Proceedings of the
44th IEEE Conference on Decision and Control, and
the European Control Conference 2005
Seville, Spain, December 12-15, 2005

Reliability Modeling of Fault Tolerant Control Systems

Hongbin Li[1], Qing Zhao[1*]

Abstract— **This paper proposes a novel approach of reliability modeling for Fault Tolerant Control Systems (FTCS). By introducing the reliability function of FTCS based on the control performance and hard deadline, a semi-Markov process model is proposed to describe the system operation for reliability evaluation. The degraded performance of FTCS in the presence of imperfect Fault Detection & Isolation (FDI) is reflected by the states of the semi-Markov process. The semi-Markov kernel, the key parameter of the process, is determined by four probabilistic parameters from the Markovian model of FTCS. The reliability function, computed from the transition probability of the semi-Markov process, gives a suitable quantitative measure of the overall performance because it incorporates the control objectives, performance degradation, hard deadline and effects of imperfect FDI.**

I. Introduction

In order to improve the reliability of control systems, major progress have been made in Fault Tolerant Control Systems (FTCS) [1], [2], [3]. FTCS usually employ the Fault Detection and Isolation (FDI) scheme and the reconfigurable controller to eliminate the effects of the component faults, also known as active FTCS [4], [5]. But the imperfect FDI due to modeling uncertainties and disturbances may corrupt the overall stability and performance, which is one of the most important characteristics of FTCS.

Earlier work on the analysis and design of FTCS with the imperfect FDI exists in literature. In [6], Mariton studied the effects of FDI delays on stability by modeling FTCS as Markovian stochastic systems; by using two Markov process to represent the faults and FDI results, Srichander et al. developed the necessary and sufficient conditions for exponential stability in the mean square [7]; Mahmoud et al. derived the stability of FTCS in the presence of noise in [8] and summarized their results on the analysis and design of FTCS based on Markovian model in [9]. Although the Markovian modeling of FDI may be restrictive, the influence of imperfect FDI is treated in Markovian model. Furthermore, the simplicity of Markov process and the availability of analysis tools make it a valid model for FTCS. In this paper, we use this Markovian model to study the reliability evaluation problem of active FTCS.

Reliability is an important concern in FTCS and has been investigated using various methods. An ongoing research contribution is due to Wu [3], [13], [14], [15], [16]. In her latest results, the reliability is evaluated from a Markov process model built from the serial-parallel block diagram which describes the functional relations among subsystems and components. Coverage of failures is used as a link between the reliability and the control actions. A similar system configuration was deployed in [17] where reliability was evaluated from serial-parallel structures and optimization was conducted to find the best structure based on reliability and cost. However, this framework is restricted to those FTCS that can be described by serial-parallel block diagram.

Other methods are based on Markov or semi-Markov reliability modeling. In [18], a semi-Markov model was built by defining the semi-Markov states as the combinations of status of faults and FDI schemes without considering any dynamical relations and control objectives. In [19], [20], the reliability evaluations from the Markov modeling of FDI were used to determine the residue threshold of FDI and to compare several sensor fault detection schemes respectively. In [21], a similar discrete-time Markov model was established for a redundant navigator. However, in these Markov or semi-Markov models, the state is simply defined as a combination of the fault modes and FDI results, in which the role of control was not considered. Hence, a link between the reliability and the overall control performance of FTCS is missing.

Different from these available results, this paper proposes a semi-Markov reliability model which is built from the dynamical model and incorporates the following characteristics of FTCS.

• Control objectives. In control systems, the overall system performance is usually described in the sense of control objectives. We say that the control system performs its function well if it satisfies the given control objectives. Hence, the reliability analysis of control systems in general should take control objectives into account.

• Performance degradation. Fault tolerant control deals with the system under various faulty conditions. In this case, it should allow certain degree of performance degradation. The degraded control objectives are usually applied based on current available system resources. The reliability model should consider such degraded performance requirements.

• Hard deadline in FTCS. Controller reconfiguration may temporally deteriorate the control performance then recover the degraded performance, which should be distinguished from a failure. Therefore, the amount of violation time should be examined to determine the system failure. For this reason, the hard deadline concept proposed in the analysis of real-time systems [22], [23] is used to define the reliability of FTCS.

• Effects of imperfect FDI. False alarms and missing detections may corrupt control performance in FTCS and

[1] The authors are with Department of Electrical & Computer Engineering, University of Alberta, Edmonton, Alberta, Canada, T6G 2V4.

[*] The corresponding author. Tel: (780)492-5792; Fax: (780)492-1811; Email: qingzhao@ece.ualberta.ca.

0-7803-9568-9/05/$20.00 ©2005 IEEE

their crucial influence need to be described in the reliability evaluation. The remainder of this paper is organized as follows. In section 2, the model of FTCS and a description of the reliability evaluation problem is discussed. The semi-Markov reliability process model is presented in section 3. An example is given in section 4 to illustrate the modelling procedure followed by the conclusions in section 5.

II. Problem formulation

A. Modeling of FTCS

Consider the following general Markovian model of FTCS [9], [7],

$$\mathcal{M}:\begin{cases}\dot{x}(t)=[A(\zeta(t))+\Delta A(\zeta(t))]x(t)+[B(\zeta(t))\\ \qquad +\Delta B(\zeta(t))]u(\eta(t),t)+E(\zeta(t))w(t),\\ y(t)=[C(\zeta(t))+\Delta C(\zeta(t))]x(t)+[D(\zeta(t))\\ \qquad +\Delta D(\zeta(t))]u(\eta(t),t)+F(\zeta(t))w(t),\end{cases} \tag{1}$$

where, $x(t)\in\mathbb{R}^n$, $u(\eta(t),t)\in\mathbb{R}^m$, $y(t)\in\mathbb{R}^l$ and $w(t)\in\mathbb{R}^h$ denote the system state, control input, output and exogenous input respectively. $A(\zeta(t)), B(\zeta(t)), C(\zeta(t)), D(\zeta(t)), E(\zeta(t))$ and $F(\zeta(t))$ are system matrices with compatible dimensions. $\Delta A(\zeta(t))$, $\Delta B(\zeta(t))$, $\Delta C(\zeta(t))$ and $\Delta D(\zeta(t))$ are uncertainty matrices which are assumed to be bounded and have known probabilistic distributions.

$\zeta(t)$ and $\eta(t)$ are assumed to be two separate continuous-time Markov processes to represent the system fault process and FDI process with finite state spaces $S_1=\{0,1,2,\cdots,N_1\}$ and $S_2=\{0,1,2,\cdots,N_2\}$. $\zeta(t)$ is a homogeneous process while the transition rates of $\eta(t)$ depend on the current state of $\zeta(t)$.

Let us begin with the case that the state spaces of $\zeta(t)$ and $\eta(t)$ are equal and both take values from $\{0,1\}$, where '0' denotes fault-free situation and '1' the faulty state. This type of FTCS is referred to as the basic case of FTCS in the sequel. The behavior of $\zeta(t)$ is governed by its generator matrix G [24], [25]; when $\zeta(t)=0$ or 1, the behavior of $\eta(t)$ is determined by the corresponding generator matrix H^0 or H^1. $\zeta(t)$ and $\eta(t)$ may take different values from each other and this discrepancy represents the incorrect decision of FDI; the imperfect properties of FDI are described by H^0 and H^1 [26]. The generator matrices of the basic case have the following form:

$$G=\begin{bmatrix}\alpha_{00} & \alpha_{01}\\ 0 & 0\end{bmatrix}, H^0=\begin{bmatrix}\beta^0_{00} & \beta^0_{01}\\ \beta^0_{10} & \beta^0_{11}\end{bmatrix}, H^1=\begin{bmatrix}\beta^1_{00} & \beta^1_{01}\\ \beta^1_{10} & \beta^1_{11}\end{bmatrix},$$

where α_{ij} and β^k_{ij} are the transitions rates of $\zeta(t)$ and $\eta(t)$. Note that the transition rates in the second row of G are assumed to be zeros, meaning that no repair or intermediate fault is involved and our attention is focused on the role of fault tolerant control to improve reliability.

Considering the modeling uncertainties, the control performance of the system in (1) is given in terms of probabilistic robustness analysis, which assumes a probability distribution of the parameter uncertainties and evaluate the probability that a specific performance is satisfied by randomized algorithms [27]. This probabilistic robustness avoids the possible conservativeness of classical robustness and has clear meaning in practice where the required performance objectives are always associated with certain minimum probability levels [28]. In the sequel, we call this description as *probabilistic performance* and apply the randomized algorithm given in [29] to estimate it.

B. Problem description

The problem considered in this paper is to find an appropriate reliability criterion as an overall performance measure for FTCS in (1). To consider the characteristics of FTCS, we introduce the following reliability function for FTCS.

Definition 1: The reliability function $R(t)$ of FTCS is defined as the probability that, during the time interval $[0,t]$, the FTCS either satisfy the presumed control objective or violate it only temporally for a short time no more than the presumed hard deadline, T_{hd}.

Remark 1: Suppose the scalar function $\mu(\cdot)$ represents a static performance measure of linear control systems and smaller value indicates better performance. By static, we mean $\mu(\cdot)$ only depends on the closed-loop system model, such as the system norm. For FTCS in (1), the performance value at t, denoted by $J(t)$, is calculated based on the linear model $\mathcal{M}(\zeta(t),\eta(t))$.

$$J(t)\triangleq\mu(\mathcal{M}(\zeta(t),\eta(t))). \tag{2}$$

Set a performance upper bound J^i_{max} for $\zeta(t)=i$. If $J(t)\le J^i_{\text{max}}$, the control objective is said to be satisfied.

Remark 2: Performance degradation is described by the different performance bounds under various fault modes. For example, if $\zeta(t)=0$ denotes the normal case and $\zeta(t)=1$ the faulty case, we usually have the relation that $J^0_{\text{max}}<J^1_{\text{max}}$.

Remark 3: Due to imperfect FDI results, the performance value $J(t)$ may exceed J^i_{max} only temporally for a short time. We assume that, if this time is greater than a particular limit T_{hd}, the system is generally unable to return to the functional state. In this sense, T_{hd} is called the hard deadline in FTCS.

To recap, the reliability function given in Definition 1 is introduced to analyze the performance of FTCS which reflects the control performance, performance degradation, hard deadline and effects of imperfect FDI. The remainder of this paper focuses on finding an approach to evaluate the reliability function for FTCS in (1). We use the semi-Markov process to describe the system for reliability evaluation due to its flexibility of sojourn time distribution [12], [24], [30].

III. A semi-Markov process model of FTCS for reliability evaluation

A. State definitions of the semi-Markov process

For the basic case of FTCS, a semi-Markov process, denoted as $X(t)$, for reliability evaluation is presented. The state transition diagram is given in Fig. 1.

The state space of the semi-Markov process contains 5 elements, denoted by $S_{\text{r}}=\{(0,\text{N}),(0,\text{F}),(1,\text{N}),\ (1,\text{F}),\text{F}\}$. 'F' represents the unique nonfunctional state, the total failure

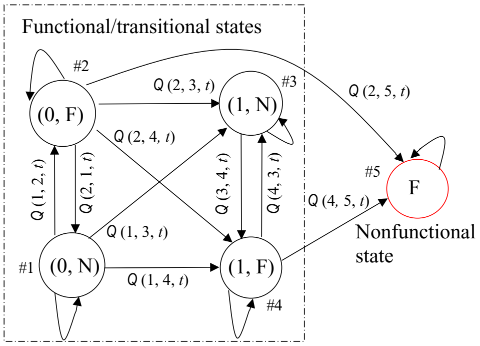

Fig. 1. State transition diagram of the semi-Markov process.

of the system that cannot return to functional state without human intervention. The functional state is represented by a pair with a number and a letter in the bracket: the number represents the fault mode, 0 or 1 in the basic cases; letter 'N' indicates satisfactory performance and 'F' unsatisfactory performance but within the hard deadline. The exact definitions of these states are given in (3)-(4) as follows.

For $i \in S_1$,

$$(i, \mathrm{N}) : \{\zeta(t) = i\} \cap \{J(t) \le J^i_{\max}\}, \tag{3}$$

$$(i, \mathrm{F}) : \{\zeta(t) = i\} \cap \{J(t) > J^i_{\max}\} \cap \{\text{sojourn time} \le T_{\mathrm{hd}}\}. \tag{4}$$

Here, for one particular fault mode i, two states (i, N) and (i, F), associated with different performance levels, are defined to account for the effects of the imperfect FDI and the hard deadline.

The definitions of these states reflect different performance levels with different fault modes, which demonstrates the performance degradation in FTCS. Different regions of performance grades in FTCS are illustrated in Fig. 2, where the inner circle and square represent the regions of functional states.

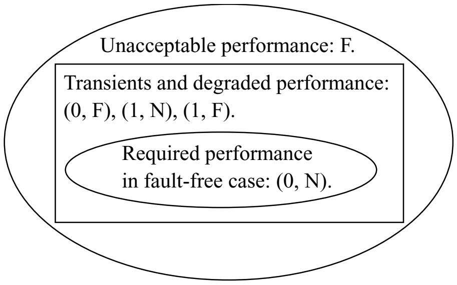
Unacceptable performance: F.
Transients and degraded performance: (0, F), (1, N), (1, F).
Required performance in fault-free case: (0, N).

Fig. 2. Regions of performance grades.

For notational simplicity, the indices, $\#1 \sim \#5$, are used to denote the states, e.g., $X(t) = 1$ is equivalent to $X(t) = (0, \mathrm{N})$.

B. Probabilistic parameters

In this subsection, several probabilistic terms are defined to be used in the semi-Markov reliability model.

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

$$\gamma_{ij} \triangleq \Pr\{J(t) \le J^i_{\max} | \zeta(t) = i, \eta(t) = j\}, i \in S_1, j \in S_2.$$

γ_{ij} is the probabilistic performance when the fault mode is i and FDI mode is j. This value can be estimated by randomized algorithm given in [29].

Definition 3: For a particular fault mode, the stationary distribution of the FDI mode is defined by

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

π^i_j can be calculated based on the generator matrix of $\eta(t)$ when $\zeta(t) = i$ [24], [25].

Definition 4: Given $X(t) = (i, N), \quad i \in S_1$, the probability that the FDI process equals a specific mode is defined by

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

w^i_j can be calculated based on the Bayes' formula as shown in the example of w^0_0 below. If γ_{00} and γ_{01} are not equal to zero simultaneously, then

$$\begin{aligned} w^0_0 &= \lim_{t \to \infty} \Pr\{\eta(t) = 0 | X(t) = (0, N)\} \\ &= \lim_{t \to \infty} \Pr\{\eta(t) = 0 | \zeta(t) = 0 \cap J(t) \le J^0_{\max}\} \\ &= \frac{\gamma_{00}\pi^0_0}{\gamma_{00}\pi^0_0 + \gamma_{01}\pi^0_1}. \end{aligned} \tag{5}$$

The details of the derivation are given in (6) on the next page. In case that $\gamma_{00} = \gamma_{01} = 0$, define $w_{00} = \pi^0_0$. The procedures of calculating w^i_j are similar for other values of i and j.

Definition 5: Given $X(t) = (i, F), \quad i \in S_1$, the probability that the FDI process equals a specific mode is defined by

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

v^i_j can be calculated in the similar way.

C. Calculation of the semi-Markov kernel

For the semi-Markov process $X(t)$, denote the associated Markov-renewal process as $(Y_n, T_n, n \in \mathbb{N})$. The so-called embedded Markov chain, Y_n, is the state sequence that $X(t)$ visits consecutively and T_n is the time instant of transition. The semi-Markov kernel matrix of $X(t)$ is denoted as Q and its element as $Q(i, j, t)$, $i, j \in S_{\mathrm{r}}, t \in \mathbb{R}, t \ge 0$.

$$Q(i, j, t) \triangleq \Pr\{Y_{n+1} = j, T_{n+1} - T_n \le t | Y_n = i\},$$

which gives the probability that $X(t)$ starts from i and jumps to j with sojourn time $T_{n+1} - T_n$ no greater than t. For details of the Markov-renewal process and semi-Markov kernel, please refer to [24].

Due to the previous assumption on the static performance measure and time-invariance of modeling uncertainty, the state transition of $X(t)$ is only triggered by the change of mode of $\zeta(t)$ or $\eta(t)$. It assures that only the events of faults,

$$
\begin{aligned}
w_0^0 &= \lim_{t\to\infty} \frac{\Pr\{J(t) \le J^0_{\max} | \eta(t) = 0 \cap \zeta(t) = 0\}\Pr\{\eta(t) = 0 \cap \zeta(t) = 0\}}{\sum_{k\in S_2} \Pr\{J(t) \le J^0_{\max} | \eta(t) = k \cap \zeta(t) = 0\}\Pr\{\eta(t) = k \cap \zeta(t) = 0\}} \\
&= \frac{\Pr\{J(t) \le J^0_{\max} | \eta(t) = 0 \cap \zeta(t) = 0\} \lim_{t\to\infty} \Pr\{\eta(t) = 0 | \zeta(t) = 0\}}{\sum_{k\in S_2} \Pr\{J(t) \le J^0_{\max} | \eta(t) = k \cap \zeta(t) = 0\} \lim_{t\to\infty} \Pr\{\eta(t) = k | \zeta(t) = 0\}} \qquad (6)
\end{aligned}
$$

the FDI decision and controller reconfiguration have major influence on the system performance of FTCS, which may lead to the transition to itself or to a different state if there is abrupt change of performance.

When the initial state is (i, N), the main steps of calculating the element of the semi-Markov kernel are similar. They are listed as follows for the case of $X(t) = (0, \mathrm{N})$.

1) Estimate the FDI mode $\eta(t)$ before the transition using w_j^i or v_j^i based on the current semi-Markov state.
2) Both $\zeta(t)$ and $\eta(t)$ may jump to a new mode. The first process that jumps determines the possible transitional destination states. For example, if the current state is (0, N) and $\zeta(t)$ jumps before $\eta(t)$, the destination state is (1, N) or (1, F); otherwise, $\eta(t)$ jumps first and the destination state is (0, F) or (0, N). This competition between $\zeta(t)$ and $\eta(t)$ determines the destination states and the probability of different competition result is calculated from a property of exponential distribution.
3) Use γ_{ij} to calculate the probability that the performance value is less or greater than the bound at the destination states.
4) Based on the total probability formula, calculate the jumping probability from i to j, i.e., the element $Q(i, j, t)$ of the semi-Markov kernel.

Consider $Q(1, 2, t)$ as an example for the case that $X(t)$ starts from state (0, N) and jumps to (0, F) with sojourn time no greater than t. This jump is triggered by the false alarms of $\eta(t)$, which jumps before $\zeta(t)$, and the probability can be decomposed into two terms as shown in the following equation. The first term is for the case of $\eta(T_n) = 0$ and the second for $\eta(T_n) = 1$. For notational simplicity, denote $\zeta_n := \zeta(T_n)$, $\eta_n := \eta(T_n)$ and $J_{n+1} := J(T_{n+1})$.

$$
\begin{aligned}
&Q(1,2,t) \triangleq Q((0,\mathrm{N}),(0,\mathrm{F}),t) \\
&= \Pr\{Y_{n+1} = (0,\mathrm{F}) \cap T_{n+1} - T_n \le t | Y_n = (0,\mathrm{N})\} \\
&= \Pr\{Y_{n+1} = (0,\mathrm{F}) \cap \eta_{n+1} = 1 \cap T_{n+1} - T_n \le t | Y_n = (0,\mathrm{N}) \\
&\cap \eta_n = 0\} \cdot \Pr\{\eta_n = 0 | Y_n = (0,\mathrm{N})\} + \Pr\{Y_{n+1} = (0,\mathrm{F}) \cap \\
&\eta_{n+1} = 0 \cap T_{n+1} - T_n \le t | Y_n = (0,\mathrm{N}) \cap \eta_n = 1\} \qquad (7) \\
&\cdot \Pr\{\eta_n = 1 | Y_n = (0,\mathrm{N})\}. \qquad (8)
\end{aligned}
$$

These two terms are in the same form hence the first one, denoted as q_1, is taken as an example to show the derivation. Replace (0, F) by its definition in (4), we have

$$
\begin{aligned}
q_1 &\triangleq \Pr\{Y_{n+1} = (0,\mathrm{F}) \cap \eta_{n+1} = 1 \cap T_{n+1} - T_n \le t \\
&\quad | Y_n = (0,\mathrm{N}) \cap \eta_n = 0\} \cdot \Pr\{\eta_n = 0 | Y_n = (0,\mathrm{N})\} \\
&= \Pr\{J_{n+1} > J^0_{\max} \cap \zeta_{n+1} = 0 \cap \eta_{n+1} = 1 \cap T_{n+1} - T_n \le t \\
&\quad | Y_n = (0,\mathrm{N}) \cap \eta_n = 0\} \cdot \Pr\{\eta_n = 0 | Y_n = (0,\mathrm{N})\}. \qquad (9)
\end{aligned}
$$

Then, use the conditional probability to decompose q_1 into three terms.

$$
\begin{aligned}
&q_1 = \Pr\{J_{n+1} > J^0_{\max} | \zeta_{n+1} = 0 \cap \eta_{n+1} = 1 \cap T_{n+1} - T_n \le t \\
&\cap Y_n = (0,\mathrm{N}) \cap \eta_n = 0\} \cdot \Pr\{\zeta_{n+1} = 0 \cap \eta_{n+1} = 1 \cap T_{n+1} - T_n \\
&\le t | Y_n = (0,\mathrm{N}) \cap \eta_n = 0\} \cdot \Pr\{\eta_n = 0 | Y_n = (0,\mathrm{N})\}. \qquad (10)
\end{aligned}
$$

Considering that $J_{n+1} = \mu(\mathcal{M}(\zeta_{n+1}, \eta_{n+1}))$ does not depend on $T_{n+1} - T_n \le t$, Y_n or η_n, (10) is simplified as follows.

$$
\begin{aligned}
&q_1 = \Pr\{J_{n+1} > J^0_{\max} | \zeta_{n+1} = 0 \cap \eta_{n+1} = 1\} \\
&\cdot \Pr\{\zeta_{n+1} = 0 \cap \eta_{n+1} = 1 \cap T_{n+1} - T_n \le t | \zeta_n = 0 \cap \eta_n = 0\} \\
&\cdot \Pr\{\eta_n = 0 | Y_n = (0,\mathrm{N})\}. \qquad (11)
\end{aligned}
$$

Now, q_1 is decomposed into three terms and each of them can be calculated by the probabilistic parameters introduced in section III-B. Firstly the last term is approximated by w_0^0, a stationary probability.

$$\Pr\{\eta_n = 0 | Y_n = (0,\mathrm{N})\} \approx w_0^0. \qquad (12)$$

Secondly, γ_{01} is used to approximate the first term.

$$\Pr\{J_{n+1} > J^0_{\max} | \zeta_{n+1} = 0 \cap \eta_{n+1} = 1\} \approx 1 - \gamma_{01}. \qquad (13)$$

The second term in the right hand side of (11) shows the competition between $\zeta(t)$ and $\eta(t)$. Due to the property of exponential distribution [25], we have

$$
\begin{aligned}
&\Pr\{\zeta_{n+1} = 0 \cap \eta_{n+1} = 1 \cap T_{n+1} - T_n \le t | \zeta_n = 0 \cap \eta_n = 0\} \\
&\qquad = \frac{\beta^0_{01}}{\alpha_{01} + \beta^0_{01}} (1 - e^{-(\alpha_{01} + \beta^0_{01})t}). \qquad (14)
\end{aligned}
$$

Combining all these terms in (12)-(14), we obtain the expression of q_1. The other term in (8) can be calculated by the same procedure and the final expression of $Q(1, 2, t)$ is given below.

$$
\begin{aligned}
Q(1,2,t) &= w_0^0 \frac{\beta^0_{01}}{\alpha_{01} + \beta^0_{01}} (1 - e^{-(\alpha_{01} + \beta^0_{01})t})(1 - \gamma_{01}) \\
&\quad + w_1^0 \frac{\beta^0_{10}}{\alpha_{01} + \beta^0_{10}} (1 - e^{-(\alpha_{01} + \beta^0_{10})t})(1 - \gamma_{00}). \qquad (15)
\end{aligned}
$$

When $X(t) = (0, \mathrm{F})$, if the sojourn time is less than the hard deadline T_{hd}, the next possible states are (0, N), (0, F), (1, N) and (1, F); otherwise, it jumps to F. The calculation of $Q(2, 1, t)$ is similar as that of $Q(1, 2, t)$ except for the effect of hard deadline, which can be described by a minimum between t and T_{hd}, denoted as $\min(t, T_{\text{hd}})$.

$$Q(2,1,t) = v_0^0 \frac{\beta_{01}^0}{\alpha_{01} + \beta_{01}^0}(1 - e^{-(\alpha_{01}+\beta_{01}^0)\min(t,T_{\text{hd}})})\gamma_{01}$$
$$+v_1^0 \frac{\beta_{10}^0}{\alpha_{01} + \beta_{10}^0}(1 - e^{-(\alpha_{01}+\beta_{10}^0)\min(t,T_{\text{hd}})})\gamma_{00}. \quad (16)$$

$Q(2,5,t)$ is the probability that $X(t)$ jumps from (0, F) to F within sojourn time no greater than t. Due to the hard deadline T_{hd}, $Q(2,5,t)$ is zero when $t \le T_{\text{hd}}$ and the value when $t > T_{\text{hd}}$ is complementary to the probability of jumping to other states. This characteristic is described by the following step function.

$$\mathcal{U}(t - T_{\text{hd}}) = \begin{cases} 0, & t \le T_{\text{hd}}, \\ 1, & t > T_{\text{hd}}. \end{cases}$$

$$Q(2,5,t) =$$
$$\mathcal{U}(t-T_{\text{hd}})(1-v_0^0(1-e^{-(\alpha_{01}+\beta_{01}^0)T_{\text{hd}}})-v_1^0(1-e^{-(\alpha_{01}+\beta_{10}^0)T_{\text{hd}}})).$$

We simply assign the elements in the 5th row of Q to zeros as F is assumed to be absorbing.

Remark 4: In the derivation of $Q(1,2,t)$, the key step is to decompose it by the total probability and conditional probability formula into probabilities that can be approximated or calculated by the probabilistic parameters.

Remark 5: When $X(t)$ jumps from (0, F), the effects of hard deadline T_{hd} are described by min(t, T_{hd}) and $\mathcal{U}(t-T_{\text{hd}})$. When $t \le T_{\text{hd}}$, the calculation procedures are the same as those when $X(t)$ jumps from (0, N); when $t > T_{\text{hd}}$, $X(t)$ transits to the absorbing state F.

Remark 6: Once the semi-Markov kernel is determined, the reliability function and other criteria, such as Mean Time To Failure (MTTF), are ready to be calculated [30].

Remark 7: The above procedures can be extended to the system with multiple fault modes. The procedures remain the same though the dimension of the semi-Markov model and the calculation burden increase. The details are omitted for brevity.

IV. An Illustrative Example

Consider a system in the form of (1) and $S_1 = S_2 = \{0, 1\}$. Using the subscripts '0' or '1' to denote the parameters under the corresponding fault mode '0' or '1', the nonzero system parameters are given below.

$$A_0 = \begin{bmatrix} 8 & 6 \\ 9 & 4 \end{bmatrix}, A_1 = \begin{bmatrix} 10 & 13 \\ 14 & 18 \end{bmatrix},$$

$$B_0 = \begin{bmatrix} 4 & 7 \\ 5 & 6 \end{bmatrix}, B_1 = \begin{bmatrix} 10 & 12 \\ 25 & 15 \end{bmatrix},$$

$$E_0 = [5 \;\; 2]^T, E_1 = [16 \;\; 10]^T, C_0 = [3 \;\; 8], C_1 = [10 \;\; 20].$$

The generator matrices of for fault process $\zeta(t)$ and FDI process $\eta(t)$ are:

$$G = \begin{bmatrix} -0.5 & 0.5 \\ 0 & 0 \end{bmatrix},$$

$$H^0 = \begin{bmatrix} -0.0204 & 0.0204 \\ 3.9039 & -3.9039 \end{bmatrix}, H^1 = \begin{bmatrix} -2.9925 & 2.9925 \\ 0.0515 & -0.0515 \end{bmatrix}.$$

The static state feedback controller for the FDI mode '0' and '1' are:

$$K_0 = \begin{bmatrix} 56.2152 & -20.7314 \\ -88.8067 & -15.2863 \end{bmatrix},$$

$$K_1 = \begin{bmatrix} 49.2438 & -29.1472; \\ -137.3958 & -6.3796 \end{bmatrix}.$$

Here we use H_∞ norm as the performance measure and the performance evaluation function with the thresholds for the two fault modes is defined as follows:

$$J(t) = \begin{cases} 1, \text{ internally unstable at } t, \\ \frac{\|G_{yw}(\zeta(t),\eta(t),s)\|_\infty}{1+\|G_{yw}(\zeta(t),\eta(t),s)\|_\infty}, \text{ internally stable at } t, \end{cases}$$

$$J_{\text{max}}^0 = 0.1, \quad J_{\text{max}}^1 = 0.2,$$

where $G_{yw}(\zeta(t), \eta(t), s)$ is the transfer function from w to y at time t corresponding to the current fault mode $\zeta(t)$ and FDI mode $\eta(t)$. By the assumption of known distributions of uncertainties and the randomized algorithm in [29] , we have

$$\gamma \triangleq \begin{bmatrix} \gamma_{00} & \gamma_{01} \\ \gamma_{10} & \gamma_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The simple form of γ means that when FDI result matches the real fault mode, the controller has good robust performance; when they do not match, the performance requirement is not satisfied.

Based on H^0 and H^1, we have

$$\pi_0^0 = 0.9948, \quad \pi_1^0 = 0.0052, \quad \pi_0^1 = 0.0169, \quad \pi_1^1 = 0.9831.$$

By the method in section III-B , we obtain the values of w_j^i and v_j^i, $i, j \in \{0, 1\}$, as follows. Due to the special structure of γ, w and v also have simple forms.

$$w \triangleq \begin{bmatrix} w_0^0 & w_1^0 \\ w_0^1 & w_1^1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad v \triangleq \begin{bmatrix} v_0^0 & v_1^0 \\ v_0^1 & v_1^1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The hard deadline T_{hd} is arbitrarily set as 1 second. The semi-Markov kernel is obtained by following the procedure in section III-C. Then, use the methods in [30] to calculate its transition probability and reliability function.

Suppose the initial state of the system is $(0, N)$, the transition probability is given in Fig. 3. From this figure, we can see that when the process is at state No. 1 initially, it jumps to state No. 2 with high probability; the probability that the process stays at state No. 1 decreases mononically due to the assumption of no repair; the probability that the process jumps to state No. 2 quickly reaches its peak value then gradually decreases to 0 because the process jumps to F when sojourn time in (0, F) is greater than the hard deadline; the probability that the process jumps to state No. 5, the total failure state, remains at 0 within the first second then increases mononically, because the hard deadline $T_{\text{hd}} = 1$ second and the jump to the total failure state only occurs after the hard deadline. The reliability curve is shown in Fig. 4. From the figure, we can see that the reliability remain at 1 within the first second, which again is consistent with

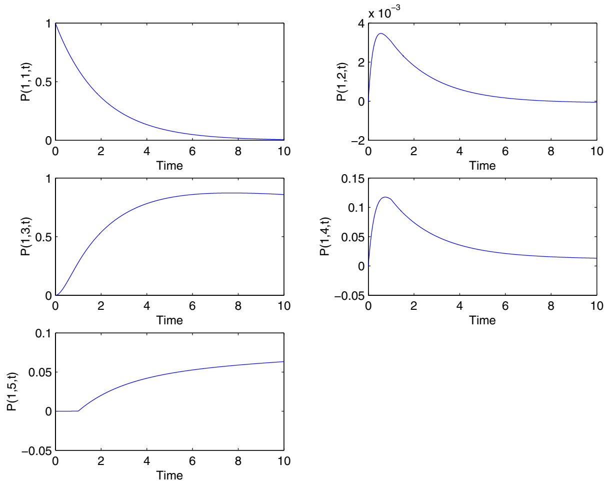

Fig. 3. The transition probability

the hard deadline of $T_{\text{hd}} = 1$ second because the violation of the performance requirements within the hard deadline is considered to be transients. We may also evaluate other scalar criteria, such as Mean Time to Failure (MTTF) equals 375.9082 second.

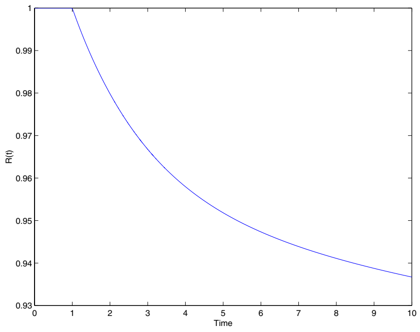

Fig. 4. The reliability curve.

V. Conclusions

A reliability evaluation approach for FTCS is presented in this paper. We start from defining the reliability function based on the control performance and hard deadline of FTCS. Then a semi-Markov process model is constructed for reliability evaluation. The states of this semi-Markov process describe the performance degradation of FTCS and the effects of imperfect FDI on control performance. Finally, we discuss a example to show the procedure. This reliability evaluation reflects the critical characteristics of FTCS and it may be more suitable for practical applications, such as controller design based on the reliability evaluation.

References

[1] M. Blanke, M. Staroswiecki and N. Wu. "Concepts and methods in fault-tolerant control", *Proc. American Contr. Conf.*, Arlington, USA, 2001, pp. 2606 - 2620.

[2] R. Stengel, "Intelligent failure-tolerant control", *IEEE Contr. Sys. Magazine*, vol. 11, no. 4, pp. 14-23, 1991.

[3] N. Wu and R. Patton, "Reliability and supervisory control", *Proc. IFAC-Safeprocess 2003*, Washington, 2003.

[4] R. Patton, "Fault-tolerant control systems: the 1997 situation", *IFAC Symp. Fault Detection Supervision and Safety for Technical Processes*, edited by R. Patton and J. Chen, Kingston Upon Hull, UK, vol. 3, pp. 1033-1054, 1997.

[5] M. Blanke, M. Kinnaert, J. Lunze and M. Staroswiecki, *Diagnosis and Fault-Tolerant control*, Springer, 2003.

[6] M. Mariton, "Detection delays, false alarm rates and the reconfiguration of control systems", *Int. J. Contr.*, vol. 49, pp. 981-992, 1989.

[7] R. Srichander and B. Walker, "Stochastic stability analysis for continuous-time fault tolerant Control Systems", *Int. J. Contr.*, vol. 57, no. 2, pp. 433-452, 1993.

[8] M. Mahmoud, J. Jiang and Y. Zhang, "Stochastic statbility analysis of active fault-tolerant control systems in the presence of noise", *IEEE Trans. Automat. Contr.*, vol. 46, no. 11, pp. 1810-1815, 2001.

[9] M. Mahmoud, J. Jiang and Y. Zhang, *Active Fault-tolerant Control Systems: Stochastic Analysis and Synthesis*, Springer-Verlag, 2003.

[10] A. Samir, J. Christophe and S. Dominique, "Output feedback stochastic stabilization of active fault tolerant control systems: LMI formulation", *16th IFAC World Congress*, Prague, 2005.

[11] A. Kaoutar and B. El-Kebir, "Hinf Based Fault Detection and Isolation for Markovian Jump Systems", *16th IFAC World Congress*, Prague, 2005.

[12] A. Birolini, *On the Use of Stochastic Processes in Modeling Reliability Problems*, Springer-Verlag, Berlin, 1985.

[13] N. Wu, "Coverage in fault-tolerant control", *Automatica*, vol. 40, no. 4, pp. 537-548, 2004.

[14] N. Wu, "Reliability prediction for self-repairing flight control systems", *Proc. 35th IEEE Conf. Decision Contr.*, Kobe, Japan, 1996.

[15] N. Wu, "Reliability criteria based reconfigurable control system design", *IFAC Symp. Fault Detection Supervision and Safety for Technical Processes*, edited by R. Patton and J. Chen, Kingston Upon Hull, UK, 1997, vol. 3, pp. 1065-1070.

[16] N. Wu, "Reliability of fault tolerant control systems", *Proc. 40th IEEE Conf. Decision Contr.*, Orlando, USA, 2001, pp. 1460-1471.

[17] F. Guenab, D. Theilliol, P. Weber, J. Ponsart and D. Sauter, " Fault tolerant control method based on cost and reliability analysis", *16th IFAC World Congress*, Prague, 2005.

[18] B. Walker, "Fault Tolerant Control System Reliability and Performance Prediction Using Semi-Maarkov Models", *IFAC Symp. Fault Detection Supervision and Safety for Technical Processes*, edited by R. Patton and J. Chen, Kingston Upon Hull, UK, vol. 3. pp. 1053-1064, 1997.

[19] B. Walker, "Fault detection threshold determination using markov Theory", in *Fault Diagnosis in Dynamic Systems: Theory and Application*, edited by R. Patton, P. Frank and R. Clark, Prentice Hall, 1989.

[20] D. Schrick and P. Müller, "Reliability models for sensor fault detection with state-estimator schemes", *Issues of Fault Diagnosis for Dynamic Systems*, edited by, R. Patton, P. Frank and R. Clark, Springer-Verlog, London, 2000.

[21] J. Harrison, K. Daly and E. Gai, "Reliability and accuracy prediction for a redundant strapdown navigator", *J. Guidance Contr.*, vol. 4, no. 5, pp. 523-529, 1981.

[22] K. Shin and H. Kim, "Derivation and application of hard deadlines for real-time control systems", *IEEE Trans. Sys., Man Cybernet.*, vol. 22, no. 6, pp. 1403-1412, 1992.

[23] H. Kim and K. Shin, "Reliability modeling of real-time systems with deadline information", *Proc. IEEE Aerospace Conf.*, 1997.

[24] E. Çinlar, *Introduction to Stochastic Processes*, Prentice-Hall, Englewood Cliffs, 1975.

[25] G. Takahara, *Lecture Notes on Applied Stochastic Processes*, [online]available: http:// www.mast.queensu.ca/ ∼stat455.

[26] H. Li and Q. Zhao, "Analysis of fault tolerant control by using randomized algorithms", *Proc. American Contr. Conf.*, 2005.

[27] R. Stengel and L. Ray, "Stochastic robustness of linear time-invariant control systems", *IEEE Trans. Automat. Contr.*, vol. 36, no. 1, pp. 82-87, 1991.

[28] I. Yaesh, S. Boyarski and U. Shaked, "Probability-guaranteed robust H_∞ performance analysis and state-feedback design", *Sys. Contr. Lett.*, vol. 48, no. 5, pp. 351-364, 2003.

[29] R. Tempo, E. Bai and F. Dabbene, "Probabilistic robustness analysis: explicit bounds for the minimum number of samples", *Sys. Contr. Lett.*, vol. 30, no. 5, pp. 237-242, 1997.

[30] N. Limnios and G. Oprisan, *Semi-markov Processes and Reliability*, Birkhauser, Boston, 2001.