文章编号: 1001-0920(2017)11-2081-04 DOI: 10.13195/j.kzyjc.2016.1054

赋时离散事件系统的安全诊断

刘富春†, 蔡家德

(广东工业大学 计算机学院，广州 510006)

摘 要: 针对一类计时或非计时自动机模型,研究其赋时离散事件系统(TDES)故障诊断的安全性问题. 首先对TDES的安全可诊断性进行形式化;然后通过构造一个非法语言识别器对被禁止危险操作序列进行识别,在此基础上构建一个安全诊断器,提出一种基于安全诊断器的安全诊断方法,并得到一个关于TDES安全可诊断性的充分必要条件,从而实现TDES的安全故障诊断.

关键词: 赋时离散事件系统；故障诊断；安全诊断；安全诊断器

中图分类号: TP13 **文献标志码:** A

Safe diagnosability of timed discrete-event systems

LIU Fu-chun†, CAI Jia-de

(School of Computers，Guangdong University of Technology，Guangzhou 510006，China)

Abstract: An approach for safe diagnosis of timed discrete-event systems(TDESs) is proposed. Firstly, the notion of safe diagnosability of TDESs is formalized. Then by constructing the recognizer of illegal language, the sequences of the forbidden unsafe operations are identified, and the safe diagnoser is constructed to perform the safe diagnosis. In particular, a necessary and sufficient condition for safe diagnosability is deduced, and the safe diagnosis of TDES is realized.

Keywords: time discrete-event systems；fault diagnosis；safe diagnosis；safe diagnoser

0 引 言

近年来,离散事件系统的故障诊断研究引起了国内外许多学者的广泛关注. Sampath等[1]提出了一种基于诊断器的故障诊断方法. 文献[2]将该方法推广至分布式系统,提出了一种分散诊断方法. 文献[3]研究了不完备离散事件系统的故障诊断问题. Liu等则针对随机离散事件系统和模糊离散事件系统提出了相应的随机分散诊断方法[4]和模糊诊断方法[5].

对于许多工业应用系统,在考虑其运行过程的逻辑行为的同时,往往还需要进一步考虑运行中的时间信息. 为此,文献[6]首次提出了一种赋时离散事件系统(TDES)模型. 文献[7]提出了一种TDES模块化监控方法. 文献[8]则提出了一种基于诊断器的故障诊断方法,并将其应用于工业自动化系统的故障诊断. 尽管这种故障诊断方法能在故障发生之后的有限时延内被诊断出来,但在这段时延期间,系统仍可能会执行某些被禁止的危险操作,这对故障已发生的“病态”系统而言是极其危险的. 为此,文献[9]研究了故障诊断的安全性问题,提出了一种安全故障诊断方法. Liu等[10-11]也对安全诊断问题进行了研究. 文献[10]在随机系统模型的框架下构建马尔科夫转移矩阵,提出了一种随机离散事件系统的安全诊断方法. 文献[11]针对模糊离散事件系统,提出了一种基于模糊验证器的具有多项式时间复杂性的安全诊断方法.

本文继续文献[10-11]的工作,在文献[6,8]的基础上进一步研究TDES安全诊断问题. 首先对TDES的安全可诊断性进行形式化;然后通过构造一个非法语言识别器对被禁止危险操作序列进行识别,并在此基础上构建一个安全诊断器,提出一种基于安全诊断器的安全诊断方法,得到一个关于TDES安全可诊断性的充分必要条件,从而实现TDES的安全故障诊断. 不仅保证故障一旦发生能被及时诊断出来,而且还可确保在故障诊断期间系统不会执行任何不安全

收稿日期: 2016-08-18；**修回日期:** 2017-01-03.

基金项目: 国家自然科学基金项目(61273118, 61673122)；广东省教育厅省级重大项目(2014KZDXM033)；广东省公益研究与能力建设专项资金项目(2015A030402006)；广东工业大学计算机学院重大奖项培育项目.

作者简介: 刘富春(1971–), 男, 教授, 博士生导师, 从事控制理论与应用、算法设计等研究；蔡家德(1989–), 男, 硕士生, 从事控制理论与应用、算法设计的研究.

†通讯作者. E-mail: 452085874@qq.com

操作,弥补了文献[8]只考虑故障诊断而未考虑诊断期间安全性的缺陷.

1 赋时离散事件系统

一个计时自动机[5]是指有限状态机$G_a = (A, \Sigma_a, \delta_a, a_0)$. 其中: A为有限状态集; Σ_a为事件集,它分为可观事件集Σ_o和不可观事件集Σ_{uo}; $\delta_a : A \times \Sigma_a \to A$为局部转移函数; $a_0 \in A$为初始状态. 用$\delta_a(a,\sigma)!$表示$\delta_a(a,\sigma)$有定义,用$L(G_a)$或L表示G_a的行为语言,包括空串ε. 对于$s \in \Sigma^*$, $\bar{s}$表示s的前缀闭包, L/s表示s的后缀语言[9].

由于任一事件$\sigma \in \Sigma_a$的发生或完成都与一个时间上界ℓ_σ和一个时间下界μ_σ相关联[6-8],为此,用一个三元组$\sigma = [\sigma, \ell_\sigma, \mu_\sigma]$表示该事件. 其中: $\ell_\sigma \in N, \mu_\sigma \in N \bigcup \{\infty\}$, N为自然数集. 根据ℓ_σ与μ_σ的界限值,还可将Σ_a进一步分为远期事件集Σ_r和近期事件集Σ_s,即$\Sigma_a = \Sigma_r \bigcup \Sigma_s$. $\sigma \in \Sigma_s$表示$0 \leqslant \mu_\sigma < \infty$和$0 \leqslant \ell_\sigma \leqslant \mu_\sigma$; $\sigma \in \Sigma_r$表示$\mu_\sigma = \infty$和$0 \leqslant \ell_\sigma < \mu_\sigma$.

设$\Sigma_f \subseteq \Sigma_a$表示待诊断的故障事件集,其中$\Sigma_f \subseteq \Sigma_{uo}$. 根据故障事件对系统的不同影响,将故障事件集划分为不同故障类型: $\Sigma_f = \Sigma_{f1} \bigcup \cdots \bigcup \Sigma_{fm}$,并用$\Pi_f$表示. 对于任意$s \in \Sigma^*$,设$s_f$表示$s$的结尾事件. 用$\Psi(\Sigma_{fi})$表示以第$i$类故障事件结尾的事件串集,即$\Psi(\Sigma_{fi}) = \{s \in L : s_f \in \Sigma_{fi}\}$.

定义1 设$G_a = (A, \Sigma_a, \delta_a, a_0)$是一个以计时自动机为模型的TDES, $A_\sigma = \{b \in A | \delta_a(b, \sigma, \ell_\sigma, \mu_\sigma)!\}$,称$G_a$具有单调上界特性是指对于任意$\sigma \in \Sigma_a$和$a_1, a_2 \in A_\sigma$,下列条件满足:

$$\delta_a(a_1,\sigma,\ell_\sigma,\mu_\sigma)! \bigwedge \delta(a_2,\sigma,\ell_\sigma,\mu_\sigma)! \bigwedge (\exists \beta) \in (\Sigma_a - \{\sigma\})\delta_a(a_1,\beta,\ell_\beta,\mu_\beta) = a_2 \Rightarrow \mu_\beta \geqslant \mu_\sigma. \quad (1)$$

例1 考虑如图1给出的计时自动机G_a. 其中: f为故障事件, $\Sigma_o = \{\alpha, \beta, \gamma, \omega\}$. 设$f \in \Sigma_r, \alpha, \beta, \gamma, \omega \in \Sigma_s, f = (f, 0, \infty), \alpha = (\alpha, 1, 2), \beta = (\beta, 1, 1), \gamma = (\gamma, 0, 1), \omega = (\omega, 0, 0)$. 显然, $\mu_f \geqslant \mu_\alpha \geqslant \mu_\beta$. 因此, G_a具有单调上界特性.

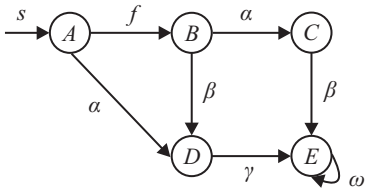

图1 计时自动机G_a

非计时自动机模型[8]是在上述计时自动机模型基础上引入了tick事件,用于描述赋时离散事件系统全局时间单元的流逝. 用T_σ表示事件σ的标签时钟值区间,用t_σ表示系统在当前状态的标签时钟值.

定义2[8] 设$G_a = (A, \Sigma_a, \delta_a, a_0)$是一个计时自动机,与$G_a$等价的非计时自动机是指有限状态机$G = (X, \Sigma, \delta, x_0)$. 其中: $\Sigma = \Sigma_a \bigcup \{\text{tick}\}$为事件集; $X = A \times \Pi\{T_\sigma | \sigma \in \Sigma_a\}$为状态集: 对于任意$x \in X$和$\sigma \in A$,状态$x$不仅包含当前状态信息,还包含此时事件的标签时钟值,其具体表示为$x = (a, \{t_\sigma \in T_\sigma | \sigma \in \Sigma_a\})$. $x_0 = (a_0, \{t_{\sigma 0} | \sigma \in \Sigma_a\})$为初始状态; $\delta : X \times \Sigma \to X$为状态转移函数. 为避免出现由非tick事件转移构成环路而导致无限期抢占tick转移,一般要求G满足无活动环(ALF)条件[7],即$(\forall x \in X, \forall s \in \Sigma_a^+)\delta(s, x) \neq x$.

例2 图2给出了与例1中计时自动机G_a等价且满足ALF条件的非计时自动机G,其中t表示tick事件,且除事件t的发生需占用一个时钟单元,其他事件都是瞬发事件,系统各状态如表1所示.

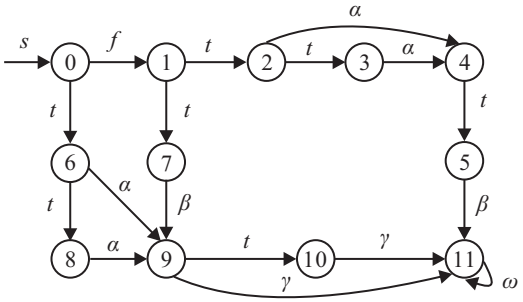

图2 非计时自动机模型G

表1 非计时自动机模型G的状态表

x	$(a, [t_\alpha, t_\beta, t_\gamma, t_\omega, t_f])$	x	$(a, [t_\alpha, t_\beta, t_\gamma, t_\omega, t_f])$
0	$(A, [2,1,1,0,0])$	6	$(A, [1,1,1,0,0])$
1	$(B, [2,1,1,0,0])$	7	$(B, [2,0,1,0,0])$
2	$(B, [1,1,1,0,0])$	8	$(A, [0,1,1,0,0])$
3	$(B, [0,1,1,0,0])$	9	$(D, [2,1,1,0,0])$
4	$(C, [2,1,1,0,0])$	10	$(D, [2,1,0,0,0])$
5	$(C, [2,0,1,0,0])$	11	$(E, [2,1,1,0,0])$

2 赋时离散事件系统安全诊断的形式化

用$\Omega_i \subseteq \Sigma^*$表示对应于第$i$种类型故障的被禁止事件串集($i = 1, 2, \cdots, m$),相应的非法语言$\lambda_f^i$定义为

$$\lambda_f^i = \{\kappa \in \Sigma^* : (\exists s \in \Psi(\Sigma_{fi}))(\exists \tau \in \Omega_i)(\kappa \in L/s \bigwedge \tau \in \bar{\kappa})\}. \quad (2)$$

定义3 设$G = (X, \Sigma, \delta, x_0)$是一个TDES,称$G$为安全可诊断的,如果对于任意$i \in \Pi_f$,下述可诊断条件满足:

$$(\exists n_i \in N)[\forall s \in \psi(\Sigma_{fi})](\forall t \in L/s)(||t|| \geqslant n_i \Rightarrow \wp),$$

其中$\wp$为$\omega \in P_L^{-1}[P(st)] \Rightarrow \Sigma_{fi} \in \omega$;并且下述安全性条件也满足: $(\forall s \in \Psi(\Sigma_{fi}), \forall t \in L/s)(\bar{t_c} \bigcap \lambda_f^i = \varnothing)$,其中$\|t\| = n_i$且$t_c$为$t$中满足条件$\wp$的最短前缀.

3　赋时离散事件系统安全诊断器的构造

先引入禁止标识符集 $\Lambda_i = \{B_i, S_i^1, S_i^2\}$ 以标记系统是否执行 Ω_i 中被禁止操作. 其中: B_i 表示故障 f_i 已发生且在故障诊断期间又执行了 Ω_i 中的被禁止操作, S_i^1 表示当前系统处于正常状态, 而 S_i^2 表示故障 f_i 已发生但当前系统未执行 Ω_i 中的被禁止操作.

定义 4　设 $G = (X, \Sigma, \delta, x_0)$ 是一个 TDES, 将 G 的非法语言 λ_f^i 识别器构造为一个有限状态机

$$G_r = (Q_r, \Sigma, \delta_r, q_{r0}). \tag{3}$$

其中: $Q_r = X \times \Lambda_i$ 为有限状态集, Σ 为事件集, $q_{r0} = (x_0, S_i^1)$ 为初始状态, $\delta_r : Q_r \times \Sigma \to Q_r$ 为状态转移函数, 其具体形式将在定义 5 中给出.

定义 5　G_r 的状态转移函数 $\delta_r : Q_r \times \Sigma \to Q_r$ 定义为: 对于任意 $\sigma \in \Sigma, q_{rj} \in Q_r$, 有

$$\delta_r(q_{rj}, \sigma) = (\delta(q_{rj}, \sigma), \eta_r(q_{rj}, \sigma)).$$

其中 $\eta_r: Q_r \times \Sigma \to \Lambda_i$ 为标签修改函数, 其定义如下:

1) 如果存在 $\sigma \in \Sigma$ 使得 $\delta(x_0, \sigma)$ 有定义, 则当 $\sigma \notin \Sigma_{fi}$ 时, $\eta_r(q_{r0}, \sigma) = S_i^1$; 当 $\sigma \in \Sigma_{fi}$ 时, $\eta_r(q_{r0}, \sigma) = S_i^2$.

2) 如果存在 $s \in \Sigma^*$ 和 $\sigma \in \Sigma$ 使得 $\delta_r(q_{r0}, s\sigma) = (q_{rj}, \sigma)$ 且 $\delta_r(q_{rj}, \sigma, q_{rk})$ 和 $\delta(x_j, \sigma, x_k)$ 都有定义, 其中 $q_{rj} = (x_j, T_j), q_{rk} = (x_k, T_k)$, 则: i) 当 $T_j = S_i^1$ 时, 若 $\sigma \notin \Sigma_{fi}$, 则 $\eta_r(q_{rj}, \sigma) = S_i^1$; 若 $\sigma \in \Sigma_{fi}$, 则 $\eta_r(q_{rj}, \sigma) = S_i^2$. ii) 当 $T_j = S_i^2$ 时, 若 $\sigma \notin \Omega_i$, 则 $\eta_r(q_{rj}, \sigma) = S_i^2$; 若 $\sigma \in \Omega_i$, 则 $\eta_r(q_{rj}, \sigma) = B_i$. iii) 当 $T_j = B_i$ 时, $\eta_r(q_{rj}, \sigma) = B_i$.

例 3　考虑例 2 中给出的赋时离散事件系统 G, 设 γ 为故障诊断期间的被禁止操作事件, 则根据定义 5, 非法语言识别器 G_r 构造如图 3 所示.

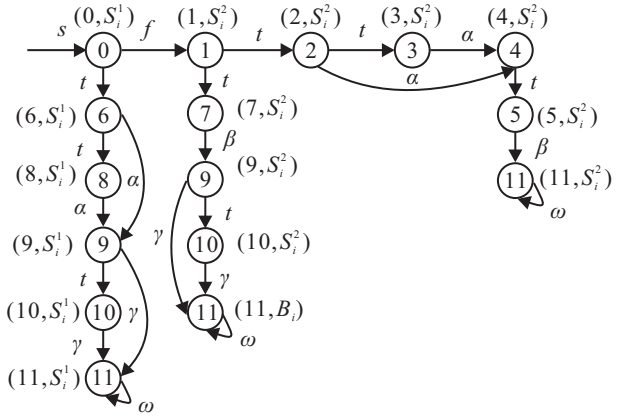

图 3　非法语言识别器 G_r

设 $q_r \in Q_r$, 定义 q_r 的可观终态串集为

$$L_o(G_r, q_r) = \{s \in L(G_r, q_r) : s = \mu\sigma, \mu \in \Sigma_{uo}^*, \sigma \in \Sigma_o\},$$

其中 $L(G_r, q_r)$ 为所有由 q_r 引出的事件串集, 并记 $L_\sigma(G_r, q_r) = \{s \in L_o(G_r, q_r) : s_f = \sigma\}$. 记故障标签集为 $\Delta = \{N\} \bigcup 2^{\{F_1, F_2, \cdots, F_m\}}$. 其中: N 表示系统正常, F_i 表示系统第 i 种类型的某故障已发生.

定义 6　设 $G = (X, \Sigma, \delta, x_0)$ 是一个 TDES, G 的安全诊断器构造为如下有限状态机:

$$G_d^s = (Q_d^s, \Sigma_o, \delta_d^s, q_0^s).$$

其中: $Q_d^s = X \times \Delta \times \Lambda_i$ 为有限状态集, Σ_o 为可观事件集; $q_0^s = (x_0, N, S_i^1)$ 为初始状态; $\delta_d^s : Q_d^s \times \Sigma_o \to Q_d^s$ 为状态转移函数, 其具体定义将在定义 7 中给出.

定义 7　G_d^s 的状态转移函数 $\delta_d^s : Q_d^s \times \Sigma_o \to Q_d^s$ 定义为: 对于任意 $q^s \in Q_d^s, \sigma \in \Sigma_o$, 有

$$\delta_d^s(q^s, \sigma) = \bigcup\{(\delta(q_{ri}, t),\ \Gamma_d^s(x_i, \phi_i, l_i, \sigma),\ P_d^s(q_{ri}, l_i, \sigma)) : (q_{ri}, l_i) \in q^s,\ t \in L_\sigma(q_{ri}),\ l_i \in \Delta\}.$$

其中

$$\Gamma_d^s(x_i, \phi_i, l_i, \sigma) = \bigcup\{\eta_r(q_{ri}, t) : t \in L_\sigma(q_{ri})\},$$

$$P_d^s(q_{ri}, l_i, \sigma) = \begin{cases} \{N\}, \text{ 如果} (\forall_i)(\Sigma_{fi} \notin t) \bigwedge (l_i = N); \\ \bigcup\{F_i : (\Sigma_{fi} \notin t) \bigvee (F_i \in l_i)\}, \text{ 否则}. \end{cases}$$

这里: $(q_{ri}, l_i) \in q^s, t \in L_\sigma(q_{ri}), l_i \in \Delta, q_{ri} = (x_i, \phi_i)$.

上述构造 G_d^s 的基本思路是: 用三维向量表示安全诊断器 G_d^s 的状态, 其中: 第 1 个分支用于跟踪系统 G 的运行轨迹, 第 2 个和第 3 个分支分别用于记录当前状态故障发生与否以及被禁止操作执行与否的信息. G_d^s 的初始状态 $q_0^s = (x_0, N, S_i^1)$ 表示系统 G 在初始状态 x_0 时是正常的 (即 q_0^s 第 2 个分支为 N), 未执行被禁止操作 (即 q_0^s 第 3 个分支为 S_i^1); 然后从 x_0 出发, 跟踪 G 的状态 x, 当故障事件 f_i 发生后, G_d^s 状态的第 2 个分支应修改为 F_i, 而第 3 个分支则应进一步考察系统是否执行被禁止操作, 如果未执行被禁止操作, 则第 3 个分支标签为 S_i^2, 如果已执行了被禁止操作, 则第 3 个分支标签为 B_i.

例 4　考虑例 3 中的赋时离散事件系统 G, 根据定义 6, G 的安全诊断器可构造如图 4 所示.

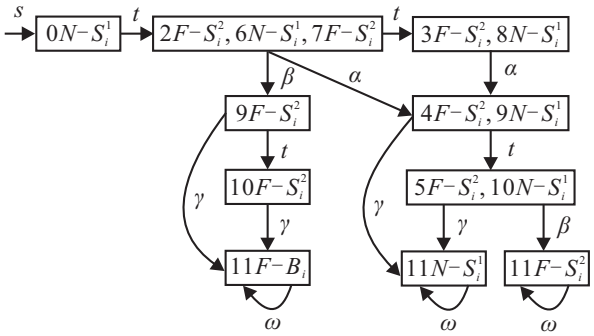

图 4　安全诊断器 G_d^s

4 安全可诊断性的充分必要条件

设$G_d^s=(Q_d^s,\Sigma_o,\delta_d^s,q_0^s)$是$G$的安全诊断器,$q^s\in Q_d^s$. 若对于任意$(q_r,l)\in q^s$都有$F_i\in l$,则称$q^s$为$F_i$-确定状态;若存在$(q_{ri},l_i),(q_{rj},l_j)\in q^s$使得$F_i\in l_i$且$F_i\notin l_j$,则称$q^s$为$F_i$-不确定状态.

定理1 设$G=(X,\Sigma,\delta,x_0)$是一个TDES,$G_d^s=(Q_d^s,\Sigma_o,\delta_d^s,q_0^s)$是$G$的安全诊断器,则$G$为安全可诊断的充分必要条件是$G_d^s$满足下列条件:

1) 不存在F_i-不确定状态$q^s\in Q_d^s$,使得$(q_r,l)\in q^s$. 其中:$F_i\in l,q_r=(x,\phi),B_i\in\phi$.

2) 不存在状态$q_i^s,q_{i+1}^s\in Q_d^s$,使得q_i^s是F_i-不确定状态且存在$e\in\Sigma_o$满足$\delta_d^s(q_i^s,e)=q_{i+1}^s$;而$q_{i+1}^s$是$F_i$-确定状态且存在$(q_r',l')\in q_{i+1}^s$满足$F_i\in l',q_r'=(x',\phi'),B_i\in\phi'$.

证明 先用反证法证明充分性. 设条件1)和条件2)满足,但G不是安全可诊断的. 由定义3可知,G不满足可诊断条件或不满足安全性条件.

若G不满足可诊断条件,则G中存在u,v满足$P(u)=P(v)$且$\Sigma_{fi}\in u,\Sigma_{fi}\notin v$,从而存在$q^s\in Q_d^s$使得$(x,\phi,l),(y,\phi',l')\in q^s$且$F_i\in l,B_i\in\phi,F_i\notin l',B_i\notin\phi'$,即$q^s$是$F_i$-不确定状态. 这与条件1)矛盾.

若不满足安全性条件,则存在$u=u_1u_2e$使$u_1\in\Psi(\Sigma_{fi}),u_2\in\lambda_f^i,e\in\Sigma_o$且$\bar{t}_c\bigcap\lambda_f^i\neq\varnothing,t_c$为$u$中满足条件$\wp$的最短前缀. 记$q_i^s=\delta_d^s(q_0^s,P(u_1u_2))$且$q_{i+1}^s=\delta_d^s(q_i^s,e)$,则$q_i^s$是$F_i$-不确定状态而$q_{i+1}^s$是$F_i$-确定状态,$B_i\in q_{i+1}^s$. 这与条件2)矛盾.

再用反证法证明必要性. 设G是安全可诊断的. 如果安全诊断器G_d^s不满足条件1),则存在F_i-不确定状态$q_i^s\in Q_d^s$,从而在G中存在u和v使得$P(u)=P(v),\delta(x_0,u)=x,\delta(x_0,v)=x',\Sigma_{fi}\in u,\Sigma_{fi}\notin v$,且$(x,\phi,l),(x',\phi',l')\in q_i^s$和$B_i\in\phi$. 根据定义3,安全可诊断条件不满足,即$G$不是安全可诊断的,这与假设相矛盾. 如果安全诊断器G_d^s不满足条件2),则存在$q_i^s,q_{i+1}^s\in G_d^s,e\in\Sigma_o$使得$q_i^s$是$F_i$-不确定状态,$\delta_d^s(q_i^s,e)=q_{i+1}^s$且$q_{i+1}^s$是$F_i$-确定状态,$q_r'=(x',\phi'),B_i\in\phi'$,这表明在故障发生之后的诊断期间系统执行了被禁止操作. 根据定义3,G不是安全可诊断的,这与假设相矛盾. □

例5 考虑例3中的赋时离散事件系统G,由定义3可知,G是安全可诊断的,因为在故障f发生之后经过一个时钟单元就能诊断出f的发生,且在故障诊断中未执行被禁止操作γ. 事实上,该结论也可根据定理1得到,G的安全诊断器G_d^s在例4中图4给出,不难验证G_d^s满足定理1中的条件1)和条件2),因此,由定理1知,G是安全可诊断的.

5 结 论

针对赋时离散事件系统故障诊断的安全性问题,本文提出了一种安全诊断方法,不仅能将发生的故障及时诊断出来,而且能确保在故障诊断期间系统不执行任何不安全操作. 在构造一个非法语言识别器对系统被禁止操作进行识别后,构建一个安全诊断器,得到了一个关于安全可诊断性的充分必要条件,实现了赋时离散事件系统的安全故障诊断.

参考文献(References)

[1] Sampath M, Sengupta R, Lafortune S, et al. Diagnosability of discrete-event systems[J]. IEEE Trans on Automatic Control, 1995, 40(9): 1555-1575.

[2] Qiu W, Kumar R. Decentralized failure diagnosis of discrete event systems[J]. IEEE Trans on Systems, Man, and Cybernetics — Part A, 2006, 36(2): 384-395.

[3] 王晓宇, 欧阳丹彤, 赵剑. 不完备模型下的离散事件系统诊断方法[J]. 软件学报, 2012, 23(3): 465-475.
(Wang X Y, Ouyang D T, Zhao J. Discrete-event system diagnosis upon incomplete model[J]. J of Sofware, 2012, 23(3): 465-475.)

[4] Liu F C, Qiu D, Xing H, et al. Decentralized diagnosis of stochastic discrete event systems[J]. IEEE Trans on Automatic Control, 2008, 53(2): 535-546.

[5] Liu F C, Qiu D. Diagnosability of fuzzy discrete-event systems: A fuzzy approach[J]. IEEE Trans on Fuzzy Systems, 2009, 17(2): 372-384.

[6] Alur R, Dill D. Automata for modeling real-time systems[J]. Lecture Notes in Computer Science, 1990, 17(43): 322-335.

[7] Schafaschek G, Max H, Jose E. Local modular supervisory control of timed discrete-event systems[J]. IEEE Trans on Automatic Control, 2014, 47(2): 271-277.

[8] Chen Y L, Provan G. Modeling and diagnosis of timed discrete-event systems — A factory automation example[C]. American Control Conf. Albuquerque, 1997: 31-36.

[9] Paoli A, Lafortune S. Safe diagnosability for fault-tolerant supervision of discrete-event systems[J]. IEEE Trans on Automatic Control, 2005, 41(8): 1335-1347.

[10] Liu F C, Qiu D. Safe diagnosability of stochastic discrete event systems[J]. IEEE Trans on Automatic Control, 2008, 53(5): 1291-1296.

[11] Liu F C. Safe diagnosability of fuzzy discrete-event systems and a polynomial-time verification[J]. IEEE Trans on Fuzzy Systems, 2015, 23(5): 1534-1544.

(责任编辑:李君玲)