控制与决策
Control and Decision

离散事件系统间歇性故障的安全诊断

刘富春， 唐顺桥， 赵锐， 邓秀勤， 崔洪刚

引用本文:
刘富春, 唐顺桥, 赵锐, 等. 离散事件系统间歇性故障的安全诊断[J]. 控制与决策, 2020, 35(5): 1205−1210.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2018.1060

文章编号: 1001-0920(2020)05-1205-06 DOI: 10.13195/j.kzyjc.2018.1060

离散事件系统间歇性故障的安全诊断

刘富春[1†], 唐顺桥[1], 赵 锐[1], 邓秀勤[2], 崔洪刚[1,3]

(1. 广东工业大学 计算机学院，广州 510006；2. 广东工业大学 应用数学学院，广州 510006；
3. 广东省东源县科技创新中心，广东 河源 517500)

摘 要: 离散事件系统的间歇性故障诊断能够将系统中发生的间歇性故障及时诊断出来,但在诊断期间的系统可能会执行不安全操作. 针对间歇性故障在诊断期间的安全性问题,提出一种基于事件的安全诊断方法. 首先对发生间歇性故障的离散事件系统进行建模,并给出系统间歇性故障的安全可诊断性的形式化定义. 然后通过构造非法语言识别器对系统的非法操作进行识别,并在此基础上构建一个安全验证器,由此得到一个关于系统间歇性故障安全可诊断性的充分必要条件,实现离散事件系统对间歇性故障的安全诊断. 这种安全诊断既保证了间歇性故障一旦发生即能被及时诊断出来,又确保了在故障诊断期间系统不会执行任何不安全操作.

关键词: 离散事件系统；间歇性故障；故障诊断；安全诊断；识别器；验证器

中图分类号: TP13 **文献标志码:** A

Safe diagnosability for intermittent faults of discrete-event systems

LIU Fu-chun[1†], *TANG Shun-qiao*[1], *ZHAO Rui*[1], *DENG Xiu-qin*[2], *CUI Hong-gang*[1,3]

(1. School of Computers，Guangdong University of Technology，Guangzhou 510006，China；2. School of Applied Mathematics，Guangdong University of Technology，Guangzhou 510006，China；3. Science and Technology Innovation Center of Dongyuan，Heyuan 517500，China)

Abstract: Intermittent faults diagnosis of discrete event systems (DES) can detect intermittent faults in the system in time, but the system may execute unsafe operation during the fault detection. An approach for safe diagnosability is proposed for intermittent faults of DESs. Firstly, the system with intermittent faults is modeled, and the notion of safe diagnosability for intermittents faults of DESs is formalized. Then we construct the recognizer of illegal language to identify the sequences of the forbidden operations. Based on the recognizer, the safe verifier is constructed. In particular, a necessary and sufficient condition of safe diagnosability for intermittent faults of DESs is proposed and a safe diagnosis of intermittent faults is achieved. It is guaranteed that not only each intermittent fault occurring in safe diagnosable DESs can be detected in time, but also the system does not execute any unsafe operation during the fault detection.

Keywords: discrete-event systems；intermittent faults；fault diagnosis；safe diagnosability；recognizer；verifier

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学者的高度关注. Sampath等[1]提出了基于事件和诊断器的故障诊断方法;Zad等[2]提出了一种基于状态的故障诊断;文献[3]将故障诊断方法拓展至随机模型,提出了一种随机离散事件系统的故障诊断方法;文献[4]将文献[3]的方法从集中式系统推广至分布式系统,提出了一种分布式随机离散事件系统的故障诊断方法;文献[5]对模糊不确定系统提出了一种模糊离散事件系统的故障诊断方法;文献[6]也以模糊离散事件系统为模型,研究了基于状态的分布式诊断问题;Cabral等[7]则利用Petri网方法对离散事件系统的故障诊断进行研究;文献[8]针对不完备离散事件系统的故障诊断问题,提出了一种在模型不完备的前提下验证系统可诊断性的方法.

尽管上述各种故障诊断方法能够确保系统在故障发生之后的有限时延内将所发生的故障事件诊断出来,但是在故障被诊断出来之前的那段时延期间,系统仍然可能会执行某些被禁止的非法操作,这对于已处于故障运行模式的“病态”系统来说是极其危险的. 针对离散事件系统故障诊断的安全性,Paoli等[9]提出了一种安全故障诊断机制. 对此,文献[10]又提

收稿日期: 2018-08-01；**修回日期:** 2018-11-03.

基金项目: 国家自然科学基金项目(61673122)；广东省自然科学基金项目(2019A1515010548)；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(2016PY01).

责任编委: 卢剑权.

†通讯作者. E-mail: fliu2011@163.com.

出了具有多项式时间复杂度的安全诊断方法;同时,文献[11]对赋时离散事件系统的安全故障诊断进行了研究.

在这些故障诊断和安全故障诊断方法中,所考虑的故障都是永久性故障[1-2],即系统一旦发生故障,则系统在之后的运行过程中将一直处于故障运行模式.针对间歇性故障的故障诊断,文献[12-13]均进行了深入探讨,分别对基于状态的故障诊断方法[12]和基于事件的故障诊断方法[13]进行了研究.虽然文献[12-13]中都对间歇性故障进行了研究,但是它们均仅考虑了间歇性故障的故障诊断问题,没有考虑故障诊断期间的安全性问题.

本文继续文献[9,13]的工作,研究离散事件系统间歇性故障的安全诊断问题.先对发生间歇性故障的离散事件系统进行建模,给出系统对间歇性故障的安全可诊断性的形式化定义;再通过构造非法语言识别器对系统的非法操作进行识别,并在此基础上构建一个安全验证器,得到一个关于系统安全可诊断性的充分必要条件,实现离散事件系统对间歇性故障的安全诊断.这种安全诊断既保证了间歇性故障发生之后能被诊断出来,又确保了在故障诊断期间系统不会执行任何不安全操作.

1 离散事件系统与间歇性故障建模

1.1 离散事件系统

一个离散事件系统是指有限状态自动机[1]:

$$G=(X,\Sigma,\delta,x_0).$$

其中:X是有限状态集,Σ是事件集,$x_0\in X$是系统初始状态,δ是状态转移函数,$\delta:X\times\Sigma\to 2^X$.

事件集Σ被划分为可观事件集Σ_o和不可观事件集Σ_{uo}.记故障事件集为Σ_f,它满足$\Sigma_f\subseteq\Sigma_{uo}$,即故障事件均为不可观事件.通常可将故障事件划分为m种故障类型,即

$$\Sigma_f=\Sigma_{f1}\bigcup\Sigma_{f2}\bigcup\cdots\bigcup\Sigma_{fm},$$

其中m为故障类型数.

记符号Σ_r为恢复事件的集合.类似文献[13],假设$\Sigma_r\subseteq\Sigma_{uo}$,即恢复事件均为不可观事件.根据不同的故障类型,可将恢复事件集划分为相应的m种恢复事件类型,即

$$\Sigma_r=\Sigma_{r1}\bigcup\Sigma_{r2}\bigcup\cdots\bigcup\Sigma_{rm},$$

其中m为恢复事件类型数,且第$i\,(i\in[1,m])$类故障事件与第$i\,(i\in[1,m])$类恢复事件相互对应.

为了能够更好地描述对间歇性故障事件的诊断,引用文献[1,13]中的相关符号:$\bar{s}$是事件串s的包括空串ε在内的前缀闭包,其中$s\in\Sigma^*$;L是由自动机G生成的语言,$L=\{s\in\Sigma^*|(\exists x\in X)\delta(x_0,s)=x\}$;对于集合$A$和$B$,用符号$A\backslash x$表示将元素$x$从集合$A$中除去,$A\backslash B$表示集合$A$中除去集合$B$中的元素;$\Psi(\Sigma_{fi})$表示以第$i$类故障事件结尾的所有路径集合,即$\Psi(\Sigma_{fi})=\{s\sigma\in L|\sigma\in\Sigma_{fi}\}$;$\Psi(\Sigma_{ri})$表示以第$i$类恢复事件结尾的所有路径集合,即$\Psi(\Sigma_{ri})=\{s\sigma\in L|\sigma\in\Sigma_{ri}\}$.

定义1 设$G=(X,\Sigma,\delta,x_0)$是一个离散事件系统,定义对于投影$P:\Sigma^*\to\Sigma_o^*$为一个满足如下规则的映射:对任意的$\sigma\in\Sigma$,如果$\sigma\in\Sigma_o$,则$P(\sigma)=\sigma$;如果$\sigma\in\Sigma_{uo}$,则$P(\sigma)=\epsilon;P(\epsilon)=\epsilon,P(s\sigma)=P(s)P(\sigma)$,其中$s\in\Sigma^*,\sigma\in\Sigma$.

反投射$P^{-1}:\Sigma_o^*\to\Sigma^*$是指满足以下规则的映射:对于$y\in\Sigma_o^*,P^{-1}(y)=\{s\in L|P(s)=y\}$.

1.2 间隙性故障建模

假设系统中有m种故障类型,先给出m个标记自动机,以跟踪系统G的运行状况.对第i类故障及恢复事件,定义系统G的i-标记自动机为

$$G_\Omega^i=(Q_\Omega^i,\Sigma_\Omega^i,\delta_\Omega^i,q_0^i),\ i\in[1,m].$$

其中:状态集$Q_\Omega^i=\{N,F_i,R_i\}$;初始状态$q_0^i=N$;事件集合$\Sigma_\Omega^i=\{\Sigma_{fi},\Sigma_{ri},\Sigma\setminus\Sigma_{ri},\Sigma\setminus\Sigma_{fi}\}$;转移函数$\delta_\Omega^i:Q_\Omega^i\times\Sigma_\Omega^i\to Q_\Omega^i$,转移规则如图1所示.

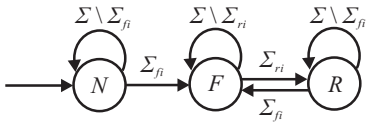


图1 i-标记自动机G_Ω^i

接下来,将自动机G与m个i-标记自动机G_Ω^i进行乘积运算,得到标记后的自动机G_l,并称G_l为系统G的并行器,表示为

$$G_l=G\times G_\Omega^1\times G_\Omega^2\times\ldots\times G_\Omega^m=(G_l,\Sigma,\delta_l,q_{l0}).$$

其中:Σ是事件集合,$q_{l0}=(x_0,N)$是初始状态;$Q_l\subseteq X\times l(s)$是状态集合,这里$Q_l=(X\times l(s))$,$l(s)$是标识函数,设标记集合$\Delta=\{F_1,F_2,\ldots,F_m\}\bigcup\{R_1,R_2,\ldots,R_m\}$,则标记函数$l(s)\in 2^{\{\Delta\cup\{N\}\}}$;$l(s)$的表现形式有$l(s)=\{N\}$和$l(s)=\{F_{i_1},F_{i_2},\ldots,F_{i_k}\}\bigcup\{R_{i_1},R_{i_2},\ldots,R_{i_n}\}$,且$\{i_1,i_2,\ldots,i_k\}\subseteq\{1,2,\ldots,m\}$,$\{i_1,i_2,\ldots,i_n\}\subseteq\{1,2,\ldots,m\}$,$i_k\neq i_n$.标识函数$l(s)$的定义如下:如果$\Sigma_{fi}\notin s,\Sigma_{ri}\notin s$,则$l(s)=\{N\}$;如果$\exists s',s''$,有$s=s's''$,且$s'\in\Psi(\Sigma_{fi}),\Sigma_{ri}\notin s''$,则$F_i\in l(s)$;如果$\exists s',s''$,有$(s=s's'')\bigwedge(\Sigma_{fi}\in s')\bigwedge[s'\in\Psi(\Sigma_{ri})]\bigwedge(\Sigma_{fi}\notin s'')$,则$R_i\in l(s)$.

G_l中的转移函数$\delta_l:Q_l\times\Sigma\to Q_l$,对于任意

$\sigma \in \Sigma, s \in L$,其转移规则如下:

1) 当$\sigma \notin \Sigma_{fi}, \sigma \notin \Sigma_{ri}$时

$$\delta_l((x, l(s)), \sigma) = (\delta(x, \sigma), l(s)).$$

2) 当$\sigma \notin \Sigma_{fi}, \sigma \in \Sigma_{ri}$时:

① 若$F_i \notin l(s)$,则$\delta_l((x, l(s)), \sigma) = (\delta(x, \sigma), l(s))$;

② 若$F_i \in l(s)$,则$\delta_l((x, l(s)), \sigma) = (\delta(x, \sigma), l'(s))$,其中$l'(s) = (l(s) \setminus F_i) \bigcup \{R_i\}$.

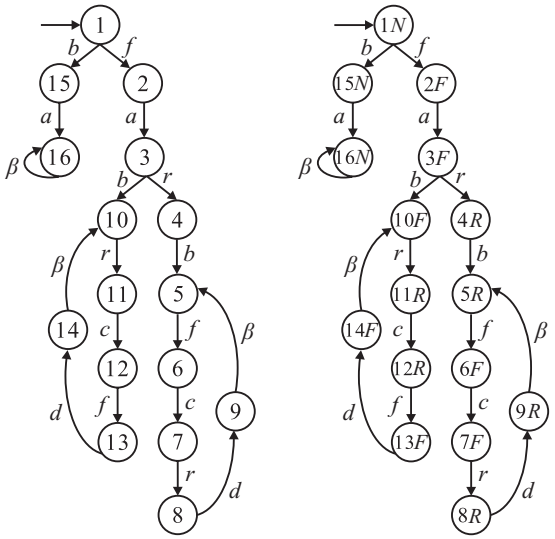
3) 当$\sigma \in \Sigma_{fi}$时:

① 若$l(s) = \{N\}$,则$\delta_l((x, l(s)), \sigma) = (\delta(x, \sigma), l'(s))$,其中$l'(s) = (l(s) \setminus N) \bigcup F_i$;

② 若$R_i \in l(s)$,则$\delta_l((x, l(s)), \sigma) = (\delta(x, \sigma), l'(s))$, 其中$l'(s) = (l(s) \setminus R_i) \bigcup F_i$;

③ 若$N \notin l(s), F_i \notin l(s), R_i \notin l(s)$,则$\delta_l((x, l(s)), \sigma) = (\delta(x, \sigma), l'(s))$, 其中$l'(s) = l(s) \bigcup F_i$.

例1　考虑图2(a)中的自动机G_1,其中$\Sigma_{fi} = \Sigma_f = \{f\}, \Sigma_{ri} = \Sigma_r = \{r\}, \Sigma_o = \{a, b, c, d, \beta\}$,则$G_1$的并行器$G_{l1}$可构建为如图2(b)所示.



(a) 自动机G_1　　(b) 并行器G_{l1}

图2　自动机G_1和并行器G_{l1}

2　安全可诊断性的形式化

给定禁止事件串集$\Phi_i (\Phi_i \subseteq \Sigma^*)$,根据不同的故障类型,将禁止事件串划分为相应的不同类型$\Phi = \Phi_1 \bigcup \Phi_2 \bigcup \ldots \bigcup \Phi_m, m$表示被禁止事件串的类型数,$\Phi_i$表示第$i$种类型的被禁止事件串.

下面引入一个集合Φ_i',它表示在故障事件发生之后直至被禁止事件串恰好发生时的这段期间没有发生恢复事件的事件串,即

$$\Phi_i' = \{t' \in L/s | s \in \Psi(\Sigma_{fi})(\exists u' \in \Sigma^*)(\Sigma_{ri} \notin u')(\exists v' \in \Phi_i)(t' = u'v')\}.$$

定义2　设Φ是禁止事件串,将G的非法语言定义为$\xi = \bigcup_{i=1}^{m} \xi_i$,其中每个$\xi_i$定义为

$$\xi_i = \{u \in L/s | [s \in \Psi(\Sigma_{fi})](\exists v \in \Phi_i')(v \in u)(\Sigma_{ri} \notin u)\},$$

这里$v \in u$表示v是u中的某子串.

定义3　设$G = (X, \Sigma, \delta, x_0)$是一个离散事件系统,如果$G$同时满足以下可诊断条件和安全性条件,则称$G$是一个安全可诊断系统:

1)可诊断性条件:对于任意$\Sigma_{fi} \in \Sigma_f$,在并行器G_l中,有

$$(\exists n \in \boldsymbol{N})[\forall s \in \Psi(\Sigma_{fi})](\forall t \in L/s)[\|t\| \geqslant n] \Rightarrow D_{sd},$$

诊断条件D_{sd}为

$$(\exists t' \leqslant t) : \forall \omega \in [P^{-1}(P(st'))] \Rightarrow F_i \in l(\omega),$$

其中$t' \leqslant t$表示t'是t的前缀子串.

2)安全性条件:对于任意的$\Sigma_{fi} \in \Sigma_f$,都有

$$[\forall s \in \Psi(\Sigma_{fi})](t \in L/s)(\overline{t_c} \bigcap \xi_i = \varnothing),$$

其中t_c是满足诊断条件D_{sd}中t'的最短前缀.

3　非法语言识别器与安全验证器的构造

在构造非法语言识别器之前,先引入禁止标识符集$\Lambda \in 2^{\Lambda_1 \cup \Lambda_2 \cup \ldots \cup \Lambda_m \cup \{NB_0\}}$,其中$\Lambda_i = \{NB_i, F_iB, B_i\}, 1 \leqslant i \leqslant m$.

NB_0表示系统从初始状态开始运行的过程中没有发生任何故障;NB_i表示系统发生第i类故障后又发生了对应类型的恢复事件,即表示系统中由第i类故障带来的影响消失;F_iB表示系统发生了第i类故障事件,且发生后既无对应恢复事件的发生,也无被禁止事件串发生;B_i表示系统发生了第i类故障事件,并在发生恢复事件之前发生了第i类禁止事件串.

定义4　设$G = (X, \Sigma, \delta, x_0)$的并行器为$G_l$,将$G$的非法语言识别器构造为如下有限状态自动机:

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

其中:$q_{r0} = (x_0, N, NB_0)$为初始状态;$Q_r \subseteq Q_l \times \Lambda$为有限状态集;$\delta_r$为转移函数,$\delta_r : Q_r \times \Sigma Q_r$. 对于任意$\sigma \in \Sigma, s \in \Sigma^*$,自动机$Q_r$中的转移规则定义如下:

1) 当$\sigma \notin \Sigma_{fi}$时

$$\delta_r((q_{l0}, NB_0), \sigma) = (\delta_l(q_{l0}, \sigma), NB_0).$$

2) 若存在$s \in \Sigma^*$使得$\delta_r(q_r, s) = q_{rk} = (q_l, \Lambda)$,其中$FB_i \in \Lambda$,则:

① 当$\sigma \notin \Sigma_{fi}, \sigma \notin \Sigma_{ri}, s\sigma \notin \xi_i$时

$$\delta_r(q_{rk}, \sigma) = \delta_r((q_l, \Lambda), \sigma) = (\delta_l(q_l, \sigma), \Lambda);$$

② 当$\sigma \notin \Sigma_{fi}, \sigma \notin \Sigma_{ri}, s\sigma \in \xi_i$时

$$\delta_r(q_{rk}, \sigma) = \delta_r((q_l, \Lambda), \sigma) = (\delta_l(q_l, \sigma), \Lambda'),$$

其中$\Lambda' = (\Lambda \setminus \{F_iB\}) \bigcup \{B_i\}$.

3) 当$\sigma \in \Sigma_{fi}$时:

① $\delta_r((q_l, NB_0), \sigma) = (\delta_l(q_l, \sigma), F_iB)$;

② 若$(q_l, \Lambda) \in Q_r, F_iB \in \Lambda$,则$\delta_r((q_l, \Lambda), \sigma) = (\delta_l(q_l, \sigma), \Lambda)$;

③ 若$(q_l, \Lambda) \in Q_r, F_iB \notin \Lambda, N_iB \notin \Lambda, N_0B \notin \Lambda, B_i \notin \Lambda$,则$\delta_r((q_l, \Lambda), \sigma) = (\delta_l(q_l, \sigma), \Lambda')$,其中$\Lambda' = \Lambda \bigcup \{F_iB\}$;

④ 若$(q_l, \Lambda) \in Q_r, NB_i \in \Lambda$,则$\delta_r((q_l, \Lambda), \sigma) = (\delta_l(q_l, \sigma), \Lambda')$,其中$\Lambda' = (\Lambda \setminus \{NB_i\}) \bigcup \{F_iB\}$;

⑤ 若$(q_l, \Lambda) \in Q_r, B_i \in \Lambda$,则$\delta_r((q_l, \Lambda), \sigma) = (\delta_l(q_l, \sigma), \Lambda)$.

4) 当$\sigma \in \Sigma_{ri}$时:

① $\delta_r((q_l, NB_0), \sigma) = (\delta_l(q_{l0}, \sigma), NB_0)$;

② 若$(q_l, \Lambda) \in Q_r, B_i \in \Lambda$,则$\delta_r((q_l, \Lambda), \sigma) = (\delta_l(q_l, \sigma), \Lambda')$,其中$\Lambda' = (\Lambda \setminus \{B_i\}) \bigcup \{NB_i\}$;

③ 若$(q_l, \Lambda) \in Q_r, NB_i \in \Lambda$,则$\delta_r((q_l, \Lambda), \sigma) = (\delta_l(q_l, \sigma), \Lambda)$;

④ 若$(q_l, \Lambda) \in Q_r, FB_i \in \Lambda$,则$\delta_r((q_l, \Lambda), \sigma) = (\delta_l(q_l, \sigma), \Lambda')$,其中$\Lambda' = (\Lambda \setminus \{FB_i\}) \bigcup \{NB_i\}$.

例如,由图1中的并行器G_{l1}构造的非法语言识别器G_{r1}如图3所示,其中禁止事件串$\Phi = \{\beta\}$.

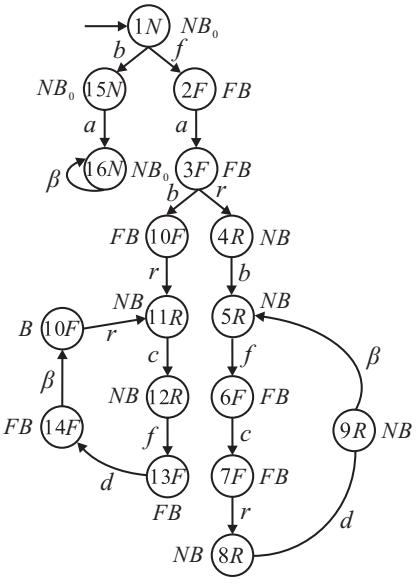


图3 非法语言识别器G_{r1}

接下来,构造安全验证器G_v^s.

定义5 设$G = (X, \Sigma, \delta, x_0)$,将$G$的安全验证器构造为有限自动机,有

$$G_v^s = (Q_v^s, \Sigma_o, \delta_v^s, q_{v0}).$$

其中:$q_{v0} = (x_0, N, NB_0)$为安全验证器初始状态;$Q_v^s \subseteq 2^{Q_r}$为有限状态集;转移函数$\delta_v^s : Q_v^s \times \Sigma_o \to Q_v^s$. 对于任意$q_v^s \in Q_v^s, \tau \in \Sigma_o$,有

$$\delta_v^s(q_v^s, \tau) = \bigcup_{q_r \in q_v^s} \bigcup_{s \in L_\tau(G_r, q_r)} \{(\delta_r(q_r, s))\}.$$

4 安全可诊断性的充分必要条件

设$G_r = (Q_r, \Sigma, \delta_r, q_{r0})$是系统$G = (X, \Sigma, \delta, x_0)$的非法语言识别器,$G_v^s = (Q_v^s, \Sigma_o, \delta_v^s, q_{v0})$是$G$的安全验证器,且$q_v^s \in Q_v^s$.

1) 若对于任意的$q_r \in q_v^s, q_r = (x, l(s), \Lambda)$都有$F_i \in l(s)$,则称$q_v^s$是$F_i$-确定状态;

2) 若存在$q_r \in q_v^s, q_r' \in q_v^s$,其中$q_r = (x, l(s), \Lambda)$, $q_r' = (x', l'(s), \Lambda')$,如果$F_i \in l(s), F_i \notin l'(s)$,则称$q_v^s$是$F_i$-不确定状态;

3) 若对于任意的$q_r \in q_v^s, q_r = (x, l(s), \Lambda)$都有$R_i \in l(s)$或者$N \in l(s)$,则称$q_v^s$是$F_i$-缺失状态.

定理1 设自动机$G = (X, \Sigma, \delta, x_0)$是一个具有间歇性故障的离散事件系统,$G_v^s = (Q_v^s, \Sigma_o, \delta_v^s, q_{v0})$是$G$的安全验证器,则$G$的间歇性故障为安全可诊断的充分必要条件是$G_v^s$同时满足以下条件:

1) 不存在如下状态q_v^s: q_v^s是F_i-不确定状态,且q_v^s中存在$q_r = (x, l(s), \Lambda)$,使得$F_i \in l(s), B_i \notin \Lambda$.

2) 不存在如下两个状态q_i^s, q_{i+1}^s:① q_i^s是F_i-不确定状态或F_i-缺失状态;② q_{i+1}^s是F_i-确定状态,存在$q_r' = (x', l'(s), \Lambda) \in q_{i+1}^s, F_i \in l'(s), B_i \in \Lambda$;③ 存在$e \in \Sigma_o$,使得$\delta_v^s(q_i^s, e) = q_{i+1}^s$.

证明 先用反证法证明充分性.

若G不满足可诊断条件,则在G_l中,存在$u, v \in \Sigma^*$,且对任意的$t' \leqslant t$,使得u、$v \in P_L^{-1}[P(st')], F_i \in l(u), F_i \notin l(v)$. 由于$P(u) = P(v)$,则在$G_v^s$中存在$q_v^s$使得$q_r$、$q_r' \in q_v^s$,且$q_r = (\delta(x_0, u), l(u), \Lambda), q_r' = (\delta(x_0, v), l(v), \Lambda')$,其中$B_i \in \Lambda, F_i \in l(u), B_i \notin \Lambda'$, $F_i \notin l(v)$. 即q_v^s是安全验证器G_v^s中的F_i-不确定状态. 这与假设中满足定理1中的条件1)矛盾.

若G不满足安全性条件但满足诊断条件,则假设$u = u_1u_2e$满足诊断条件,并且$u_2 \in \xi_i, e \in \Sigma_o, t_c = u_2e$,因此存在$q_i^s = \delta_v^s(q_{v0}, P(u_1u_2))$,使得$F_i$-确定状态$q_{i+1}^s = \delta_v^s(q_i^s, e)$. 若$q_i^s$是$F_i$-不确定状态,则因为$u_2 \in \xi_i$,所以存在$q_r' = (x', l'(s), \Lambda') \in q_{i+1}^s, B_i \in \Lambda'$;若$q_i^s$是$F_i$-缺失状态,则因为存在事件$e \in \Sigma_o$,而使$q_{i+1}^s = \delta_v^s(q_i^s, e)$,且$q_{i+1}^s$是$F_i$-确定状态,即存在$q_r' = (x', l'(s), \Lambda') \in q_{i+1}^s, B_i \in \Lambda'$. 综上$q_i^s$是$F_i$-不确定状态或者$F_i$-缺失状态,而$q_{i+1}^s$是$F_i$-确定状态,且有标记$B_i$. 这里与假设中$G_v^s$满足定理1中的条件2)矛盾.

再用反证法证明必要性.

假设G是安全可诊断的,如果安全验证器G_v^s不满足定理1中的条件1),则存在F_i-不确定状态$q_v^s \in Q_v^s$,使得在非法语言识别器G_r中存在u、$v \in \Sigma^*$, $P(u) = P(v), \delta_r(q_{r0}, u) = (x, l(u), \Lambda), \delta_r(q_{r0}, v) = (x', l(v), \Lambda')$,其中$F_i \notin l'(s), B_i \in \Lambda, F_i \in l(s), B_i \notin \Lambda'$,即$u \bigcap \xi_i \neq \varnothing$;而在并行器$G_l$中存在两条映

射相同的路径u和v,使得$\delta_l((x_0,N),u)=(x,l(u))$, $\delta_l((x_0,N),v)=(x',l(v)),F_i\in l(u),F_i\notin l(v)$. 即安全可诊断定义条件不成立,与假设矛盾.

如果G_v^s不满足定理1中的条件2),则存在Q_v^s中存在状态q_i^s和q_{i+1}^s,q_i^s是F_i-不确定状态(缺失)状态,且存在$e\in\Sigma_o$,使得F_i-确定状态$q_{i+1}^s=\delta_v^s(q_i^s,e)$;设存在$s\in\Sigma^*,q_i^s=\delta_v^s(q_{v0},s)$,也即存在$u$和$v$使得在$G_l$中$x=(\delta(x_0,u),l(u)),y=(\delta(x_0,v),l(v))$,其中$F_i\in l(u),F_i\notin l(v)$.事件串$u=u_1u_2,u_1\in\Psi(\Sigma_{fi}),\Sigma_{ri}\in u_2$.如果$G$满足可诊断条件,则存在$n\in\boldsymbol{N},t=L/u_1,\|t\|=n,t'\leqslant t$使条件$D_{sd}$成立. 取$t=e\in L/u$,则$q_{i+1}^s=\delta_v^s(q_v^s,e)$. 用$u'$表示$ut$,即$u'=u_1u_2t$,则有$t'=u_2t$,即$t'=u_2e$. 因此,$t'\in\xi_i$,即$\overline{t'}\bigcap\xi_i\neq\varnothing$. 根据定义3,$G$的间歇性故障不是安全可诊断的. 这与假设相互矛盾. □

例2　考虑图2中的具有间歇性故障的离散事件系统G_1,G_1的安全验证器G_{v1}^s可构造如图4所示.

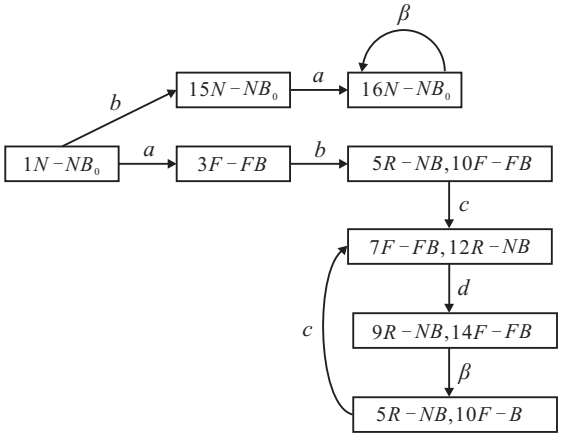


图4　安全验证器G_{v1}^s

由图4中的验证器G_{v1}^s不难看出,状态$(5R-NB,\ 10F)$中,有标记R和F,即它是F_i-不确定状态,并且状态$(5R-NB,\ 10F-B)$中含有标记B,表示在未诊断出间歇性故障时系统执行了非法操作. 因此,根据定理1,G_1的间歇性故障不是安全可诊断的.

例3　考虑离散事件系统G_2,如图5所示,其中$\Sigma_o=\{a,b,c,d,\sigma_s\},\Sigma_{fi}=\Sigma_f=\{f\},\Sigma_{ri}=\Sigma_r=r,\Phi_i=\Phi=\{\sigma_s\}$.

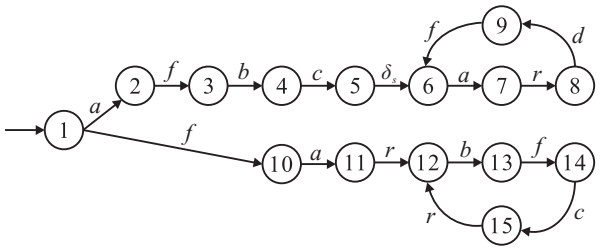
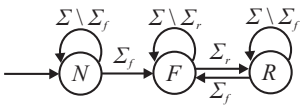
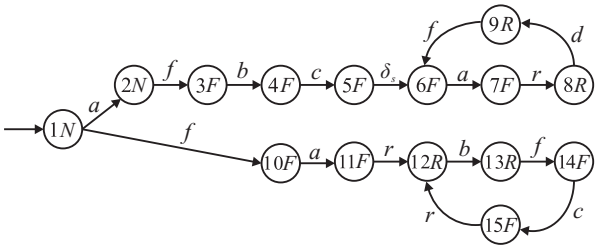


图5　自动机G_2

G_2的标记自动机G_Ω如图6(a)所示,图6(b)为G_2与G_Ω进行笛卡尔积运算后的并行器G_{l2}.



(a) i-标记自动机G_Ω



(b) 并行器G_{l2}

图6　i-标记自动机G_Ω和并行器G_{l2}

根据定义4,可构造G_2的非法语言识别器G_{r2}如图7所示.

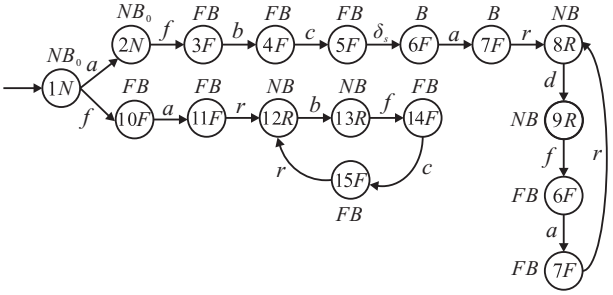


图7　非法语言识别器G_{r2}

根据G_{r2}构造出安全验证器G_{v2}^s,如图8所示.

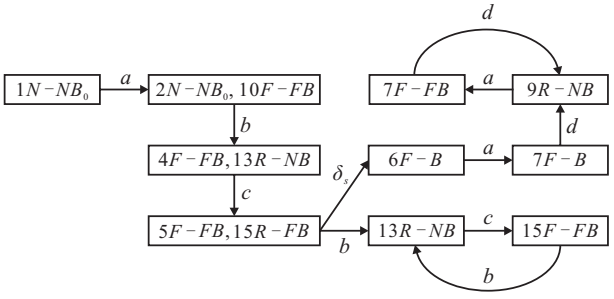


图8　安全验证器G_{v2}^s

在图8中,验证器G_{v2}^s中不存在有标记B_i的F_i-不确定状态,并且满足定理1中的条件2). 根据定理1得,G_2的间歇性故障具有安全可诊断性.

5　结　论

本文考虑了离散事件系统间歇性故障的安全诊断问题. 具有安全可诊断性的系统不仅能够将发生的间歇性故障及时诊断出来,并且确保了在诊断期间系统不执行任何非法操作. 通过构造安全验证器,得到了安全可诊断性的充分必要条件.

参考文献(References)

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

[2] Zad H, Kwong R H, Wonham W M. Fault diagnosis in discrete-event systems: Framework and model reduction[J]. IEEE Transactions on Automatic Control, 1998, 48(7): 1199-1212.

[3] Thorsley D, Teneketzis D. Diagnosability of stochastic discrete-event systems[J]. IEEE Transactions on Automatic Control, 2005, 50(4): 476-492.

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

[5] Liu F, Qiu D. Diagnosability of fuzzy discrete-event systems: A fuzzy approach[J]. IEEE Transactions on Fuzzy Systems, 2006, 17(2): 372-384.

[6] Deng W, Qiu D. State-based decentralized diagnosis of bi-fuzzy discrete event systems[J]. IEEE Transactions on Fuzzy Systems, 2017, 25(4): 854-867.

[7] Cabral F G, Moreira M V, Diene O, et al. A petri net diagnoser for discrete event systems modeled by finite state automata[J]. IEEE Transactions on Automatic Control, 2015, 60(1): 59-71.

[8] 王晓宇, 欧阳丹彤, 赵相福. 不完备离散事件系统的可诊断性[J]. 软件学报, 2015, 26(6): 1373-1385.
(Wang X Y, Ouyang D T, Zhao X F. Diagnosability of discrete event systems with an incomplete model[J]. Journal of Software, 2015, 26(6): 1373-1385.)

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

[10] 刘富春, 罗苹. 具有多项式时间复杂性的离散事件系统安全诊断[J]. 控制理论与应用, 2017, 34(6): 717-722.
(Liu F C, Luo P. Polynomial-time verification of safe diagnosability of discrete-event systems[J]. Control Theory & Applications, 2017, 34(6): 717-722.)

[11] 刘富春, 蔡家德. 赋时离散事件系统的安全诊断[J]. 控制与决策, 2017, 32(11): 2081-2084.
(Liu F C, Cai J D. Safe diagnosability of timed discrete-event systems[J]. Control and Decision, 2017, 32(11): 2081-2084.)

[12] Biswas S. Diagnosability of discrete event systems for temporary failures[J]. Computers and Electrical Engineering, 2012, 38(6): 1534-1549.

[13] Contant O, Lafortune S, Teneketzis D. Diagnosis of intermittent faults[J]. Discrete Event Dynamic Systems, 2004, 14(2): 171-202.

作者简介

刘富春(1971−), 男, 教授, 博士生导师, 从事控制理论、算法设计等研究, E-mail: fliu2011@163.com;

唐顺桥(1993−), 男, 硕士生, 从事控制理论、算法设计的研究, E-mail: 2215907230@qq.com;

赵锐(1976−), 女, 讲师, 博士, 从事离散事件系统、智能计算等研究, E-mail: zhaorui118204@163.com;

邓秀勤(1966−), 女, 教授, 从事智能计算、机器学习等研究, E-mail: dxq706@gdut.edu.cn;

崔洪刚(1976−), 讲师, 博士, 从事大数据与智能计算等研究, E-mail: cuihg@163.com.

(责任编辑：齐 霁)