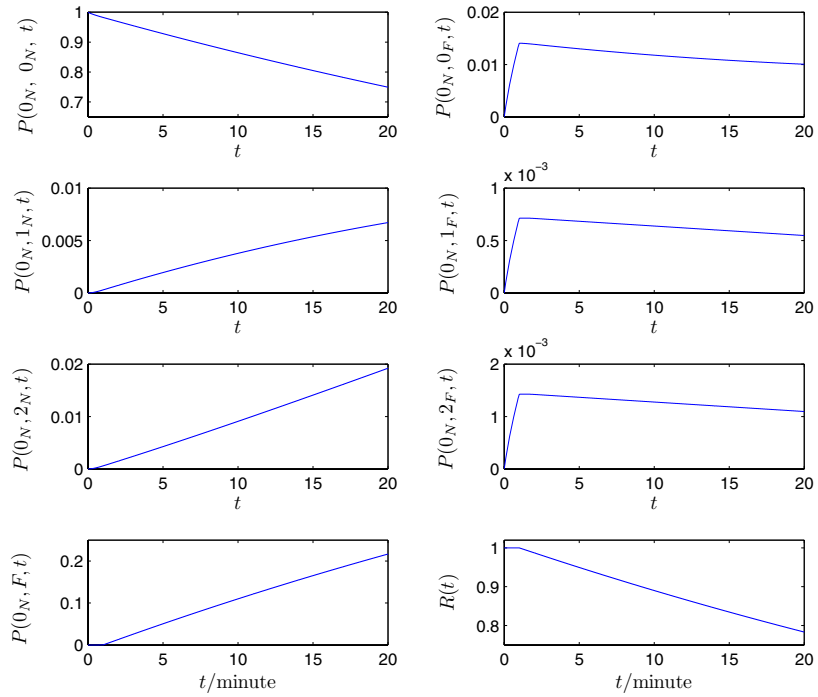

Fig. 6. Transition probability and reliability function after improving the control performance.

References

Balas G., Packard A., Renfrow J., Mullaney C., and M'Closkey R. (1998): *Control of the F-14 aircraft lateral-directional axis during powered approach*. Journal of Guidance, Control, and Dynamics, Vol. 21, No. 6, pp. 899–908.

Blanke M. (1996): *Consistent design of dependable control systems*. Control Engineering Practice, Vol. 4, No. 9, pp. 1305–1312.

Blanke M., Staroswiecki M. and Wu N.E. (2001): *Concepts and methods in fault-tolerant control*. Proceedings of American Control Conference, Arlington, USA, pp. 2606–2620.

Bonivento C., Capiluppi M., Marconi L., Paoli A. and Rossi C. (2006): *Reliability evaluation for fault diagnosis in complex systems*. Proceedings of SAFEPROCESS, Beijing, China, pp. 1405–1410.

Ciardo G., Marie R., Sericola B. and Trivedi K. (1990): *Performability analysis using semi-Markov reward processes*. IEEE Transactions on Computers, Vol. 39, No. 10, pp. 1251 –1264.

Çinlar, E. (1975): *Introduction to Stochastic Processes*. Englewood Cliffs: Prentice-Hall.

Figueras J., Vicencc P. and Quevedo J. (2006): *Multiple fault diagnosis system design using reliability analysis: Application to Barcelona rain-gauge network*. Proceedings of SAFEPROCESS, Beijing, China, pp. 1399–1404.

Guenab F., Theilliol D., Weber P., Ponsart J., and Sauter D. (2005): *Fault tolerant control method based on cost and reliability analysis*. Proceedings of the 16th IFAC World Congress, Prague, Czech Republic, (on DVD).

Guenab F., Theilliol D., Weber P., Zhang Y.M., and Sauter D. (2006): *Fault tolerant control system design: A reconfiguration strategy based on reliability analysis under dynamic behavior constraints*. Proceedings of SAFEPROCESS, Beijing, China, pp. 1387–1362.

Harrison J., Daly K. and Gai E. (1981): *Reliability and accuracy prediction for a redundant strapdown navigator*. Journal of Guidance and Control, Vol. 4, No. 5, pp. 523–529.

Jiang J. and Zhang Y.M. (2006): *Accepting performance degradation in fault-tolerant control system design*. IEEE Transactions on Control Systems Technology, Vol. 14, No. 2, pp. 284–292.

Li H. and Zhao Q. (2007): *Probabilistic design of fault tolerant control via parametrization*. Circuits, Systems, and Signal Processing, (in press).

Li H. and Zhao Q. (2006): *Reliability evaluation of fault tolerant control systems with a semi-Markov FDI model*. Proceedings of SAFEPROCESS, Beijing, China, pp. 1381–1386.

Limnios N., and Oprisan G. (2001): *Semi-Markov Processes and Reliability*. Boston: Birkhäuser.

Mahmoud M., Jiang J. and Zhang Y. (2003): *Active Fault-Tolerant Control Systems: Stochastic Analysis and Synthesis*. Berlin: Springer-Verlag.

Mariton M. (1989): *Detection delays, false alarm rates and the reconfiguration of control systems*. International Journal of Control, Vol. 49, No. 3, pp. 981–992.

Patton R. (1997): *Fault-tolerant control systems: The 1997 situation*. Proceedings of SAFEPROCESS, Kingston Upon Hull, UK, pp. 1033–1054.

Patton R., Uppal F., Simani S. and Polle B. (2006): *A Monte Carlo analysis and design for FDI of a satellite attitude control system*. Proceedings of Safeprocess, Beijing, China, pp. 1393–1398.

Polyak B.T. and Tempo R. (2001): *Probabilistic robust design with linear quadratic regulators*. Systems and Control Letters, Vol. 43, pp. 343–353.

Ross S.M. (2002): *Introduction to Probability Models, 8th Ed.* San Diego: Academic Press.

Schrick D. and Müller P. (2000): *Reliability models for sensor fault detection with state-estimator schemes*. In: Issues of Fault Diagnosis for Dynamic Systems (R. Patton, P. Frank, and R. Clark, Eds.), London: Springer-Verlag.

Shin K. and Kim H. (1992): *Derivation and application of hard deadlines for real-time control systems*. IEEE Transactions on Systems, Man and Cybernetics, Vol. 22, No. 6, pp. 1403–1412.

Spencer B., Sain M., Won C., Kaspari D. and Sain P. (1994): *Reliability-based measures of structural control robustness*. Structural Safety, Vol. 15, No. 1–2, pp. 111–129.

Srichander R. and Walker B. (1993): *Stochastic stability analysis for continuous-time fault tolerant control systems*. International Journal of Control, Vol. 57, No. 2, pp. 433–452.

Tempo R., Bai E. and Dabbene F. (1997): *Probabilistic robustness analysis: Explicit bounds for the minimum number of samples*. Systems and Control Letters, Vol. 30, No. 5, pp. 237–242.

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

Walker B. (1989): *Fault detection threshold determination using Markov theory*, In: Fault Diagnosis in Dynamic Systems: Theory and Application (R. Patton, P. Frank, and R. Clark, Eds.), Upper Saddle River: Prentice Hall.

Wu N. E. (2001): *Reliability of fault tolerant control systems: Part I and II*. Proceedings of the 40th IEEE Conference on Decision and Control, Orlando, USA, pp. 1460–1471.

Wu N.E. and Patton R. (2003): *Reliability and supervisory control*. Proceedings of SAFEPROCESS, Washington, (on CD-ROM).

Wu N. E. (2004): *Coverage in fault-tolerant control*. Automatica, Vol. 40, No. 4, pp. 537–548.

Wu N.E. and Thavamani S. (2006): *Effect of acknowledgement on performance of a fault-tolerant wireless network*. Proceedings of SAFEPROCESS, Beijing, China, pp. 1411-1416.

Yaesh I., Boyarski S. and Shaked U. (2003): *Probability-guaranteed robust H_∞ performance analysis and state-feedback design*. Systems and Control Letters, Vol. 48, No. 5, pp. 351–364.

Zhang Y.M. and Jiang J. (2001): *Integrated active fault-tolerant control using IMM approach*. IEEE Transactions on Aerospace and Electronic Systems, Vol. 37, No. 4, pp. 1221–1235.

Received: 2 February 2007
Revised: 10 July 2007