DOI：10.11830/ISSN.1000-5013.201605114

离散事件系统的故障一次可修复性诊断

郭忠宝，王飞，刘清兰，张波业

（华侨大学 信息科学与工程学院，福建 厦门 361021）

摘要： 为了突破周期可修复性的局限性，提出一种新的可修复性定义及相关诊断方法.针对可修复状态为一次可达状态的情况，通过详细分析这类离散事件系统的特点，提出一次可修复性的形式化定义；然后，从不可区分串和可修复性诊断器角度，讨论一次可修复性的诊断方法和证明过程.实例结果表明：所提出的一次可修复性诊断方法能有效解决系统的诊断需求.

关键词： 离散事件系统；不可区分串；状态估计；可修复性

中图分类号： TP 271.8 **文献标志码：** A **文章编号：** 1000-5013(2018)03-0451-06

Diagnosis of Disposable Recoverability Based on Discrete Event Systems With Faults

GUO Zhongbao, WANG Fei, LIU Qinglan, ZHANG Boye

(College of Information Science and Engineering, Huaqiao University, Xiamen 361021, China)

Abstract: In order to break through the limitations of periodic recoverability, a new definition of recoverability and related diagnostic methods are proposed. Aiming at the situation that the recoverable state is once reachable state, a formal definition of disposable recoverability is proposed after analysing the characteristics of this kind of discrete event systems in detail, and then the diagnostic methods and theoretical proofs of disposable recoverability are discussed from two aspects, indistinguishable strings and diagnoser. The results of an example show that the diagnosis methods of disposable recoverability can effectively solve the diagnostic requirements of the system.

Keywords: discrete event systems; indistinguishable string; state estimate; recoverability

随着现代工程系统的不断复杂化，自动化生产领域因设备故障引发的事故变得难以预测.如何有效区分故障类型[1]、检测和诊断故障[2-4]，以及如何及时采取适当的修复措施显得尤为重要.由于这类故障的离散化和事件驱动的特点，基于离散事件模型[5-6]的故障诊断和容错控制是十分有效的.容错控制[7]虽然能保证离散事件系统在安全的故障模式下运行，然而，其性能往往会降低.基于状态[8]的故障诊断建模往往涉及到更为一般的状态估计问题[9-10].关于故障恢复问题，Saboori 等[11]提出系统控制的 3 种模式，即正常模式、过度模式和恢复模式.Qin 等[12]在事件完全可观的假设下进行思考，但可修复性局限于返回非故障状态.Shu 等[13-14]对可修复性概念进行进一步研究，提出具体的可修复性理论及检测策略.离散事件系统的可纠错研究中将系统状态分成可接受状态和不可接受状态[15-16]，对可纠错状态形式

收稿日期： 2016-05-03

通信作者： 王飞(1977-)，男，副教授，博士，主要从事离散事件系统、资源优化配置的研究.E-mail：feiw545@163.com.

基金项目： 国家自然科学基金资助项目(61203040)

化,故障纠错的目标是控制系统进入到可接受状态圈,纠错结果极大地缩小了系统的状态量.基于此,本文对离散事件系统的故障可修复性概念进行拓展,提出一次可修复性的定义,并给出相关诊断策略.

1 故障状态的离散事件系统

用确定性自动机模型描述一个离散事件系统,即

$$G=(Q,\Sigma,\delta,q_0). \tag{1}$$

式(1)中:Q 为离散状态集合;Σ 为离散事件集合;$\delta:Q\times\delta\to Q$ 是状态转移关系;q_0 是初始状态.$\delta(q,s)$ 有定义可用 $\delta(q,s)!$ 表示,即 $\delta(q,s)\neq\emptyset$.因此,自动机的形式语言可表示为 $L(G)=\{s\in\Sigma^*:\delta(q_0,s)!\}$.

假设系统有一个正常模式和 k 个故障模式,正常模式用 $G_0=(Q_0,\Sigma_0,\delta_0,q_0)$ 表示,第 i 个故障模式 $G_i=(Q_i,\Sigma_i,\delta_i)(i=1,2,\cdots,k)$,$G_i$ 的初始状态与 G_0 下发生第 i 类故障的状态有关,Σ_i 可分为可观事件集 $\Sigma_{o,i}$ 和不可观事件集 $\Sigma_{uo,i}$.对于 G_i 的部分事件可观测情形可以描述为

$$P_i(\varepsilon)=\varepsilon,\qquad P_i(s\sigma)=\begin{cases}P_i(s)\sigma, & \sigma\in\Sigma_{o,i},\\ P_i(s), & \sigma\notin\Sigma_{o,i}.\end{cases}$$

假设故障只在正常模式中发生,第 i 类故障 f_i 发生后,系统由 G_0 进入 G_i,G_i 不再发生其他故障,因此,故障集 $F=\{f_i:i=1,2,\cdots,k\}$.简单起见,同样地,用 f_i 表示当故障 f_i 发生时的状态转移映射关系,即

$$f_i:Q_0\to Q_i,\qquad i=1,2,\cdots,k.$$

上式中:$Q_0=\{q_{1,0},q_{2,0},\cdots,q_{|Q_0|,0}\}$;$Q_i=\{q_{1,i},q_{2,i},\cdots,q_{|Q_i|,i}\}$;$f_i(q_{1,0})=q_{m,i}$ 表示故障 f_i 在状态 $q_{1,0}$ 发生,系统进入故障模式 G_i 且下一个状态为 $q_{m,i}$.

包含故障状态的离散事件系统 $H=(G_0,G_1,\cdots,G_k,F)$ 可看成一个扩展自动机[13],有

$$G_{exd}=Ac(Q_{exd},\Sigma_{exd},\delta_{exd},q_0). \tag{2}$$

式(2)中:$Q_{exd}=Q_0\cup Q_1\cup\cdots\cup Q_k$;$\Sigma_{exd}=\Sigma_0\cup\Sigma_1\cup\cdots\cup\Sigma_k\cup\{f_i:i=1,2,\cdots,k\}$;$\delta_{exd}=\delta_0\cup\delta_1\cup\cdots\cup\delta_k\cup\{(q_{1,0},f_i,q_{m,i}):f_i(q_{1,0})=q_{m,i}\}$.

对于故障 f_i,其故障语言可表示为 $L_i=\{s\in L(G_{exd}):(\exists s_1,s_2\in\Sigma_{exd}^*)s=s_1f_is_2\}$,当前状态估计 $SE=\{q:(\exists t\in L(G_{exd}))P(t)=P(s)\wedge q\in\delta_{exd}(q_0,t)\}$.

2 修复行为

为方便建模,假设每一个故障模式对应一种修复行为.修复行为集合表示为

$$\underset{r}{\Sigma}=\{r_1,r_2,\cdots,r_i,\cdots,r_k\}. \tag{3}$$

式(3)中:r_i 表示故障 f_i 对应的修复行为,在 G_i 的可修复状态触发 r_i 能使系统恢复到正常模式运行.因此,Q_i 分为可修复状态集合 $Q_{r,i}$ 和不可修复状态集合 $Q_{ur,i}$,仅当系统到达 $Q_{r,i}$ 时,可以触发 r_i,即

$$R_i:Q_i\to\{0,1\},\qquad i=1,2,\cdots,k.$$

上式中:$R_i(q_{1,i})=\begin{cases}1, & q_{1,i}\in Q_{r,i},\\ 0, & q_{1,i}\in Q_{ur,i}.\end{cases}$

对于给定的 $s\in L_i$,不可区分串的集合[14]定义为

$$L_{ind}(s)=\{s':\delta_{exd}(q_0,s')!\wedge P(s)=P(s')\}. \tag{4}$$

确定性自动机中的不可区分串是由于部分事件不可观导致不同事件序列有相同投影,而相同投影无法对原不同事件序列进行有效区分.假设 t 是故障模式 G_i 中初始状态 $q_{m,i}$ 下有定义的事件序列,同理可定义 G_i 下不可区分串集 $L_{ind}^i(t)=\{t':\delta_{exd}(q_{m,i},t')!\wedge P_i(t)=P_i(t')\}$.

3 离散事件系统的故障一次可修复性

针对各个故障模式,文献[14]给出以下2个假设条件.

假设 1　任一故障模式 $G_i(i=1,2,\cdots,k)$均为非死锁，即对于 G_i 中的任一状态 $q\in Q_i$，至少有一个事件有定义，即

$$(\forall\ \in Q_i)(\exists\sigma\in\Sigma_i)\delta_i(q,\sigma)!,\qquad i=1,2,\cdots,k.$$

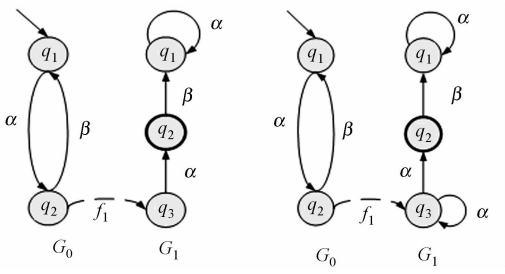
假设 2　任一故障模式 $G_i(i=1,2,\cdots,k)$，不存在只包含不可观事件的环，即

$$\neg(\exists q\in Q_i)(\exists s\in\Sigma_{\mathrm{uo},i}^{*})s\neq\varepsilon\wedge q\in\delta_i(q,s).$$

文献[14]的可修复状态出现在环上，将这种情况称为周期可修复性.

故障的离散事件系统，如图 1 所示. 图 1(a)中：系统存在故障 f_1 和相应的修复行为 r_1，可修复状态 $q_{2,1}$未出现在环上，初始状态为 $q_{1,0}$. 假设事件和故障均可观测，$\alpha f_1\alpha$ 后系统到达 $q_{2,1}$，此时，可以触发 r_1，系统具有可修复性，但是如果不触发 r_1，系统将进入且一直处于 $q_{1,1}$状态，此后，没机会再触发 r_1. 因此，系统进入 G_1 后，有且仅有一次机会触发 r_1. 假设事件 β 不可观测，则有 $P(\alpha f_1\alpha\beta)=P(\alpha f_1\alpha)$，存在不可区分串，$\mathrm{SE}(\alpha f_1\alpha)=\{q_{2,1},q_{1,1}\}$，不能确定系统是否处于 $q_{2,1}$. 因此，系统不可修复.

图 1(b)中：系统进入 G_1 后，系统可能经过事件序列 $\alpha\alpha\alpha\cdots$且一直处于状态 $q_{3,1}$. 因此，系统也不具有可修复性. 为了避免概念混淆，增加 2 个假设条件.



(a) 系统 1　　(b) 系统 2

图 1　故障的离散事件系统

Fig. 1　Faulty discrete event systems

假设 3　任一故障模式 $G_i(i=1,2,\cdots,k)$均不存在包含 $Q_{\mathrm{r},i}$状态的环，即

$$(\nexists q\in Q_{\mathrm{r},i})(\forall s\in\Sigma_i^{*})q\in\delta_i(q,s).$$

假设 4　任一故障模式 $G_i(i=1,2,\cdots,k)$，轨迹均经过 $Q_{\mathrm{r},i}$，且到达 $Q_{\mathrm{r},i}$之前不经过任何环，即

$$(\exists q\in Q_{\mathrm{r},i})(\exists q'\in Q_i)(\forall s\in\Sigma_i^{*})(\nexists s'\in\mathrm{Pr}(s))q\in\delta_i(q',s)\ \vee\ q'\in\delta_i(q',s').$$

上式中：$\mathrm{Pr}(s)$表示事件序列 s 的所有前缀的集合.

定义　对于给定的有故障的离散事件系统 H，假设故障模式 $G_i(i=1,2,\cdots,k)$后，随着系统在 G_i 中运行，有且仅有一次机会触发相应的修复行为 r_i，那么，称系统具有一次可修复性，即

$$(\forall s\in L_i)(\forall t\in\Sigma_i^{*})(\exists n\in\mathbf{N})\mid t\mid>n\wedge\delta_{\mathrm{exd}}(q_0,st)!\Rightarrow$$
$$(\exists s=hf_i)(\exists t'\in\mathrm{Pr}(t))(\exists L_{\mathrm{ind}}^{i}(t')=\emptyset)R_i(\delta_{\mathrm{exd}}(q_0,st'))=1$$
$$\vee\ (\exists s=hf_i)(\exists t'\in\mathrm{Pr}(t))(\exists L_{\mathrm{ind}}(t')=\emptyset)(\exists s'\sigma_1\in L_{\mathrm{ind}}^{i}(t'\sigma_1))R_i(\delta_{\mathrm{exd}}(q_0,st'\sigma_1))=1\Rightarrow$$
$$(\exists s''\in L_i)(\mathrm{SE}(s'')\subseteq Q_{\mathrm{r},i}.$$

上式中：$|t|$表示序列 t 的长度；$\mathbf{N}$ 表示自然数的集合.

定理 1　对于给定的有故障的离散事件系统 H，如果满足以下条件：1) 系统到达 $Q_{\mathrm{r},i}$之前可诊断；2) 由故障模式初始状态到可修复状态的下一状态组成的事件序列 $s_j(j=1,2,\cdots,m)$，其可观事件序列 $P_i(s_j)$均不是不可区分串，那么，系统对于故障 f_i 具有一次可修复性.

证明　假设给定系统故障可诊断，故障 f_i 发生后，系统会进入故障模式 G_i，即

$$(\forall s\in L_i)(\forall t\in\Sigma_i^{*})(\exists n\in\mathbf{N})\mid t\mid>n\wedge\delta_{\mathrm{exd}}(q_0,st)!\Rightarrow\delta_{\mathrm{exd}}(q_0,P(st))\in Q_i.$$

假设系统经过事件序列 s 刚好进入故障模式，即 $s=hf_i$，G_i 状态到修复状态的下一状态的事件序列 $t'(\exists t'\in\mathrm{Pr}(r))$不经过任一环，如果 $P_i(t')$不是不可区分串，即 $L_{\mathrm{ind}}^{i}(t')=\emptyset$，那么，$P_i(t')=t'$，$t'$完全可观，$\mathrm{SE}(P_i(t'))$为 $Q_{\mathrm{r},i}$中可修复状态的下一状态，$|\mathrm{SE}(P_i(t'))|=1$，此时，状态唯一确定.

如果 $P_i(t')$不是不可区分串，$t''(t'=t''\sigma)$必定也不是不可区分串，即 $L_{\mathrm{ind}}^{i}(t'')=\emptyset$，有 $P_i(t'')=t''$，故障后经过 t''系统到达 $Q_{\mathrm{r},i}$，$|\mathrm{SE}(P_i(t''))|=1$，状态唯一确定. 因此，可以断定系统会到达可修复状态.

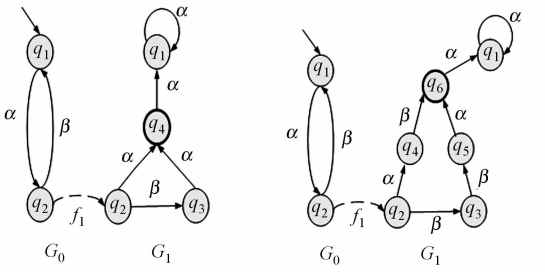
由于假设 st'不经过任一环且环中不包含 $Q_{\mathrm{r},i}$中的状态，系统有且仅有一次机会触发修复行为，满足

$$(\forall s\in L_i)(\forall t\in\Sigma_i^{*})(\exists n\in\mathbf{N})\mid t\mid>n\wedge\delta_{\mathrm{exd}}(q_0,st)!\Rightarrow$$
$$(\exists s=hf_i)(\exists t'\in\mathrm{Pr}(t))(\exists L_{\mathrm{ind}}^{i}(t')=\emptyset)R_i(\delta_{\mathrm{exd}}(q_0,st'))=1\Rightarrow$$
$$(\exists s''\in L_i)\mathrm{SE}(s'')\subseteq Q_{\mathrm{r},i}.$$

此时，系统对于故障 f_i 具有一次可修复性. 证毕.

系统进入故障模式后，到达可修复状态的事件序列可能不止一组，且其中某些序列是不可区分串.

故障的离散事件系统,如图2所示.图2(a)中:系统存在故障 f_1 和修复行为 r_1,且在状态 $q_{4,1}$ 可触发,$q_{1,0}$ 为初始状态.当事件和故障均可观测时,故障模式初始状态到可修复状态下一状态的2组事件序列可区分.由定理1可知:系统具有一次可修复性.假设事件 β 不可观,故障 f_1 后存在 $P(\beta\alpha)=P(\alpha)$,即有不可区分串,$\mathrm{SE}(\alpha f_1\alpha)=\{q_{4,1}\}$,系统仍然具有一次可修复性. 图2(b)中:系统存在故障 f_1 和可修复状态 $q_{6,1}$,初始状态是 $q_{1,0}$.当事件和故障均可观时,系统具有一次可修复性.假设事件 β 不可观时,故障 f_1 后有 $P(\alpha\beta)=P(\beta\beta\alpha)=\alpha$,即存在不可区分串,当前状态估计为 $\mathrm{SE}(\alpha f_1\alpha)=\{q_{4,1},q_{6,1}\}$,故系统不具有一次可修复性.



(a) 系统3 (b) 系统4

图2 含多支路的故障的离散事件系统

Fig. 2 Faulty discrete event systems with multiple branches

定理2 对于给定有故障的离散事件系统 H,如果满足以下条件:1) 系统到达 $Q_{r,i}$ 之前可诊断;2) 由故障模式初始状态到 $Q_{r,i}$ 前一状态组成的事件序列 $s_j(j=1,2,\cdots,m)$ 的可观事件序列 $P_i(s_j)$ 是不可区分串,且驱使系统进入修复状态再到下一状态的事件均为可观事件.那么,系统对于故障 f_i 具有一次可修复性.

证明 假设给定系统故障可诊断,故障 f_i 发生后,系统会进入故障模式 G_i,即

$$(\forall s\in L_i)(\forall t\in\Sigma_i^*)(\exists n\in\mathbf{N})\mid t\mid>n\wedge\delta_{\mathrm{exd}}(q_0,st)!\Rightarrow$$
$$\delta_{\mathrm{exd}}(q_0,P(st))\subseteq Q_i.$$

假设系统经过事件序列 s 刚好进入故障状态,则有 $s=hf_i$,G_i 初始状态到 $Q_{r,i}$ 前一状态的事件序列 $t'(\exists t'\in\mathrm{Pr}(r))$不经过任一环,如果 $P_i(t')$是不可区分串,即 $L_{\mathrm{ind}}^i(t')=\emptyset$,$t'$部分可观,有 $s'=P_i(t')$.

由于驱使系统进入修复状态再到下一状态的事件均为可观事件,即

$$(\exists\sigma_1\in\Sigma_i)(\exists\sigma_2\in\Sigma_i)P_i(t'\sigma_2)=s'\sigma_1\sigma_2.$$

上式中:t'包含不可观事件;事件 σ_1 使状态转移到 $Q_{r,i}$;事件 σ_2 使系统离开 $Q_{r,i}$ 到达下一状态.

在故障模式下,系统经过 $t'\sigma_1$ 到达 $Q_{r,i}$,$P_i(t'\sigma_1)=s'\sigma_1$,$\sigma_1$ 可观,$\mathrm{SE}(P_i(s'\sigma_1))$是唯一确定的;同理,$P_i(t'\sigma_1\sigma_2)=s'\sigma_1\sigma_2$,$Q_{r,i}$的下一状态也是唯一确定的,因此,可以断定系统会到达可修复状态.

由于假设 st'不经过任一环且环中不包含 $Q_{r,i}$中的状态,系统有且仅有一次机会触发修复行为,满足

$$(\forall s\in L_i)(\forall t\in\Sigma_i^*)(\exists n\in\mathbf{N})\mid t\mid>n\wedge\delta_{\mathrm{exd}}(q_0,st)!\Rightarrow$$
$$(\exists s=hf_i)(\exists t'\in\mathrm{Pr}(t))(\exists L_{\mathrm{ind}}^i(t')=\emptyset)(\exists s'\sigma_1\in L_{\mathrm{ind}}^i(t'\sigma_1))R_i(\delta_{\mathrm{exd}}(q_0,st'))=1\Rightarrow$$
$$(\exists s''\in L_i)\mathrm{SE}(s'')\subseteq Q_{r,i}.$$

此时,系统对于故障 f_i 具有一次可修复性.证毕.

在假设条件不发生变化的前提下,也可对给定有故障的离散事件系统构造可修复性诊断器,具体方法见文献[9-10],G_{exd}的可修复性诊断器模型为

$$G_{\mathrm{rd}}=(X,\Sigma_{0,\mathrm{exd}},\xi,x_0)=Ac(2^{Q_{\mathrm{exd}}},\Sigma_{o,\mathrm{exd}},\xi,\mathrm{UR}(q_0)).\tag{5}$$

诊断器 G_{rd}中能确定故障 f_i 发生的状态标记为 $X_{D,i}=\{x\in X:(\forall q\in x)q\in Q_i\}$,能执行修复行为的状态标记为 $X_{R,i}=\{x\in X:(\forall q\in x)q(q)=1\}$.

定理3 给定有故障的的离散事件系统 H 对于故障 f_i 具有一次可修复性,当且仅当在假设条件下的状态估计是可修复状态或者可修复状态集,即

$$(\exists s\in L_i)\mathrm{SE}(P(s))\subseteq X_{R,i}.$$

证明 假设系统故障可诊断,故障 f_i 发生后系统会进入 G_i,构造可修复性诊断器,即

$$(\forall s\in L_i)(\forall t\in\Sigma_i^*)(\exists n\in N)\mid t\mid>n\wedge\delta_{\mathrm{exd}}(q_0,st)!\Rightarrow$$
$$\xi(x_0,P(st))\subseteq X_{D,i}.$$

在假设条件下系统经事件序列 s 的状态可观测,如果 $\mathrm{SE}(P(s))\subseteq X_{R,i}$,那么,系统满足

$$(\forall s\in L_i)(\forall t\in\Sigma_i^*)(\exists n\in\mathbf{N})\mid t\mid>n\wedge\delta_{\mathrm{exd}}(q_0,st)!\Rightarrow$$
$$\delta_{\mathrm{exd}}(q_0,s)\subseteq Q_{r,i}.$$

此时,系统具有一次可修复性.

在假设条件下，如果系统有一次可修复性，必定存在事件序列 s 使系统到达可修复性状态，即

$$(\exists s \in L_i)\delta_{\mathrm{exd}}(q_0, s) \subseteq Q_{\mathrm{r},i}.$$

建立相应可修复性诊断器，那么，有 $\xi(x_0, P(s)) \subseteq X_{\mathrm{D},i}$.

如果 $\xi(x_0, P(s)) \not\subset X_{\mathrm{R},i}$，系统将无法确定是否到达相应的可修复状态，因此，不具有可修复性，与假设相矛盾. 所以诊断器中必须满足 $(\exists s \in L_i)\mathrm{SE}(P(s)) \subseteq X_{\mathrm{R},i}$. 证毕.

如果给定系统是非确定自动机模型 $G=(Q, \Sigma, \delta, q_0)$，其中，转移关系为 $\delta: Q \times \Sigma \to 2^Q$，将 G_{exd} 中所有不可观事件用空串 ε 替换，再将非确定性自动机转化成确定自动机后，定理 3 仍适用.

4　实例分析

液压系统如图 3 所示. 液压系统由管道将槽 T_1，T_2，泵 P 和阀门 V_1，V_2 连接所组成. 如果要将液体从槽中通过管道导引出来，液体在系统中的流动通过打开/关闭阀门和启动/停止泵实现. 泵、阀门的转移关系，如图 4 所示. 系统事件可定义为：op1，cls1 分别表示打开和关闭 V_1；op2，cls2 分别表示打开和关闭 V_2；start 表示启动泵；stop 表示停止泵，且事件均可观测；p_{s} 表示泵的空闲状态；p_{w} 表示泵的工作状态；$v_{1,\mathrm{c}}$，$v_{1,\mathrm{o}}$ 分别表示 V_1 处于闭合和开启状态；$v_{2,\mathrm{c}}$，$v_{2,\mathrm{o}}$ 分别表示 V_2 处于闭合和开启状态.

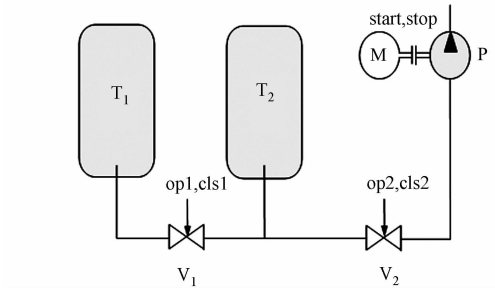


图 3　液压系统

Fig. 3　Hydraulic system

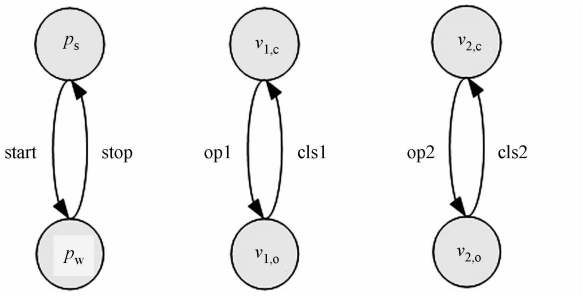


图 4　泵、阀门的状态转移

Fig. 4　State transition of pump and threshold gate

由于考虑到系统的安全性，泵的工作状态和阀门 V_2 的闭合状态是不能同时存在的. 因此，系统正常运行的可达状态及转移关系，如图 5 所示. 假设泵突然卡住作为系统故障事件 f_1，f_1 可观测. 此时，系统将由正常模式 G_0 进入到故障模式 G_1，f_1 的自动机模型，如图 6 所示.

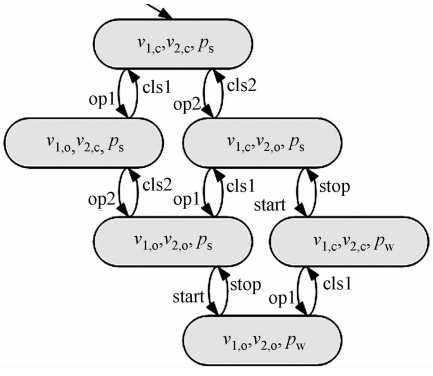


图 5　液压系统正常模式

Fig. 5　Normal mode of the hydraulic system

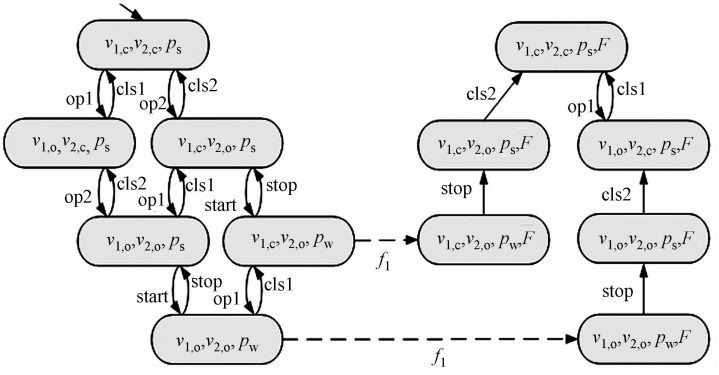


图 6　故障 f_1 的液压系统

Fig. 6　Hydraulic system with fault f_1

假设故障模式下，当停止泵的工作状态即可安全进行修复操作，此时，系统有 4 个可修复状态：$(v_{1,\mathrm{c}}, v_{2,\mathrm{c}}, p_{\mathrm{s}}, F)$，$(v_{1,\mathrm{c}}, v_{2,\mathrm{o}}, p_{\mathrm{s}}, F)$，$(v_{1,\mathrm{o}}, v_{2,\mathrm{c}}, p_{\mathrm{s}}, F)$，$(v_{1,\mathrm{o}}, v_{2,\mathrm{o}}, p_{\mathrm{s}}, F)$. $\mathrm{SE}(f_1\text{-stop}) = \{(v_{1,\mathrm{c}}, v_{2,\mathrm{o}}, p_{\mathrm{s}}, F)(v_{1,\mathrm{o}}, v_{2,\mathrm{o}}, p_{\mathrm{s}}, F)\}$，由故障模式初始状态到可修复状态前不存在不可区分串，当系统在 $(v_{1,\mathrm{c}}, v_{2,\mathrm{o}}, p_{\mathrm{w}})$ 发生故障，有且仅有一次机会进入 $(v_{1,\mathrm{c}}, v_{2,\mathrm{o}}, p_{\mathrm{s}}, F)$；当系统在 $(v_{1,\mathrm{o}}, v_{2,\mathrm{o}}, p_{\mathrm{w}})$ 发生故障，有且仅有一次机会进入 $(v_{1,\mathrm{o}}, v_{2,\mathrm{o}}, p_{\mathrm{s}}, F)$. 因此，系统具有一次可修复性. 同样地，$\mathrm{SE}(f_1\text{-stop-cls2}) = \{(v_{1,\mathrm{c}}, v_{2,\mathrm{c}}, p_{\mathrm{s}}, F)(v_{1,\mathrm{o}}, v_{2,\mathrm{c}}, p_{\mathrm{s}}, F)\}$，系统会进入由 $(v_{1,\mathrm{c}}, v_{2,\mathrm{c}}, p_{\mathrm{s}}, F)$ 和 $(v_{1,\mathrm{o}}, v_{2,\mathrm{c}}, p_{\mathrm{s}}, F)$ 组成的环内. 因此，系统也具有周期可修复性. 构造可修复性诊断器就是故障 f_1 的自动机模型，也可以得到相同结论.

5 结束语

在周期可修复性诊断理论的基础上,提出一次可修复性的概念及判定方法.对于给定有故障的离散事件系统,分别基于不可区分串和可修复性诊断器,研究了系统的故障可修复性诊断问题,并通过一个液压系统进行验证分析.

参考文献:

[1] DENG Guanqian, QIU Jing, LIU Guanjun, *et al*. A discrete event systems approach to discriminating intermittent from permanent faults[J]. Chinese Journal of Aeronautics, 2014, 27(2): 390-396.

[2] 吴旋. 基于离散事件动态系统的故障诊断理论的研究[D]. 杭州:浙江大学, 2002.

[3] SAMPATH M, SENGUPTA R, LAFORTUNE S. *et al*. Diagnosability of discrete-event systems[J]. IEEE Transactions on Automatic Control, 1995, 40(9): 1555-1575. DOI: 10.1109/9.412626.

[4] JIANG Shengbing, HUANG Zhongdong, CHANDRA V, *et al*. A polynomial algorithm for testing diagnosability of discrete-event systems[J]. IEEE Transactions on Automatic Control, 2001, 46(8): 1318-1321. DOI: 10.1109/9.940942.

[5] 郑大钟,郑应平. 离散事件动态系统理论: 现状和展望[J]. 自动化学报, 1992, 18(2): 129-142.

[6] CASSANDRAS C G, LAFORTUNE S. Introduction to discrete event systems[M]. New York: Springer, 1999.

[7] SHU Shaolong, LIN Feng. Fault-tolerant control for safety of discrete-event systems[J]. IEEE Transactions on Automation Science and Engineering, 2014, 11(1): 78-89. DOI: 10.1109/TASE.2013.2264809.

[8] LIN Feng. Diagnosability of discrete event systems and its applications[J]. Discrete Event Dynamic Systems, 1994, 4(2): 197-212.

[9] SHU Shaolong, LIN Feng, YING Hao, *et al*. State estimation and detectability of probabilistic discrete event systems [J]. Automatica the Journal of Ifac the International Federation of Automatic Control, 2008, 44(12): 3054-3060. DOI: 10.1016/j.automatica.2008.05.025.

[10] SHU Shaolong, LIN Feng. Generalized detectability for discrete event systems[J]. Systems and Control Letters, 2011, 60(5): 310-317.

[11] SABOORI A, ZAD S H. Fault recovery in discrete event systems[C]// Proceedings of the ICSC Congress on Computational Intelligence Methods and Applications. Istanbul: IEEE Press, 2005: 1-6. DOI: 10.1109/CIMA.2005.1662332.

[12] QIN Wen, KUMAR R, HUANG Jing, *et al*. A framework for fault-tolerant control of discrete event systems[J]. IEEE Transactions on Automatic Control, 2008, 53(8): 1839-1849.

[13] SHU Shaolong. Recoverability of discrete-event systems with faults[J]. IEEE Transactions on Automation Science and Engineering, 2014, 11(3): 930-935. DOI: 10.1109/TASE.2014.2314331.

[14] SHU Shaolong, ZONG Wenhao. Recoverability of faulty discrete event systems[C]// International Conference on Control Automation Robotics and Vision. Guangzhou: IEEE Press, 2013: 258-263. DOI: 10.1109/ICARCV.2012.6485168.

[15] 莫日翔,刘富春. 离散事件系统的可纠错性研究[J]. 云南大学学报(自然科学版), 2015, 37(2): 187-193. DOI: 10.7540/j.ynu.20140251.

[16] 莫日翔. 经典与随机离散事件系统的可纠错性研究[D]. 广州:广东工业大学, 2015. DOI: 10.7666/d.Y2795796.

(**责任编辑:** 钱筠 **英文审校:** 吴逢铁)