Maintenance modeling and scheduling in fault tolerant control

Hongbin Li, Qing Zhao*

Department of Electrical and Computer Engineering, University of Alberta

Edmonton, Alberta, Canada, T6G 2V4

Abstract

This paper studies the modeling and scheduling problem of maintenance strategies in Fault Tolerant Control Systems (FTCS's) using stochastic modeling method. In FTCS's, the controller reconfigures itself to accommodate for the occurrence of critical faults based on the information obtained from a fault detection and identification (FDI) scheme. Discrete semi-Markov chains are constructed to describe the operation of FTCS's with their unique characteristics incorporated. Two different maintenance strategies are discussed: FDI-dependent and FDI-independent periodic strategies, classified based on the use of FDI information in maintenance decision making. For each strategy, we present the methods of calculating the stationary availability and determining the optimal maintenance strategy to achieve the best availability. Two examples are given to demonstrate the proposed methods for both of FDI-dependent and -independent cases.

Keyword: Maintenance, fault tolerant control systems, semi-Markov processes

1 Introduction

Component faults in a control system may result in sudden system failures causing major damages and economic losses. Aiming to improve system safety and availability, Fault Tolerant Control systems (FTCS's) have been developed to accommodate fault effects by employing analytic redundancies, and performing fault detections and controller reconfigurations. A fault tolerant control system has two important schemes, one is called fault detection and identification (FDI) scheme which performs diagnosis of faults; the other is called reconfigurable control

*Corresponding author. Tel. +1-780-492-5792. Fax +1-780-492-1811. *E-mail:* qingzhao@ece.ualberta.ca.

(RC) scheme, which reconfigure itself based on the fault information provided by FDI to compensate for the fault effects. The objective of FTCS's is to prevent system from catastrophic failure. This is extremely important for safety critical systems.

In order to reduce accumulated deterioration, maintenance is undertaken regularly as a preventive activity when the system is satisfactorily operating in an up state. On the other hand, repair is to bring the system back to an up state after it has experienced a failure. Maintenance cost is usually much less than repair cost, hence it is important to study and make appropriate maintenance decisions. This paper discusses the maintenance modeling and scheduling in FTCS's. In general, the design and analysis of FTCS's belong to the subject of control system and engineering, and the problem of major concern is to maintain high-priority performance of the system when severe component faults occur. However, faults occurrences are primarily caused by component aging or deteriorating effects, as a well-defined system, maintenance of FTCS's is necessary.

The maintenance policies can be generally classified into condition-based and time-based periodic maintenances. In the former case, maintenance decisions are made based on the deterioration condition of the system; in the latter case, maintenance activities are performed at scheduled time intervals. These maintenance strategies have been investigated in various systems and configurations. Markov process and semi-Markov process have served as important tools in the investigation. For example, a semi-Markov decision process was used in [1] to solve a joint optimization of inspection rate and maintenance decisions; in [2], a model was developed to provide maintenance decision for a deteriorating system modeled by Markov chain; the long-run cost was minimized in [3] and [4] by using a semi-Markov decision process and defining its states based on different thresholds of failure rates; considering a finite time period, maintenance policy was studied in [5] for a repairable systems based on a semi-Markovian process. Previous results on maintenance can be found in a review paper by [6]. However, to the best of authors' knowledge, the maintenance of FTCS's has not been studied.

Different from available results, the maintenance of FTCS's has to consider their unique characteristics: in FTCS's, the system performance is maintained by using analytical redundancies , i.e. FDI scheme and control actions. Both FDI and controller reconfiguration have critical timing requirement. Moreover, the possible error made by FDI may lead to further deterioration of the system and even to a system failure. In simple words, the existence of FDI and automatic control action as well as their interactions make it difficult to model and

analyze overall system operations from reliability and maintenance perspective. In [7] and [8], efforts were made to construct a model for reliability evaluation of FTCS's based on Markov and semi-Markov processes. In this paper, discrete semi-Markov chains are used to describe the stochastic evolution of the system. Both time-based and condition-based maintenance strategies are studied, and they are named herein as FDI-independent and FDI-dependent maintenance respectively. The scheduling methods are discussed to find the optimal maintenance period with the best stationary availability for each case.

This paper is organized as follows. The description of FTCS's and the semi-Markov modeling are given in Section 2; the modeling and scheduling of two types of maintenance policies are discussed in Section 3 and 4; and two numerical examples are provided in Section 5 followed by conclusions in Section 6.

2 System description

FTCS's are mainly composed of two subsystems: a Fault Detection & Isolation (FDI) scheme and a reconfigurable controller, as shown in Figure 1. The FDI scheme provides fault diagnosis information on the kind, location, and occurrence time of faults, and the reconfigurable controller is modified to maintain system performance based on FDI information.

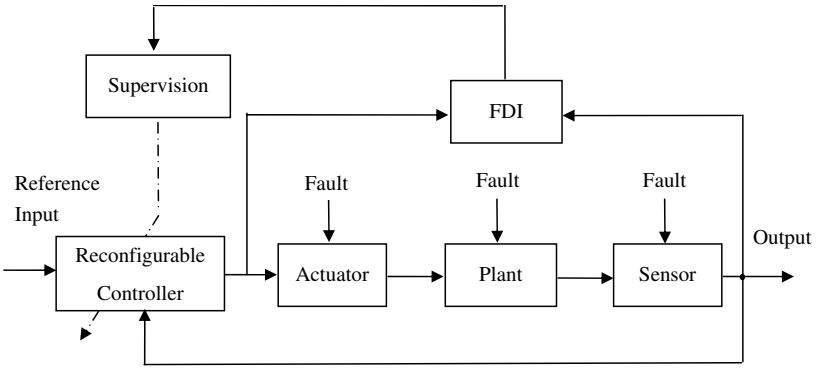

Figure 1: Structure of FTCS's

Most FDI schemes are designed based on the assumption of known system models, as shown in Figure 2. Its main idea is to check the consistency between process measurement and corresponding estimate calculated from process model. A residual signal is generated indicating fault occurrences. Various methods can be applied for residual generation, such as observer-based design and identification-based schemes.

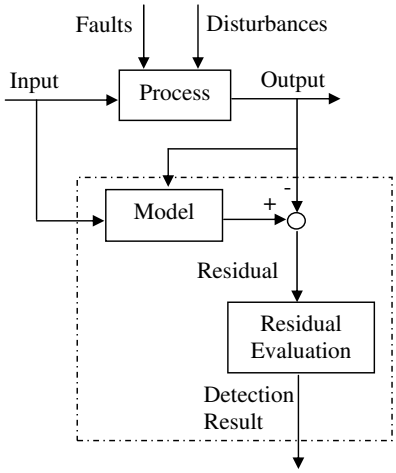

Figure 2: Structure of model-based FDI.

Reconfigurable control is designed to maintain acceptable control performance under fault occurrences by modifying controller according to FDI results. For example, the control law scheduling method pre-computes gain parameters for all faulty cases and switches to the corresponding gain when fault occurs

To recap, this description of FTCS's contains the following assumptions:

1) There are finite number of fault scenarios in the system, and the dynamics for each fault scenario can be effectively represented by a linear system model; the fault-free mode and various fault occurrence scenarios are defined as plant modes, which are collectively denoted as $S = \{0, 1, 2, \cdots, N\}$.

2) FDI modes determine controller reconfigurations and may take different state from plant mode; reconfigurable controller contains a bank of controllers that are pre-designed for the system.

3) Both the plant mode (i.e., fault scenario) and FDI mode determine system performance: if they are identical, implying that FDI result is correct and controller is used for its designated scenario, system performance is deemed as satisfactory; otherwise, FDI provides incorrect fault estimation, system performance is not desirable, and system is deemed to fail if the duration at this mismatched state exceeds a certain threshold denoted as T_{hd}.

3 Stochastic modeling

The FDI scheme is assumed to be in a cyclic structure: it generates an estimate based on a batch of measurement data and calculations for every fixed period T_{s}. Let $\theta_m \in S$ and $T_m \in \mathbb{N}$ denote the FDI mode and cycle index respectively after the m-th transition of η_n, where $m \in \mathbb{N}$ and $\mathbb{N}$ denotes the set of non-negative integers. For example, in Figure 3, $\theta_1 = \eta_5$ and $T_2 = 5$. θ_m and T_m together determine FDI trajectory, and $\eta_n = \theta_{S_n}$, where $S_n = \sup\{m \in \mathbb{N} : T_m \leq n\}$ is the discrete-time counting process of the number of jumps in $[1, n]$. Corresponding to FDI cycles, a discrete-time Markov chain ζ_n can be used to describe the stochastic evolution of plant mode by assuming that the failure rate is constant, where $n \in \mathbb{N}$ and the time duration between consecutive discrete indices is equal to FDI detection period T_{s}. Let G denote the transition probability matrix of ζ_n, and then $\Pr\{\zeta_{n+1} = j | \zeta_n = i\} = G_{ij}$, where G_{ij} denotes the ij-th element, $i, j \in S$.

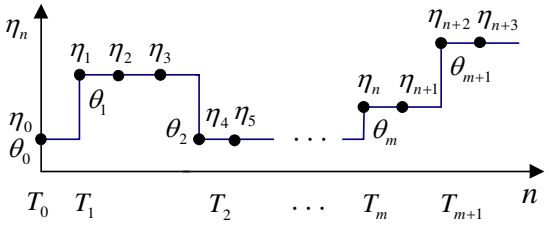

Figure 3: A sample path of η_n.

$(\theta, T) \triangleq \{\theta_m, T_m : m \in \mathbb{N}\}$ is called a discrete-time Markov renewal process if

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

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

Given $\zeta_{T_m} = \zeta_{T_m+1} \cdots = \zeta_{T_{m+1}} = k$, let $\tau_{ij}^k = T_{m+1} - T_m$ if $\theta_m = i$ and $\theta_{m+1} = j$, $i, j, k \in S$. τ_{ij}^k is the sojourn time of η_n between its transition to state i at T_m and the consecutive transition to j at T_{m+1}. If the transition destination state is not specified, let τ_i^k denote the sojourn time at state i. Let $H^k(i, j, l)$ denote the sojourn time distribution function, meaning $\Pr\{\tau_{ij}^k = l\} = \Pr\{T_{m+1} - T_m = l | \theta_m = i, \theta_{m+1} = j\} = H^k(i, j, l)$, where $i, j \in S$ and $l \in \mathbb{N}$.

Note that the behavior and parameters of η_n depend on ζ_n as η_n is an estimate of ζ_n. According to system description, the states of ζ_n and η_n and their interaction are the key elements to system operation. A discrete-time stochastic process can be defined as $X_n = (\zeta_n, \eta_n)$ and its state space $S_X = S \times S$.

Lemma 1 *X_n can be modeled as a semi-Markov chain.*

Proof: Let T_m^X denote the transition time when ζ_n or/and η_n jumps to a different state. Denote θ_m^X as the state of X_n at the transition time T_m^X. It suffices to show that $(\theta^X, T^X) \triangleq \{\theta_m^X, T_m^X : m \in \mathbb{N}\}$ is a Markov renewal process. In other words, the following equation holds:

$$\Pr\{\theta_{m+1}^X = (k,l), T_{m+1}^X - T_m^X = h | \theta_0^X, \cdots, \theta_m^X, T_0^X, \cdots, T_m^X\}$$

$$= \Pr\{\theta_{m+1}^X = (k,l), T_{m+1}^X - T_m^X = h | \theta_m^X = (i,j)\}. \quad (1)$$

This equation is shown based on three cases. The first case is that only ζ_n transits to a new state at T_m^X. As a result, the parameters of η_n are changed. So the sojourn time of η_n is reset to 0, considering that the state of η_n remains unchanged but it begins to evolve according to a new parameter. Consequently, the transitions of η_n depends on θ_m^X only. This also holds for the transition of ζ_n because of its latest transition at T_m^X. Therefore, (1) holds.

The second case is that η_n transits at T_m^X while ζ_n remains the same. In this case, the sojourn time of η_n starts at 0 at a new state, so its transition is independent of previous states before T_m^X. Considering that ζ_n is a Markov chain, its transition depends on θ_m^X only because this is the most recent state. Therefore, (1) also holds.

The third case is that both ζ_n and η_n change at T_m^X. In this case, both ζ_n and η_n start to evolve at new states, and (1) holds obviously. ■

Remark 1 *In general, the combination of a Markov and an independent semi-Markov chain is not a semi-Markov chain. Lemma 1 is mainly because of the dependence of the parameters of η_n on ζ_n.*

Using the total probability formula, the semi-Markov kernel of X_n can be calculated from the parameters of ζ_n and η_n. For brevity, the calculation formulas are given in the following theorem without proof. Please refer to [8] for the derivation.

Theorem 1 *The semi-Markov kernel of X_n is given by the following equations:*

$$\begin{aligned}
Q_X((i,j),(k,l),m) &= G_{ii}^{m-1} G_{ik} P_{jl}^i H^i(j,l,m), \\
Q_X((i,j),(i,l),m) &= P_{jl}^i H^i(j,l,m) \sum_{n=1}^{\infty} G_{ii}^n \sum_{k\in S_1} P_{jk}^i \sum_{h=1}^{n} H^i(j,k,h), \\
Q_X((i,j),(k,j),m) &= G_{ii}^{m-1} G_{ik} [1 - \sum_{n=1}^{\infty} G_{ii}^{n-1}(1-G_{ii}) \sum_{l\in S_1} P_{jl}^i H^i(j,l,n) \\
&\quad - \sum_{n=1}^{\infty} G_{ii}^n \sum_{l\in S_1} P_{jl}^i \sum_{h=1}^{n} H^i(j,l,h)],
\end{aligned}$$

where $m \in \mathbb{N}$, G denotes the transition matrix of ζ_n, P^i the transition matrix of the embedded Markov chain of η_n when $\zeta_n = i$, and H^i the matrix of sojourn time distribution functions of η_n when $\zeta_n = i$. (i,j) and (k,l) denote the states of X_n, $i \neq k$, $j \neq l$.

X_n is the key semi-Markov process determining system operation, and by expanding its state space, reliability, repair and maintenance can be described by similar stochastic processes.

To model reliability, $\bar{X}_n$ is defined as a discrete-time semi-Markov chain with state space $S_{\bar{X}} = S_X \cup \{\mathrm{F}\}$, where F denotes the absorbing failure state, and others are up states. The state transition diagram when $S = \{0,1\}$ is shown in Figure 4. The reliability at nT_s, defined as the probability of staying within functional states for $[0, nT_\mathrm{s}]$, is equal to

$$R_n = 1 - \Pr\{X_n = \mathrm{F} | X_0 = (0,0)\}, \tag{2}$$

where R_n denotes the reliability function at nT_s and $P((0,0),\mathrm{F},n)$ the transition probability from (0, 0) to F. Therefore the key step of evaluating reliability is to obtain the semi-Markov kernel of $\bar{X}_n$ and to solve its transition probability.

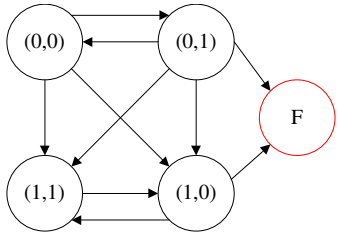

Figure 4: State transition diagram of $\bar{X}_n$.

Theorem 2 *The semi-Markov kernel of $\bar{X}_n$ can be derived by that of X_n, as given by the*

following equations:

$$Q_{\bar{X}}((i,i),(k,l),m) = Q_X((i,i),(k,l),m), \tag{3}$$

$$Q_{\bar{X}}((i,j),(k,l),m) = \begin{cases} Q_X((i,j),(k,l),m), \ m \leq T_{\text{hd}}, \\ 0, \ m > T_{\text{hd}}, \end{cases} \tag{4}$$

$$Q_{\bar{X}}((i,j),\text{F},m) = \begin{cases} 1 - \sum_{h=1}^{T_{\text{hd}}} Q((i,j),(k,l),h), \ m = T_{\text{hd}}+1, \\ 0, \ \text{otherwise}, \end{cases} \tag{5}$$

$$Q_{\bar{X}}(\text{F},a,m) = 0, \tag{6}$$

where $(i,i),(i,j),(k,l),a \in S_{\bar{X}}$, $i \neq j$, $m \in \mathbb{N}$ *and* T_{hd} *denotes the hard deadline.*

Proof: These equations are derived based on the connections between X_n and $\bar{X}_n$ and the implication of hard deadline. (3) is obvious, because it represents the transition probability of X_n and has been given by the semi-Markov kernel of X_n in Lemma 1. (6) holds as the failure state F is assumed to be absorbing. (4) and (5) are based on the hard deadline concept: When $\bar{X}_n = (i,j)$, $i \neq j$, the system is in a mis-matched mode that FDI gives an incorrect detection; the transition from (i,j) to other functional states (k,l) can be made within T_{hd} only, which leads to (4); if the system stays at (i,j) for a sojourn time over T_{hd}, it transits to the absorbing failure state at the earliest time $T_{\text{hd}}+1$, which is described by (5). ■

With semi-Markov kernel, transition probability is readily solved by using available formulas [9], and reliability function R_n can be calculated from (2). In the next two sections, two maintenance policies are presented. The problem of interest is to find the optimal maintenance period to minimize costs and maximize availability. By representing the maintenance and repair costs in the corresponding duration times, stationary availability is used as the overall maintenance scheduling objective.

4 Maintenance with dependence on Fault Detection and Identification (FDI)

4.1 Semi-Markov modeling

Consider the following FDI-dependent maintenance policy: when FDI mode is 0, indicating a fault-free operation, no maintenance action is needed; when FDI mode is i, $i \in S_1$, $i \neq 0$, maintenance is undertaken when the sojourn time is over T_{M}^i, an FDI -dependent maintenance

period; and an emergency repair state is conducted immediately after system fails. The durations of the repair and maintenance are described by two discrete random variables, denoted by D_{R} and D_{M} respectively and representing the multiples of T_{s}.

To describe the system operation under this maintenance policy, a discrete stochastic process Y_n is defined on the state space $S_Y = S_X \cup \{\mathrm{M}, \mathrm{R}\}$, where M denotes the maintenance state, and R the repair state. For the case of binary fault modes, the state transition diagram is shown in Figure 5.

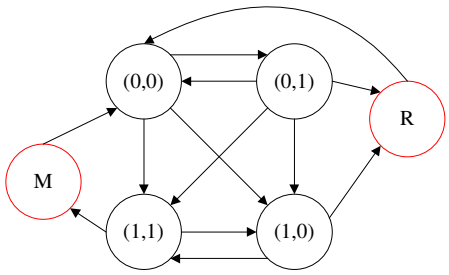

Figure 5: State transition diagram of Y_n.

It can be shown that Y_n is also a semi-Markov chain, and its semi-Markov kernel can be derived from those of X_n and $\bar{X}_n$. The proofs are similar to those of Lemma 1 and Theorem 2 and omitted here for brevity.

Theorem 3 *The semi-Markov kernel of Y_n is given by the following equations:*

$$
\begin{aligned}
Q_Y((0,0),(k,l),m) &= Q_X((0,0),(k,l),m), \\
Q_Y((i,j),(k,l),m) &= Q_{\bar{X}}((i,j),(k,l),m), \\
Q_Y((i,j),\mathrm{R},m) &= Q_{\bar{X}}((i,j),\mathrm{F},m), \\
Q_Y((i,i),(k,l),m) &= \begin{cases} Q_X((i,i),(k,l),m), & m \le T_{\mathrm{M}}^i, \\ 0, & m > T_{\mathrm{M}}^i, \end{cases}
\end{aligned}
$$

$$
\begin{aligned}
Q_Y((i,i),M,m) &= \begin{cases} 1 - \sum_{h=1}^{T_{\mathrm{M}}^i} Q_X((i,j),(k,l),h), & m = T_{\mathrm{M}}^i + 1, \\ 0, & \text{otherwise}, \end{cases} \\
Q_Y(\mathrm{R},(0,0),m) &= F_{\mathrm{R}}(m), \\
Q_Y(\mathrm{M},(0,0),m) &= F_{\mathrm{M}}(m), \\
Q_Y(\mathrm{M},a,m) &= Q_Y(\mathrm{F},a,m) = 0,
\end{aligned}
$$

where $(i,i),(i,j),(k,l),a \in S_Y$, $a \neq (0,0)$, $i \neq 0$, $i \neq j$, $m \in \mathbb{N}$, *and* T_{hd} *denotes the hard deadline.* F_{M} *and* F_{R} *denote the discrete probability distributions functions of* D_{M} *and* D_{R} *respectively, the maintenance and repair durations.*

4.2 Maintenance scheduling

With Y_n constructed by Theorem 4, its stationary availability A_1, defined as the stationary probability that the system is in a up state, can be calculated by the following equation: [9]:

$$A_1 = \frac{\sum_{i=1}^{N_{\text{u}}} v_i m_{Yi}}{v^T m_Y}, \tag{7}$$

where v is denoted as the stationary distribution of the embedded Markov chain of Y_n, and m_Y the mean sojourn time of the states of Y_n, in which the first N_{u} elements denote the mean sojourn time for up states.

The vector of FDI dependent maintenance periods is denoted as $\mathbf{T}_{\text{M}} = [T_{\text{M}}^1 \ \cdots \ T_{\text{M}}^{N_1}]^T$. The interested problem is to find the optimal $\mathbf{T}_{\text{M}}$ to achieve the maximum of A_1. The main idea is to calculate the gradient of A_1 with respect to $\mathbf{T}_{\text{M}}$, and to use an iterative gradient search algorithm to find the optimum $\mathbf{T}_{\text{M}}^*$: at $\mathbf{T}_{\text{M}} = x_k$,

$$x_{k+1} = x_k + \lambda \nabla A_1|_{x_k},$$

where $\nabla A_1|_{x_k}$ represents the gradient of A_1 at $\mathbf{T}_{\text{M}} = x_k$, and λ step size. From (7), we have

$$\nabla A_1 = \frac{dA_1}{dv}\frac{dv}{d\mathbf{T}_{\text{M}}} + \frac{dA_1}{dm_Y}\frac{dm_Y}{d\mathbf{T}_{\text{M}}}, \tag{8}$$

where $\frac{dA_1}{dv}$ and $\frac{dA_1}{dm_Y}$ can be directly obtained from (7), and it remains to calculate $\frac{dv}{d\mathbf{T}_{\text{M}}}$ and $\frac{dm_Y}{d\mathbf{T}_{\text{M}}}$.

According to semi-Markov process theory [10], v is obtained based on the transition matrix of the embedded Markov chain of Y_n, denoted as P, and

$$P_{ij} = \sum_{k=1}^{\infty} Q_Y(i,j,k), \tag{9}$$

$$m_{Yi} = \sum_{k=1}^{\infty} k \sum_{j=1}^{N_Y} Q_Y(i,j,k), \tag{10}$$

where P_{ij} denotes the (i,j)-th element of P, and m_{Yi} i-th element of m_Y, $i,j \in S_Y$. According to Theorem 3, the semi-Markov kernel Q_Y is a matrix function of $\mathbf{T}_{\text{M}}$. So both v and m_Y vary with $\mathbf{T}_{\text{M}}$.

Considering that maintenance period T_{M}^k is usually in a higher order of T_{s}, the following differences are used to approximate $\frac{dm_Y}{d\mathbf{T}_{\mathrm{M}}}$:

$$\frac{dm_{Yi}}{dT_{\mathrm{M}}^k} \approx m_{Yi}|_{[T_{\mathrm{M}}^1 \ \cdots (T_{\mathrm{M}}^k+1) \cdots T_{\mathrm{M}}^{N_1}]^T} - m_{Yi}|_{[T_{\mathrm{M}}^1 \ \cdots T_{\mathrm{M}}^k \cdots T_{\mathrm{M}}^{N_1}]^T}, \tag{11}$$

where $P_{ij}|_{[T_{\mathrm{M}}^1 \ \cdots (T_{\mathrm{M}}^k+1) \cdots T_{\mathrm{M}}^{N_1}]^T}$ denotes the (i,j) element of P evaluated at $\mathbf{T}_{\mathrm{M}} = [T_{\mathrm{M}}^1 \ \cdots (T_{\mathrm{M}}^k + 1) \cdots T_{\mathrm{M}}^{N_1}]^T$.

To calculate $\frac{dv}{d\mathbf{T}_{\mathrm{M}}}$, the following result on the derivative of the stationary distribution of Markov chain is adopted [11]:

$$\frac{dv}{dT_{\mathrm{M}}^k} = v^T \frac{dP}{dT_{\mathrm{M}}^k}(I-P)^{\#}, \tag{12}$$

where I denotes the identity matrix and $(I-P)^{\#}$ denotes the group inverse [11]. In addition,

$$\frac{dP_{ij}}{dT_{\mathrm{M}}^k} \approx P_{ij}|_{[T_{\mathrm{M}}^1 \ \cdots (T_{\mathrm{M}}^k+1) \cdots T_{\mathrm{M}}^{N_1}]^T} - P_{ij}|_{[T_{\mathrm{M}}^1 \ \cdots T_{\mathrm{M}}^k \cdots T_{\mathrm{M}}^{N_1}]^T}, \tag{13}$$

where $P_{ij}|_{[T_{\mathrm{M}}^1 \ \cdots (T_{\mathrm{M}}^k+1) \cdots T_{\mathrm{M}}^{N_1}]^T}$ denotes the (i,j) element of P evaluated at $\mathbf{T}_{\mathrm{M}} = [T_{\mathrm{M}}^1 \ \cdots (T_{\mathrm{M}}^k + 1) \cdots T_{\mathrm{M}}^{N_1}]^T$. Substitute (13) to (12), $\frac{dv}{d\mathbf{T}_{\mathrm{M}}}$ is obtained. ∇A_1 can be calculated by substituting $\frac{dv}{d\mathbf{T}_{\mathrm{M}}}$ and $\frac{dm_Y}{d\mathbf{T}_{\mathrm{M}}}$ to (8). The gradient search algorithm is finally implemented to find the optimum.

5 Periodic maintenance independent of Fault Detection and Identification (FDI)

Consider the following periodic maintenance strategy for an FTCS system described by $\bar{X}_n$ in Figure 1: The initial state of the system is assumed to be fault-free, $\zeta_0 = \eta_0 = 0$; for every period T_{M}, if the system is up, it goes to the maintenance state which brings the system to the initial state; and if the system is under repair at T_{M}, we continue the repair, after which the system restarts from the initial state.

This maintenance policy and operation cycle can be considered as a special case of the system described in [12], and we therefore have the following result available for maintenance scheduling.

Lemma 2 *[12] The mean duration time of maintenance and repair are denoted as S_M and S_R respectively. The reliability function of the system without maintenance and repair is denoted as $R(t)$. The stationary availability $A_2(T_M)$ of the overall system with maintenance period T_M is then given as follows:*

$$A_2(T_M) = \frac{1}{1+B(T_M)}, \tag{14}$$

$$B(T_M) = \frac{S_R + (S_M - S_R)R(T_M)}{\int_{t=0}^{T_M} R(t)dt}. \tag{15}$$

Taking derivative with respect to $T_{\rm M}$, we have

$$B'(T_{\rm M}) = [(S_{\rm M} - S_{\rm R})R'(T_{\rm M}) \int_{t=0}^{T_{\rm M}} R(t)dt - S_{\rm R} \cdot R(T_{\rm M}) + (S_{\rm M} - S_{\rm R})R^2(T_{\rm M})]/(\int_{t=0}^{T_{\rm M}} R(t)dt)^2.$$

$B'(T_{\rm M}) > 0$ if and only if

$$f(T_{\rm M}) := \frac{R(T_{\rm M})}{R^2(T_{\rm M}) - R'(T_{\rm M}) \int_{t=0}^{T_{\rm M}} R(t)dt} < 1 - \frac{S_{\rm M}}{S_{\rm R}}.$$

Usually the cost of repair is much higher than scheduled maintenance cost due to the interception of regular operations, so $\frac{S_{\rm M}}{S_{\rm R}} < 1$. If $\lim_{T_{\rm M}\to\infty} f(T_{\rm M}) > 1 - \frac{S_{\rm M}}{S_{\rm R}}$, then

$$\lim_{T_{\rm M}\to\infty} B'(T_{\rm M}) < 0, \quad \lim_{T_{\rm M}\to\infty} A_1'(T_{\rm M}) > 0.$$

It implies that the stationary availability is monotonously increasing when $T_{\rm M}$ is large enough, and the best strategy is not to take maintenance. So the relation between $f(T_{\rm M})$ and $\frac{S_{\rm M}}{S_{\rm R}}$ determines the existence of optimal maintenance period, as summarized in the following theorem.

Theorem 4 *An optimal FDI-independent periodic maintenance period exists if and only if* $\lim_{T_M\to\infty} f(T_M) < 1 - \frac{S_M}{S_R}$*, and* $f(T_M) = 1 - \frac{S_M}{S_R}$ *at the optimum.*

Using the reliability predication available at discrete points $nT_{\rm s}$ provided by $\bar{X}_n$, the following equation is used to estimate $f(T_{\rm M})$:

$$f(T_{\rm M}) \approx \frac{R_{T_{\rm M}}}{R_{T_{\rm M}}^2 - [R_{T_{\rm M}+1} - R_{T_{\rm M}}] \sum_{n=0}^{T_{\rm M}} R_n}, \tag{16}$$

where $T_{\rm M} \in \mathbb{N}$, and $R_{T_{\rm M}}$ represents the reliability prediction at $T_{\rm M}T_{\rm s}$.

6 Examples

6.1 Example 1: Fault detection and identification (FDI) dependent maintenance

Consider an FTCS with two plant modes: 0 and 1, denoting the fault-free mode and faulty mode respectively. A discrete Markov chain with the following transition matrix is used to describe fault occurrence.

$$G = \begin{bmatrix} 0.983 & 0.017 \\ 0 & 1 \end{bmatrix}.$$

Assume $T_{\rm s} = 1$ minute. According to G, the mean time of fault occurrence is $1/0.017 = 60$ minutes.

The FDI is modeled by a semi-Markov chain η_n with the following parameters.

$$P^0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ P^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$H^0(0,1,m) = H^1(1,0,m) = \mathrm{Ps}(m|60),$$

$$H^0(1,0,m) = H^1(0,1,m) = \mathrm{Bn}(m|5,0.5),$$

where P^0 and P^1 are transition probability matrices of the embedded Markov chain and $H^0(0,1,m),\ H^0(1,0,m),\ H^1(0,1,m),\ H^1(1,0,m)$ are distribution functions of sojourn time. 'Ps$(\cdot|\cdot)$' and 'Bn$(\cdot|\cdot,\cdot)$' denote the Poisson and Binomial distributions respectively:

$$\mathrm{Ps}(m|60) = \frac{60^m}{m!}e^{-60},$$

$$\mathrm{Bn}(m|5,0.5) = \frac{5!}{m!(5-m)!}0.5^m 0.5^{5-m}, m \le 5.$$

The maintenance and repair durations follow Binomial distributions: Bn$(\cdot|200,0.5)$ and Bn $(\cdot|20,0.5)$. The hard deadline $T_{\rm hd} = 5$.

Let the initial maintenance period $T_{\rm M} = 80$. Y_n is constructed using Theorem 3, and its transition probabilities are shown in Figure 6, which converges to steady state values in the long run. The stationary availability in this case is calculated as 0.7368.

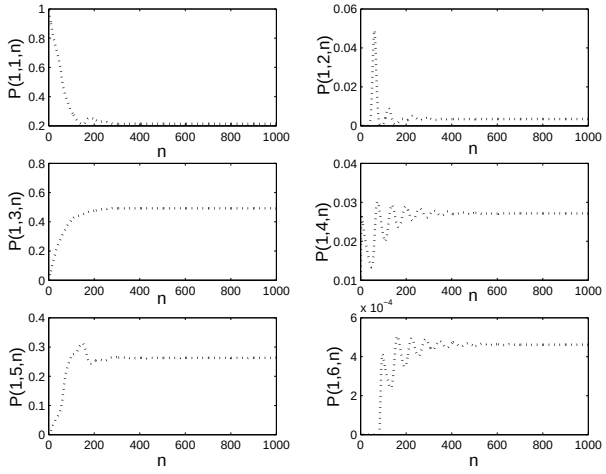

Figure 6: Transition probability functions.

Using the gradient search algorithm to optimize T_{M}, it takes 27 iterations to find the optimum $T_{\mathrm{M}}^{*} = 54$ with availability 0.7525, as shown in Figure 7. So the gradient algorithm is effective on maintenance scheduling.

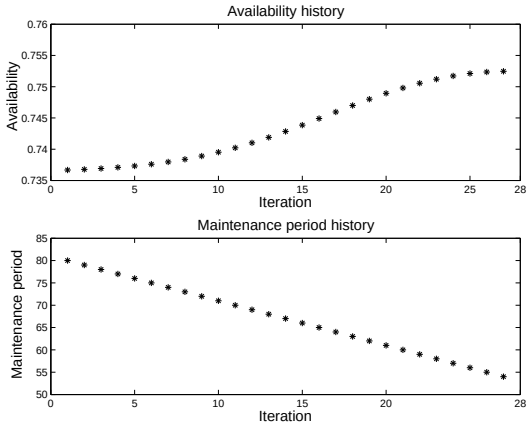

Figure 7: The history of searching the optimal maintenance period.

6.2 Example 2: Periodic maintenance

Consider the same system as in Example 1 but with the FDI-independent maintenance. The system parameters remain the same as in Example 1. To evaluate its reliability, $\bar{X}_n$ is constructed based on Theorem 2, and the calculated transition probability and the reliability functions are shown in Figure 8.

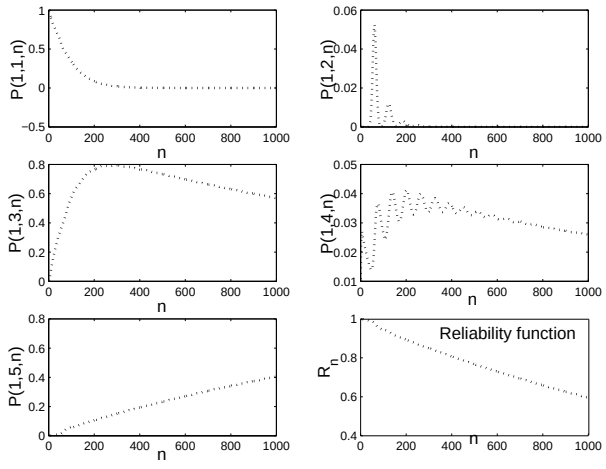

Figure 8: Transition probability and reliability functions.

Assume maintenance and repair are available for this system with mean duration times

as: $S_M = 5$ and $S_R = 100$. To find out if reliability can be improved by taking preventive maintenance, $f(T_{\rm M})$ is calculated using reliability prediction and (16), as shown in the first curve of Figure 9. As we can see, $f(T_{\rm M})$ converges to a constant slightly over 1. Based on Theorem 4, no maintenance is needed for this system, as verified by the stationary availability $A(T_{\rm M})$ in Figure 9.

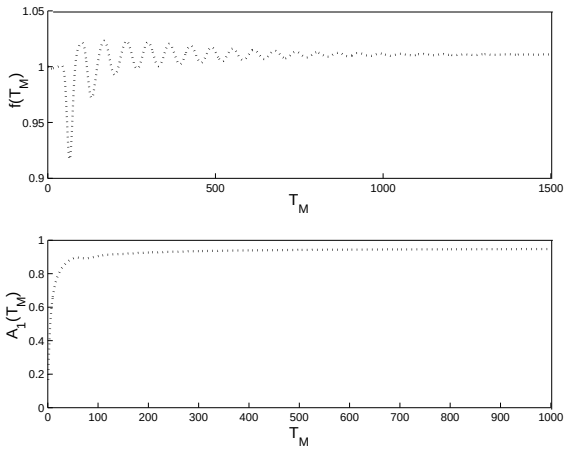

Figure 9: $f(T_{\rm M})$ and stationary availability.

Now, let us change the sojourn time distribution of FDI to the following:

$$H'^0(0,1,m) = H'^1(1,0,m) = \mathrm{Ps}(m|60),$$

$$H'^0(1,0,m) = H'^1(0,1,m) = \mathrm{Bn}(m|8,0.5).$$

The transition probability and the reliability functions of the new system are given in Figure 10. Obviously, the reliability of this system is much worse than the original system in Figure 8.

In a similar way, $f(T_{\rm M})$ of this new system is calculated and shown in Figure 11. As $f(T_{\rm M})$ converges to 0.66 approximately, a optimal maintenance period exists if the $S_{\rm M}/S_{\rm R} < 0.34$. For instance, if $S_{\rm R} = 100$ and $S_{\rm M} = 19$, the optimal maintenance period exists, which can be found by solving $f(T_{\rm M}) = 1 - S_{\rm M}/S_{\rm R} = 0.81$. As shown in Figure 11, $T_{\rm M} = 33$ is found to be the optimal maintenance period.

This example shows that the FDI sojourn time distribution has a crucial influence on reliability and maintenance scheduling, and Theorem 4 can be used to check the existence of the optimal maintenance period.

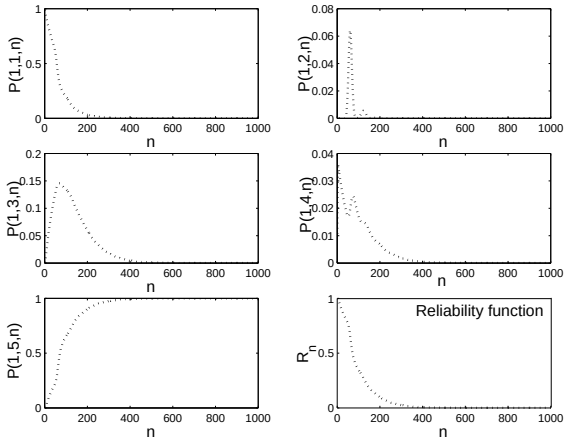

Figure 10: Transition probability and reliability functions.

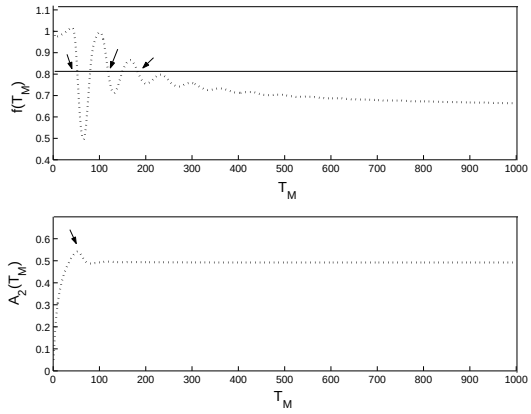

Figure 11: $f(T_{\mathrm{M}})$ and stationary availability.

7 Conclusions

In this paper, the maintenance modeling and scheduling problem in fault tolerant control systems is treated. Although commonly studied for industry systems in the community of reliability engineering, this problem has not been fully investigated for dynamical control systems, especially for fault tolerant control systems that are designed for safety critical systems to achieve high reliability and availability. Discrete semi-Markov process models are applied to describe the system operation of FTCS's, incorporating unique dynamical relationships among controller, systems and fault detection and identification components. Two types of maintenance, FDI-dependent and periodic FDI-independent strategies, are proposed; and we present the methods of calculating the stationary availability and finding the optimal maintenance periods for each strategy. Theses methods are illustrated at last by numerical examples.

References

[1] **Chen, D.** and **Trivedi, K.**, Optimization for condition-based maintenance with semi-markov decision process. *Reliability Engineering & System Safety*, 2005, 90, 25–29.

[2] **Chiang, J.** and **Yuan, J.**, Optimal maintenance policy for a markovian system under periodic inspection. *Reliability Engineering and System Safety*, 2001, 71(2), 165–172.

[3] **Berenguer, C.**, **Chu, C.**, and **Grall, A.**, Inspection and maintenance planning: an application of semi-markov decision processes. *Journal of Intelligent Manufacturing*, 1997, 8, 467–476.

[4] **Moustafa, M.**, **Abdel, E.**, and **Sadek, S.**, Optimal major and minimal maintenance policies for deteriorating systems. *Reliability Engineering and System Safety*, 2004, 83(3), 363–368.

[5] **Crespo, A.** and **Sánchez, A.**, Models for maintenance optimization: a study for repairable systems and finite time periods. *Reliability Engineering and System Safety*, 2002, 75(3), 367–377.

[6] **Valdez-Flores, C.** and **Feldman, R.**, A survey of preventive maintenance models for stochastically deteriorating single-unit systems. *Naval Research Logistics*, 1989, 36, 419–446.

[7] **Li, H.** and **Zhao, Q.**, Reliability modeling of fault tolerant control systems. In *Proc. IEEE Conference on Decision and Control* (Spain), 2005 .

[8] **Li, H.** and **Zhao, Q.**, Reliability evaluation of fault tolerant control systems with semi-markov FDI model. *Proceedings of the Institution of Mechanical Engineers, Part I - Journal of Systems and Control Engineering*, 2006, 220(I5), 329–338.

[9] **Barbu, V.**, **Boussemart, M.**, and **Limnios, N.**, Discrete-time semi-markov model of reliability and survival analysis. *Communications in Statistics Theory and Methods*, 2004, 33(11), 2833–2868.

[10] **Howard, R.**, *Dynamic Probabilistic Systems*, vol. II (Wiley, New York), 1971.

[11] **Golub, G.** and **Meyer, C.**, Using the qr factorization and group inversion to compute, differentiate, and estimate the sensitivity of stationary probabilities for markov chains. *SIAM Journal of Algebra and Discrete Methods*, 1986, 7(2), 273–281.

[12] **Bloch-Mercier, S.**, Stationary availability of a semi-markov system with random maintenance. *Applied Stochastic Models in Business and Industry*, 2000, 16, 219–234.