Article ID: 1000 - 8152(2005)04 - 0609 - 06

Fault diagnosis of timed event graph

XUE Fei, ZHENG Da-zhong
(Department of Automation, Tsinghua University, Beijing 100084, China)

Abstract: Timed event graphs (TEG) are an important subclass of Petri nets that are well adapted to model synchronizations. The problem of fault diagnosis for timed event graph is studied in this paper. Two different system faults are defined, transition invalidation fault and transition time-lag fault. The observable propagating path of invalidation fault is studied based on the relevance matrix of event graph, and fault character vector is firstly introduced to mark the propagating character of transition invalidation fault. Based on that, a sufficient and necessary condition of diagnosability for invalidation fault is given. For the time-lag fault, a simple fault diagnosis algorithm based on transition firing time estimation is given. Finally, the diagnosable condition is studied.

Key words: discrete event systems; fault diagnosis; Petri net; timed event graph; max-plus algebra
CLC number: TP306 **Document code**: A

基于赋时事件图的故障诊断

薛 飞, 郑大钟
(清华大学 自动化系, 北京 100084)

摘要: 赋时事件图(TEG)是一类用于描述同步特性的重要的 Petri 网. 本文提出并研究了基于赋时事件图的故障诊断问题. 文中定义了两类系统故障类型: 变迁失效(Invalidation)故障和变迁时间延迟(Time-lag)故障. 基于事件图关联矩阵, 通过研究变迁失效故障的可观测传播特性, 引入了故障特征向量的概念. 基于此, 给出了失效故障的可诊断性的充分必要条件. 对于时延故障, 提出了一种基于变迁触发时间估计进行故障诊断的简单算法. 并基于此算法, 研究了时延故障的可诊断条件.

关键词: 离散事件系统; 故障诊断; Petri 网; 赋时事件图; 极大代数

1 Introduction

For the problem of fault diagnosis of discrete event system, many results have been given and many effective methods have been proposed since 1994. Based on the definition of system fault, the methods can be classified into two kinds: state-based method and event-based method.

In [1], Lin proposed both on-line and off-line algorithms for the determination of input commands that detect failure states, and these algorithms are applied to mixed circuit. Moreover, distributed fault detection[2] and fault detection using templates[3] are investigated. In the above methods, they define failure states firstly, and then from (partially) observed data, they detect if current states are failure states or not. Thus, this method is a state-based method.

In [4 ~ 6], S. Lafortune et al. proposed a method for the design of an event-based fault diagnoser. The faults of system are defined as special unobservable transitions. Hence, the fault diagnosis is reduced to an estimation problem for occurrence of special events. In [7], this method was extended to Petri net model with faulty behaviors. In [8], this framework was extended to utilize information about the timing of events. In [10], the diagnoser method was extended to deal with the telecommunication network.

Both in the above methods, state-based and event-based method, it is assumed that the model of system failure behaviors are known explicitly. However, this assumption is not always satisfied in real industry systems. Moreover, the original methods proposed by Lin in [1] and Lafortune in [4 ~ 6] did not consider the timing information of systems. In [3,8,9], those methods are extended to timed discrete event systems and the timing information of system is used to improve the fault diagnosis precision. In those methods, the timing information is considered as the extending state or clock event of system. That results the state explosion.

Timed event graphs are an important subclass of Petri

Received date: 2003 - 09 - 18; Revised date: 2004 - 12 - 06.
Foundation item: Supported by National Science Foundation of China (60074012); the National Fundamental Research Funds (G1998020310).

nets that are well adapted to model synchronizations. Moreover, they can be considered as linear systems in max-plus algebra. A linear system theory has been developed using the conventional linear system theory as guideline. In this paper, the system is assumed to be partial observable and the fault diagnosis problem under partial observation is considered. Being different form above methods, system faults are defined as the abnormal behaviors of transitions. Two kinds of system faults –the invalidation fault and the time-lag fault– are defined. The fault-propagating path in system is studied based on relevance matrix. The fault character vector and the candidate fault set are defined for transition invalidation and lag fault respectively. Based on that, the necessary and sufficient conditions for fault detectability and diagnosability are also given. At the end of this paper, an example is given to illustrate the main results. Since the timing information is not considered as an extra event or state, the state explosion problem is avoided in on-line fault diagnosis.

2 System model

The discrete event systems considered in this paper are modeled in timed event graph. In this section, we formally define the timed event graph and give the definition of fault in system. For more details about discrete event and Petri net please refer to [11].

Definition 1 A Petri net is a 5-tuple $G = (P, T, I, O, M_0)$, where

1) P and T are finite set of places and transitions, respectively;

2) $P \cap T = \phi$ and $P \cup T \neq \phi$;

3) The function $I: P \times T \to \{0,1\}$ and $O: T \times P \to \{0,1\}$;

4) M_0 is the initial marking of Petri net.

Definition 2 Given a Petri net, place p is called the input or output place of transition $t \in T$ if it satisfies that $I(p,t) = 1$ or $O(p,t) = 1$. The sets of input and output places for transition $t \in T$ are denoted as ${}^*t = \{p \mid p \in P, p \text{ is an input place of } t\}$ and $t^* = \{p \mid p \in P, p \text{ is an output place of } t\}$ respectively. Similarly, transition t is called the input or output transition of place $p \in P$ if it satisfies that $O(t,p) = 1$ or $I(p,t) = 1$. ${}^*p = \{t \mid t \in T, t \text{ is an input transition of } p\}$ and $p^* = \{t \mid t \in T, t \text{ is an output transition of } p\}$ denote the input and output transition sets for place $p \in P$ respectively.

Definition 3 Giving a Petri net, it is an event graph if for any $p \in P$, there is only one input and output transition of this place, i.e. $\sum_{t \in T} I(p,t) = \sum_{t \in T} O(t,p) = 1$.

Definition 4 Timed event graph is an event graph that for any transition $t_i \in T$, there is h_i mark the lifetime of this transition, where h_i is a stochastic value that $h_i \in [\underline{h}_i, \bar{h}_i]$. $\underline{h}_i$ and $\bar{h}_i$ are the lower and upper bound of lifetime respectively.

The discrete event systems considered in this paper are modeled in timed event graph and are assumed to be partial observable. The transition set T can be partitioned in two subsets T_o and T_u that noted observable and unobservable transition sets respectively. And it satisfy that

$$T = T_o \cup T_u \text{ and } T_o \cap T_u = \phi.$$

Under partial observation, the fire of observable transition can be detected directly and the firing time can be measured. The fire of unobservable transition can not be detected directly and the firing time can not be measured.

Definition 5 A transition $t \in T$ is called an input of timed event graph if ${}^*t = \phi$. It is assumed that all input transitions are observable without exception. $U = \{u_l\} \in T_o$ denotes the set of input transitions for system. Without loss of generality, it is assume that $\forall p \in P, {}^*p \neq \phi$, i.e. there is no "input place" of system.

For timed event graph, the relevance matrix is always used to express the relationship between transitions. In this paper, the definition of relevance matrix has a small alteration to reflect the initial marking of system.

Definition 6 The relevance matrix of an event graph is $A = [a_{ij}]_{n\times}$, where $n = |T|$. The element a_{ij} of matrix is assigned as follows

$$a_{ij} = \begin{cases} \min\limits_{r} \{m_0(p_{ij}^r)\}, & \text{if } t_i^* \cap {}^*t_j \neq \phi, \\ +\infty, & \text{else}, \end{cases} \quad (1)$$

where $p_{ij}^r \in t_i^* \cap {}^*t_j$ and $m_0(p_{ij}^r)$ is the initial token in place p_{ij}^r, $r = 1,2,\cdots |t_i^* \cap {}^*t_j|$.

Definition 7 For the relevance matrix $A = [a_{ij}]_{n\times n}$, the operator $\otimes$ is defined as follows:

$$A \otimes B = [\min_k (a_{ik} + b_{kj})]_{n\times n} \text{ and}$$

$$A^k = \overbrace{A \otimes A \otimes \cdots \otimes A}^{k}.$$

Matrix $\bar{A} = [\bar{a}_{ij}]_{n\times n} = \min\limits_{k=1}^{n} \{A^k\}$ is called the closure of the relevance matrix.

The fault in system is defined as the abnormal behaviors of transitions. In this paper, two kinds of system faults, invalidation fault and lag fault, are considered.

Definition 8 (invalidation fault) An invalidation

fault τ_i in the timed event graph is the pair of transition and its fail time $\tau_i = (t_i, k)$. Here $t_i \in T$ is the transition of timed event graph and k is a positive integer that marked the transition breaks down at its k-th fire.

Definition 9(lag fault) A lag fault γ_i in the timed event graph is the triple of transition, its lag time and a positive integer, i.e. $\gamma_i = (t_i, \Delta, k)$. Here, $t_i \in T$ is a transition of timed event graph, $\Delta \in \mathbb{R}^+$ marked the extension time for the lifetime of transition t_i and $k \in \mathbb{Z}^+$ marked that the transition lag fault occurs after its k-th fire.

3 Fault detecting and diagnosis

The dependence relationships of transitions and the observable propagating character of transition fault in timed event graph will be studied in this section. Based on that, the sufficient and necessary conditions of fault detection and diagnosis are given.

In timed event graph, a path is a finite, nonempty sequence of places and transitions such that for each two consecutive elements a and b in it, it holds that $b \in a^*$, i.e. $a \in {}^*b$. A path is unobservable if and only if all transitions in it are unobservable. Firstly, the dependence relationship between transitions of timed event graph will be defined as follows.

Definition 10 In timed event graph, transition t_j is said to be dependent on transition t_i if there is a path from t_i to t_j. Particularly, t_j is said to be directly dependent on t_i if there is a one-step-length path from t_i to t_j, i.e. $t_i^* \cap {}^* t_j \neq \phi$.

Definition 11 In a partial observable timed event graph, t_i is an observable transition and t_j is an unobservable transition of system. It is said that t_i is time-dependent on t_j if and only if there is an unobservable path form t_i to t_j.

Consider the definitions of Petri net and timed event graph. If $p \in {}^* t$, it means that the fire of transition t will consume some resources (tokens) in place p. Correspondingly, if $p \in t^*$, it means that the fire of transition t will generate some resources (tokens) in place p. It is known that for any $p \in P$ in a timed event graph, there is only one input and output transition of this place. Hence, if transition t_j depends directly on t_i, it is also to say that the fire of t_j will consume some resources (tokens) generated by t_i directly. Transition t_j depends on t_i is also to say that the fire of t_j will consume some resources (tokens) generated by t_i through some special paths. Based on the relevance matrix of timed event graph, it is easy to prove that t_j is said to be directly dependent on t_i if and only if the element a_{ij} in A is finite and t_j is said to be dependent on t_i if and only if the element $\bar{a}_{ij}$ in $\bar{A}$ is finite.

Based on that, the fault detection and diagnosis problem will be studied in the invalidation and lag fault case respectively in following sections.

a) Invalidation fault case.

Lemma 1 For a timed event graph, if transition t_i is invalidated at its k-th fire and transition t_j depends directly on t_i, transition t_j will be out of work at its $(k + a_{ij})$-th fire, where a_{ij} is the element of relevance matrix A.

Proof Assume t_i is invalidated at its k-th fire. Consider the following two cases. Assume firstly that $|t_i^* \cap {}^* t_j| = 1$ and $t_i^* \cap {}^* t_j = \{p_r\}$. Transition t_j will exhaust all tokens in this place at its $[k + m_0(p_r)]$-th fire after the invalidation of t_i, where $m_0(p_r)$ is the initial marking of place p_r and then t_j will be out of work. For the case that $|t_i^* \cap {}^* t_j| \neq 1$, denote the place $p \in t_i^* \cap {}^* t_j$ satisfied that $m_0(p) \leqslant m_0(p')$ for any $p' \in t_i^* \cap {}^* t_j$. Then the token in p will be exhausted firstly and t_j will be out of work at its $[k + m_0(p)]$-th fire, where $a_{ij} = m_0(p) = \min_{p' \in t_i^* \cap {}^* t_j} \{m_0(p')\}$ is the element of relevance matrix A.

Lemma 2 If transition t_i is invalidated at its k-th fire and transition t_j depends on t_i, transition t_j will be out of work at its $(k + \bar{a}_{ij})$-th fire, where $\bar{a}_{ij}$ is the element of the closure matrix $\bar{A}$.

Proof By graph theory, it is known that the element $\bar{a}_{ij}$ of relevance matrix $\bar{A}$ marks the shortest path form t_i to t_j. Iteratively using Lemma 1, it can be proved that the fault will propagate in net through the shortest path.

Lemma 3 The invalidation of transition t_i will cause transition t_j to be out of work in finite time if and only if transition t_j depends on t_i, i.e. the element $\bar{a}_{ij}$ of closure matrix $\bar{A}$ is finite.

Proof Lemma 2 gives the sufficiency of this lemma. And the necessity is obvious because the invalidation of transition t_i will only influence those transitions depending on it.

Theorem 1 Fault $\tau_i = (t_i, k)$ is detectable if and only if there exists an observable transition that depends on transition t_i, i.e. there is at least one path from t_i to observable transition set T_o. In other word, $\tau_i = (t_i, k)$ is detectable if and only if it satisfy that $\exists j, \bar{a}_{ij} \neq +\infty$

and $t_j \in T_o$, where $\bar{a}_{ij}$ is the element of the closure matrix $\bar{A}$.

Proof Invalidation fault $\tau_i = (t_i, k)$ is detectable if and only if it will cause an observable transition to be out of work in finite time. For Lemma 3, it is easy to prove Theorem 1.

Lemma 1 and Lemma 2 give the propagating character of the invalidation fault. Based on them, the following definition is given and then the diagnosability condition of invalidation fault is given in Theorem 2.

Definition 12 The fault character vector of transition t_i is defined as vec_{t_i}. The element of fault character vector is

$$vec_{t_i}(j) = \begin{cases} \bar{a}_{ij}, & j \neq i, \\ 0, & j = i. \end{cases} \tag{2}$$

Accordingly, the observable fault character vector of transition t_i is $vec_{t_i}^o = [vec_{t_i}(j)_{j\in T_o} - \min_{j\in T_o}\{vec_{t_i}(j)\}]$, where $\bar{a}_{ij}$ is the element of closure matrix $\bar{A}$.

Theorem 2 In timed event graph, invalidation fault $\tau_i = (t_i, k)$ and fault $\tau_j = (t_j, k)$ can be distinguished from each other if and only if their observable fault character vectors are different.

Proof Consider Lemma 2 and the definition of fault character vector. Once an invalidation fault occurs, the observable fault character uniquely marks the invalidation sequence of observable transitions. Hence, two invalidation fault can be distinguished from each other iff their observable fault character vectors are different.

b) Lag fault case.

The diagnosis of lag fault is more complicated than invalidation fault because of the stochastic character of lifetime. Because the lifetime of observable transitions can be measured directly, here we only consider the lag fault of unobservable transitions. Firstly, the estimation of transitions fire time is given based on observation, and then a simple algorithm for time-lag fault location is proposed.

For timed event graph, it is well known that the fire time of a transition can be estimated based on the following equation.

$$\hat{t}_i(k) = \max_{j,r}\{t_j(k - m_0(p_{ji}^r)) + h_j\}, \tag{3}$$

where t_i and t_j are the transitions of system and $t_j^* \cap {}^*t_i \neq \phi$. $t_i(k)$ is the k-th fire time of transition t_i. $m_0(p_{ji}^r)$ is the initial marking and $p_{ij}^r \in {}^*t_i \cap t_j^*$. h_j is the lifetime of transition t_j.

For the partial observable system, the above equation is modified as follows to estimate the fire time based on observable transitions.

$$\hat{t}_i^o(k) = \max_{j,r}\{t_j(k - m_0(p_{jk_1}^r) + m_0(p_{k_1k_2}^r) + \cdots + m_0(p_{k_ni}^r)) + h_j + \sum_m h_{k_m}\}, \tag{4}$$

where transition t_i and t_j both are observable transition and $t_jk_1k_2\cdots k_mt_i$ is an unobservable acyclic path from transition t_j to t_i. It is also to say that transition t_i is time dependent on transition t_j. Based on the estimation of fire time, the fire time of an observable transition is said to be wrong if $t_i(k) \geqslant \hat{t}_i^o(k)$, where $t_i(k)$ is the measure data and $\hat{t}_i^o(k)$ is the estimation of fire time.

Considering the above equation, the fire time of an observable transition depends only on the lifetime of those unobservable transitions on which it is time-dependent. In other words, the lag fault of an unobservable transition will only influence the fire time of those observable transitions that are time-dependent. The following definition is given to show this relationship.

Definition 13 For an observable transition t_i, the candidate fault set is $c(t_i) = \{t_j \mid t_j \in T_u \wedge t_i$ is time dependent on $t_j\}$. Correspondingly, the candidate fault map set of an unobservable transition is $c'(t_j) = \{t_i \mid t_i \in T_o \wedge t_i$ is time dependent on t_j.$\}$

To locate the lag fault we have to compute the intersection set of all the observable transitions that has been detected with fault fire time, i.e. the fault location set is $\bigcap_i c(t_i)$. Based on that, a simple algorithm is given as follows.

Algorithm 1

Step 1 $k = 1$, initial marking M_0, initial candidate fault set $c_f = \phi$, measure the first fire time of those observable transitions;

Step 2 Estimate the fire time of those observable transitions' $(k+1)$-th fire based on the above function (4) and the fire time of k-th fire;

Step 3 Measure the $(k+1)$-th fire time of observable transitions and compare them with the estimation;

Step 4 If we detect a fault fire time, compute the candidate fault set $c_f = c_f \cap \{\bigcap_{t_i} c(t_i)\}$; else $c_f = c_f$. $k = k + 1$ and go to Step 2.

In Algorithm 1, the fire time for observable transitions is estimated on-line, and then it is compared with the measured value. A time-lag fault is said to be detected if and only if the measured value violate the estimated fire time. Being different form the methods in [3,8,9], we estimate the fire time instead to estimate the probable state

of system. Thus, it avoids the state explosion problem. From equation (4), it can be seen that the computation complexity is less than $O(mn)$, where $n = |T|$ and $m = |P|$ respectively, i. e. Algorithm 1 is polynomial complexity with respect to the system scale. It should be noted that the intersection set of all observable transitions with fault fire time is not always an unique element. In fact, the location of lag fault always just can get a candidate fault set. Hence it is easy to prove the following necessary condition of location of lag fault.

Theorem 3 If the lag fault of an unobservable transition can be diagnosed, it must be satisfied that $\{\bigcap_{t_i \in c'(t_l)} c(t_i)\} = \{t_l\}$.

Proof For contrary, it is assumed that the condition is not satisfied, i.e. $\{t_l\} \subset \{\bigcap_{t_i \in c'(t_l)} c(t_i)\}$. It has been declared that the lag fault of an unobservable transition will only influence those observable transitions that depend on it directly and not all those observable transitions will have fault fire time. It is also to say that the set of observable transitions with fault fire time, noted as $c'_o(t_l)$, is included in the candidate fault map set $c'(t_l)$, i.e. $c'_o(t_l) \subseteq c'(t_l)$. Thus, we have

$$\{t_l\} \subset \{\bigcap_{t_i \in c'_o(t_l)} c(t_i)\} \subseteq \{\bigcap_{t_i \in c'_o(t_l)} c(t_i)\}.$$

Hence, we cannot locate the fault source to transition t_l.

Theorem 4 If the candidate fault map set of two unobservable transitions are the same, the lag fault of those two transitions cannot be distinguished from each other.

Proof Assumed the $c'(t_l) = c'(t_q) = C$. As shown in the proof of Theorem 3, the observable set of transitions with fault fire time caused by the fault of transition lag, $c'_o(t_l)$ and $c'_o(t_q)$, are all included in C. Hence, we have

$$\{\bigcap_{t_i \in C} C(t_i)\} \subseteq \{\bigcap_{t_i \in c'_o(t_l)} c(t_i)\}$$

and $$\{\bigcap_{t_i \in C} c(t_i)\} \subseteq \{\bigcap_{t_i \in c'_o(t_q)} c(t_i)\}.$$

Because $t_l \in \{\bigcap_{t_i \in C} c(t_i)\}$ and $t_q \in \{\bigcap_{t_i \in C} c(t_i)\}$, we can get $\{t_l, t_q\} \subseteq \{\bigcap_{t_i \in c'_o(t_l)} c(t_i)\}$ and $\{t_l, t_q\} \subseteq \{\bigcap_{t_i \in c'_o(t_q)} c(t_i)\}$. Hence, the time-lag fault for transition t_l and t_q cannot be distinguished from each other

4 Simple example

In this section, Fig. 1 shows a simple example for timed event graph and we will use it to illustrate the main results in this paper.

The initial marking of event graph in figure is $M_0 = [0,0,1,0,0,0,0]$. Hence, based on Definition 6, the relevance matrix of the timed event graph and the closure of relevance matrix are given as follows:

$$A = \begin{bmatrix} +\infty & 0 & +\infty & 0 & +\infty \\ +\infty & +\infty & 0 & +\infty & 0 \\ +\infty & 1 & +\infty & 0 & +\infty \\ +\infty & +\infty & +\infty & +\infty & +\infty \\ +\infty & +\infty & +\infty & +\infty & +\infty \end{bmatrix},$$

$$\bar{A} = \begin{bmatrix} +\infty & 0 & 0 & 0 & 0 \\ +\infty & 1 & 0 & 0 & 0 \\ +\infty & 1 & 0 & 0 & 1 \\ +\infty & +\infty & +\infty & +\infty & +\infty \\ +\infty & +\infty & +\infty & +\infty & +\infty \end{bmatrix}.$$

For the system in Fig. 1, transition 1 is the input transition and we assume that transition 4 and transition 5 are observable. It is easy to find that all the invalidation fault of transition is detectable. Based on the closure matrix $\bar{A}$, the fault character vector and observable fault character vector for each transition can be computed. For example, the fault character vector and observable fault character vector for transition 2 are $[+\infty, 0, 0, 0, 0]$ and $[0, 0]$ respectively. The fault character vector and observable fault character vector for transition 3 are $[+\infty, 1, 0, 0, 1]$ and $[0, 1]$. It is obvious that the observable fault characters for transition 2 and transition 3 are different. If transition 2 breaks down at its k-th fire, it will cause transition 4 and transition 5 both to be out of work at their k-th fire. Correspondingly, if transition 3 breaks down at its k-th fire, it will cause transition 4 to be out of work at its k-th fire and transition 5 to be out of work at its $k+1$-th fire. Thus the invalidation fault of transition 3 can be distinguished from the invalidation fault of transition 2.

For the time-lag fault case, the fault map sets of transition 2 and transition 3 are both $c'(t_2) = c'(t_3) = \{t_4, t_5\}$. No matter wether transition 2 or transition 3 has a time-lag fault, it will both influence the fire time of transition 4 and transition 5. Thus, based on Algorithm 1, the lag fault for transition 2 and transition 3 cannot be distinguished from each other.

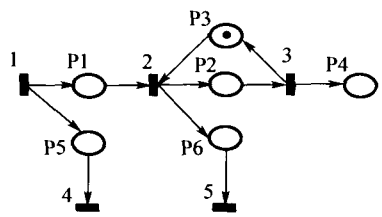

Fig. 1 Simple example for event graph

5 Conclusion

The fault diagnosis problem for timed event graph is studied in this paper. Different form other methods as in literature [1] and [5, 6], faulty behaviors model is not given explicitly in the system. Implicit faults are defined as the invalidation or time lag of transition in timed event graph. The fault character vector and the candidate fault set are defined for transition invalidation and lag fault respectively. It is proved that the fault character vector and candidate fault set uniquely mark the propagating character of transition fault. It is shown that, for the invalidation fault, the fault diagnosability of system depends not only on the system structure but also on the initial state of system. Based on the character vector, sufficient and necessary conditions for invalidation fault detectability and diagnosability are given. The lag fault case is more difficult because of the stochastic character of lifetime. A simple algorithm is given to locate the lag fault and the condition of fault diagnosability is also given in this paper.

References:

[1] LIN F. Diagnosability of discrete event systems and its application [J]. *Discrete Event Dynamic Systems: Theory and Applications*, 1994, 4(2): 197 - 212.

[2] CHAND S. Discrete-event based monitoring and diagnosis of manufacturing processes [C] // *Proc of American Control Conference*. San Francisco, CA, USA: IEEE Press, 1993: 1508 - 1522.

[3] HOLLOWAY L E, CHAND S. Time templates for discrete event fault monitoring in manufacturing systems [J]. *Proc of* 1994 *American Control Conference*. Baltimore, MD, USA: American Automatic Control Council, 1994: 701 - 706.

[4] SMAPATH M, SENGUPTA R, LAFORTUNE S, et al. Diagnosability of discrete event systems [J]. *IEEE Trans on Automatic Control*, 1995, 40(9): 1555 - 1575.

[5] SMAPATH M, LAFORTUNE S, TENEKETZIS D. Active diagnosis of discrete event systems [J]. *IEEE Trans on Automatic Control*, 1998, 43(7): 909 - 929.

[6] DEBOUK R, LAFORTUNE S, TENEKETZIS D. Coordinated decentralized protocols for failure diagnosis of discrete event systems [J]. *Discrete Event Dynamic Systems: Theory and Application*, 2000, 10(1/2): 33 - 86.

[7] USHIO T, ONISHI I, OKUDA K. Fault detection on Petri net models with faulty behaviors [C] // *Proc of* 1998 *IEEE Int Conf on Systems, Man, and Cybernetics*. San Diego, CA, USA: IEEE Press, 1998: 113 - 118.

[8] CHEN Y, PROVAN G. Modeling and diagnosis of timed discrete event systems - a factory automation example [C] // *Proc of* 1997 *American Control Conference*. Albuquerque, NM, USA: IEEE Press, 1997: 31 - 36.

[9] ZAD S H, KWONG R H, WONHAM W M. Fault diagnosis in timed discrete-event systems [C] // *Proc of the* 38*th Conference on Decision & Control*. Phoenix, AZ, USA: IEEE Press, 1999: 1756 - 1761.

[10] ROZE L, CORDIER M. Diagnosing discrete-event systems: extending the "diagnoser approach" to deal with telecommunication networks [J]. *Discrete Event Dynamic Systems: Theory and Application*, 2002, 12(1): 43 - 81.

[11] CASSANDRAS G, LAFORTUNE S. *Introduction to Discrete Event Systems* [M]. Boston, MA, USA: Kluwer Academic, 1999.

作者简介:

薛 飞 (1975—),男,清华大学自动化系博士研究生,主要研究领域包括离散事件系统、故障诊断与容错控制、电力系统监控等, E-mail: xuefei00@mails.tsinghua.edu.cn;

郑大钟 (1935—),男,清华大学自动化系教授,博士生导师,主要研究领域包括线性系统理论、控制系统鲁棒性、离散事件系统、混合动态系统等.