

DISEÑO DE DIAGNOSTICADORES DE FALLOS UTILIZANDO MEDIDAS CONTINUAS

V. Mascarós, E. García, F. Morant, A. Correcher, E. Quiles,
Dpto. de Ingeniería de Sistemas y Automática
Universidad Politécnica de Valencia
Camino de Vera S/N, 46020 Valencia (España)
vimasma@doctor.upv.es, egarciam@isa.upv.es, fmorant@isa.upv.es,
ancorsal@upvnet.upv.es, equiles@isa.upv.es

Resumen

El problema del diagnóstico de fallos se ha tratado desde distintas perspectivas. Dentro del área de los sistemas dinámicos de eventos discretos, una de las propuestas más extendidas es el diagnóstico de fallos basado en modelos de eventos discretos. En dicha propuesta, para realizar las tareas de diagnóstico se utilizan señales de medida que adoptan valores discretos. En este artículo se presenta una metodología de diseño de los diagnosticadores de fallos donde se utilizan señales de medida continuas para desarrollar las tareas de diagnóstico.

Palabras Clave: Diagnóstico de fallos, sistemas de eventos discretos, variables continuas.

1 INTRODUCCIÓN

El problema del diagnóstico de fallos en las plantas industriales se ha tratado desde distintas perspectivas. Dentro del área de los sistemas dinámicos de eventos discretos, una de las propuestas más extendidas es el diagnóstico de fallos basado en modelos de eventos discretos [7], [8]. Una de las ventajas de este método es que no requiere un modelado en profundidad del sistema a diagnosticar. No obstante, pese a su notable interés, cuando aumenta el número de modelos de dispositivos que forman parte del sistema aparece el problema de la explosión combinatorial. Este problema se soluciona mediante la aplicación de la descomposición modular de los diagnosticadores de fallos [3]. Por otro lado, cuando se utilizan distintos diagnosticadores sobre un mismo proceso, puede aparecer el fenómeno del acoplamiento [4]. El problema del diagnóstico de fallos intermitentes basado en modelos de eventos discretos también ha sido estudiado [2].

En todos estos trabajos, para desarrollar las tareas de diagnóstico se utilizan señales de medida de los sensores que toman valores discretos.

Una tendencia relativamente reciente es el desarrollo de técnicas de diagnóstico de fallos en los sistemas híbridos [5], [6], basadas en el formalismo del autómata híbrido [1].

En este artículo se plantea el diseño de los diagnosticadores de fallos basados en modelos de eventos discretos utilizando señales de medida continuas para desarrollar las tareas de diagnóstico. La propuesta presentada se basa en la identificación de la región del espacio de estados alcanzable por el vector de señales de medidas en cada uno de los estados del sistema de eventos discretos a diagnosticar.

A grandes rasgos, la metodología se compone de los siguientes pasos. En primer lugar se obtiene el modelo de eventos discretos del sistema a diagnosticar, incluyendo tanto el funcionamiento normal como el funcionamiento en fallo. A continuación se determinan las señales continuas que se van a utilizar para desarrollar las tareas de diagnóstico on-line. Posteriormente se modifica el modelo de eventos discretos siguiendo unas determinadas especificaciones. Por último, a partir del modelo obtenido se diseña el diagnosticador de fallos, cuyas transiciones dependen de condiciones asociadas al vector de señales de medidas continuas. El diagnosticador es una máquina de estados finitos que se ejecuta de forma concurrente con el sistema a diagnosticar.

El artículo está estructurado de la siguiente forma. En el punto 2 se describen los pasos a seguir para obtener el modelo del sistema para el diagnóstico. A continuación, en el punto 3 se detalla el diseño del diagnosticador de fallos, y en el 4 se trata la diagnosticabilidad, teniendo en cuenta las características del diagnosticador obtenido. En el punto 5 se aplica la metodología propuesta a un sistema de control de temperatura de un horno, del tipo todo-nada. Las principales conclusiones del trabajo realizado se comentan en el punto 6.

2 OBTENCIÓN DEL MODELO PARA EL DIAGNÓSTICO

Sea

$$\tilde{G} = (\tilde{X}, \tilde{\Sigma}, \tilde{\delta}, \tilde{x}_0) \quad (1)$$

el modelo de eventos discretos del sistema a diagnosticar, donde \tilde{X} es el conjunto de estados, $\tilde{\Sigma}$ es el conjunto de eventos, $\tilde{\delta}$ es la función de transición y \tilde{x}_0 es el estado inicial de \tilde{G} . Algunos de los eventos de $\tilde{\Sigma}$ son observables, mientras que otros son inobservables. Normalmente, los eventos observables representan señales de control, mientras que los eventos inobservables representan los eventos de fallo, de forma que

$$\tilde{\Sigma} = \tilde{\Sigma}_{obs} \cup \tilde{\Sigma}_{nobs} \quad (2)$$

Se considera que los posibles fallos que puedan ocurrir en el sistema a diagnosticar no son recuperables. Dado un conjunto de M señales de medida, se identifica el mapa de medidas h_j , $j=1, \dots, M$. Se trata de una correspondencia de \tilde{X} a Y_j , donde Y_j es el conjunto continuo de posibles valores que puede tomar la señal de medida j -ésima. Observar que se trata de una correspondencia de \tilde{X} a Y_j (no de una aplicación), de forma que a cada elemento de \tilde{X} le pueden corresponder distintos elementos de Y_j . La correspondencia h_j es un subconjunto del producto cartesiano $\tilde{X} \times Y_j$.

Asimismo se define

$$Y = \prod_{j=1}^M Y_j \quad (3)$$

de modo que se tiene la correspondencia h entre el conjunto \tilde{X} y el conjunto Y , siendo ésta un subconjunto del producto cartesiano $l \subseteq \tilde{X} \times Y$. La correspondencia l es un conjunto de pares ordenados de la forma (\tilde{x}_i, z_k) , donde $\tilde{x}_i \in \tilde{X}, z_k \in Y$.

Entonces se define $S_{\tilde{x}_i}$ como la región alcanzable por el vector de señales de medida (s_1, s_2, \dots, s_M) en el estado discreto \tilde{x}_i , es decir

$$S_{\tilde{x}_i} = \{z_k \mid (\tilde{x}_i, z_k) \in l\} \quad (4)$$

Para cada estado discreto activo \tilde{x}_i , se cumple $(s_1, s_2, \dots, s_M) \in S_{\tilde{x}_i}$. Finalmente, se transforma $\tilde{G} = (\tilde{X}, \tilde{\Sigma}, \tilde{\delta}, \tilde{x}_0)$ en $G = (X, \Sigma, S, \delta, x_0)$, donde $S = \bigcup_{i=1}^N S_{x_i}$, siendo $N = |\tilde{X}|$. Se cumple la igualdad $x_0 = \tilde{x}_0$. Considérese la transición $\tilde{\delta}(\tilde{x}_i, \sigma) = \tilde{x}_v$, donde $\tilde{x}_i, \tilde{x}_v \in \tilde{X}$ y $\sigma \in \tilde{\Sigma}$, entonces:

- 1) Si σ es observable, $\sigma \in \tilde{\Sigma}_{obs}$, entonces se renombra la transición con la expresión lógica $\sigma \cdot ((s_1, s_2, \dots, s_M) \in S_{\tilde{x}_i})$. Dicha transición se disparará cuando la expresión lógica sea cierta.
- 2) Si σ es inobservable, $\sigma \in \tilde{\Sigma}_{nobs}$, y $S_{\tilde{x}_v} - S_{\tilde{x}_i} = \emptyset$, entonces la transición no varía en G , y el evento σ sigue siendo inobservable en Σ .
- 3) Si σ es inobservable, $\sigma \in \tilde{\Sigma}_{nobs}$, y $S_{\tilde{x}_v} - S_{\tilde{x}_i} \neq \emptyset$, entonces se sustituye la transición $\tilde{\delta}(\tilde{x}_i, \sigma) = \tilde{x}_v$ por las dos transiciones siguientes:
 - a) $\delta(\tilde{x}_i, \sigma) = x_{new}$ y
 - b) se añade una transición del estado x_{new} al estado \tilde{x}_v disparada por la condición lógica $(s_1, s_2, \dots, s_M) \in S_{x_{new} \rightarrow \tilde{x}_v} = S_{\tilde{x}_v} - S_{\tilde{x}_i}$. Se define $S_{x_{new}} = S_{\tilde{x}_v}$.

La primera transición a) es inobservable, mientras que la segunda es observable b). Se cumple $S_{x_{new}} = S_{\tilde{x}_v}$. Se define X_{new} como el conjunto de todos los estados x_{new} introducidos en el paso 3. Entonces

$$X = \tilde{X} \cup X_{new} \quad (5)$$

Se obtiene así el modelo $G = (X, \Sigma, S, \delta, x_0)$, a partir del cuál se diseña el diagnosticador de fallos.

En este modelo se tienen tres tipos de transiciones:

- 1) Tipo 1 (Transiciones inobservables): Transiciones que dependen de un evento inobservable
- 2) Tipo 2 (Transiciones observables): Transiciones que dependen de una expresión lógica que depende a su vez del vector de señales de medidas.
- 3) Tipo 3 (Transiciones observables): Transiciones que dependen de una expresión lógica que depende a su vez del vector de señales de medidas y un evento observable.

El conjunto Σ está formado por eventos observables y eventos inobservables, $\Sigma = \Sigma_{obs} \cup \Sigma_{nobs}$. Se define el conjunto de eventos de fallos a diagnosticar como $\Sigma_f \subseteq \Sigma_{nobs}$. En función del tipo de fallo representado por cada uno de los eventos, el conjunto Σ_f se puede expresar como $\Sigma_f = \Sigma_{f1} \cup \dots \cup \Sigma_{fm}$, donde cada Σ_{fi} contiene aquellos eventos que modelan el fallo i .

3 REGLAS DE DISEÑO DEL DIAGNOSTICADOR DE FALLOS

El diagnosticador es una máquina de estados finitos que se ejecuta de forma concurrente con el sistema a diagnosticar. Realiza una estimación del estado o estados discretos en los que se puede encontrar el sistema, utilizando para ello el vector de señales de medida y la observación de los eventos observables. La etiqueta que lleva asociada cada estado informa sobre la posible ocurrencia de una secuencia de fallos.

A partir del modelo G del sistema a diagnosticar se obtiene el diagnosticador de fallos del sistema, representado por G_d . Cada estado q_d del diagnosticador G_d tiene la forma $q_d = \{(x_1, l_1), \dots, (x_n, l_n)\}$, donde $x_i \in X$ y l_i es una etiqueta de la forma

$$l_i = \{N\} \quad \text{o} \quad l_i = \{F_{i_1}, F_{i_2}, \dots, F_{i_k}\} \quad (6)$$

donde $\{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, m\}$, siendo m el número de fallos posibles. Las etiquetas transportan la estimación del estado y los fallos se diagnostican mediante la comprobación de dichas etiquetas.

Se supone que inicialmente el estado del diagnosticador es $(x_0, \{N\})$. Considerando que el estado actual del diagnosticador es q_1 , el estado siguiente del diagnosticador q_2 se obtiene siguiendo los pasos:

1) Determinación de los alcances a través de transiciones tipo 3: para cada estado x_r en q_1 , determinar los estados de X que se alcanzan cuando ocurre un evento $\sigma \in \tilde{\Sigma}_{obs}$ para cada uno de los puntos del espacio de medidas S (transiciones tipo 3), y teniendo en cuenta los posibles eventos inobservables que pueden preceder a σ (es decir, transiciones del tipo 1).

2) Determinación de los alcances a través de transiciones tipo 2: dada una transición tipo 2 (figura 1), el estado x_s se alcanza desde el estado x_r mediante la condición

$$(s_1, s_2, \dots, s_M) \in S_{x_r \rightarrow x_s} \quad (7)$$

Dada una transición tipo 2 precedida de transiciones inobservables tipo 1 (figura 2), el estado x_s se alcanza desde el estado x_r mediante la condición

$$(s_1, s_2, \dots, s_M) \in \left(S_{x_N \rightarrow x_s} - \left(S_{x_r} \cup \bigcup_{l=1}^{N-1} S_{x_l} \right) \right) \quad (8)$$

Si $\left(S_{x_N \rightarrow x_s} - \left(S_{x_r} \cup \bigcup_{l=1}^{N-1} S_{x_l} \right) \right) = \emptyset$ entonces no es posible observar el paso del estado x_r al estado x_s .

A partir de las condiciones de alcance obtenidas en 2), se determinan los estados de X que se alcanzan desde x_r , para cada uno de los puntos del espacio de medidas S .

3) Sea $(x_r, l) \in q_1$, y sea $(x_s, l') \in q_2$, la etiqueta l se propaga a la etiqueta l' se acuerdo con las siguientes especificaciones:

- Si $l = \{N\}$ y x_s se alcanza desde x_r sin que ocurran eventos de fallo, entonces $l' = \{N\}$.
- Si $l = \{N\}$ y x_s se alcanza desde x_r a través de la ocurrencia de eventos de fallo de los conjuntos $\Sigma_{fi}, \Sigma_{fj}, \dots$ entonces $l' = \{F_i, F_j, \dots\}$.
- Si $l = \{F_i, F_j, \dots\}$ y x_s se alcanza desde x_r a través de la ocurrencia de eventos de fallo de los conjuntos $\Sigma_{fk}, \Sigma_{fp}, \dots$ entonces $l' = \{F_i, F_j, \dots, F_k, F_p, \dots\}$.

Sea $(x_r, l) \in q_1$, donde x_r es un estado discreto que no tiene transiciones de salida. Dada una transición en el diagnosticador del estado q_1 al estado q_2 de la forma $\sigma \cdot ((s_1, s_2, \dots, s_M) \in St)$ o $(s_1, s_2, \dots, s_M) \in St$, si $St \cap S_{x_r} \neq \emptyset$ se debe cumplir $(x_r, l) \in q_2$.

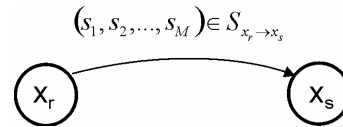


Figura 1: Transición observable tipo 2.

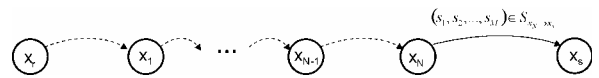


Figura 2: Transición observable tipo 2 precedida de transiciones inobservables.

4 DIAGNOSTICABILIDAD

En términos generales, un sistema es diagnosticable si es posible detectar con un retardo finito la ocurrencia de los posibles fallos, utilizando el registro de eventos y de medidas observados. Es posible determinar la diagnosticabilidad de un sistema mediante el análisis del diagnosticador de fallos obtenido. En [7] se define el concepto de estado F_i -cierto y estado F_i -incierto, de la siguiente forma:

- Un estado q_d del diagnosticador G_d se denomina F_i -cierto si $\forall(x,l) \in q_d$, se cumple $F_i \in l$. Si en la ejecución del diagnosticador se accede a un estado de este tipo, se tiene la certeza de que ha ocurrido el fallo F_i .
- Un estado q_d del diagnosticador G_d se denomina F_i -incierto si $\exists(x,l),(y,l') \in q_d$, se cumple $F_i \in l$ y $F_i \notin l'$. Si en la ejecución del diagnosticador se accede a un estado de este tipo, es posible que haya ocurrido el fallo F_i , pero no se sabe con certeza.

A partir de estas definiciones, es posible definir el concepto de F_i -diagnosticabilidad de la siguiente forma. Un sistema es F_i -diagnosticable si el diagnosticador de fallos G_d obtenido contiene al menos un estado q_d F_i -cierto. Es decir, $\exists q_d$ tal que $\forall(x,l) \in q_d$ se cumple $F_i \in l$. Asimismo, considérese un sistema donde pueden ocurrir m fallos diferentes F_i , $i=1,2,\dots,m$. Dicho sistema se puede considerar diagnosticable si $\forall i, i=1,2,\dots,m$ el sistema es F_i -diagnosticable.

5 APLICACIÓN: SISTEMA DE CONTROL DE TEMPERATURA

Considérese un sistema de control de temperatura del tipo todo-nada, basado en un comparador con histéresis, donde se desea mantener la temperatura de un horno entre un límite superior M y un límite inferior m .

Los cambios en la acción de control se representan mediante los eventos observables emitidos por el controlador (ON, OFF). Se supone que en dicho sistema pueden ocurrir los siguientes fallos:

- F1: fallo en el actuador. El horno deja de recibir energía a pesar de las órdenes de control. Evento asociado: FA

- F2: desviación positiva del límite M . Evento asociado: M+
- F3: rotura del horno por sobrecalentamiento. Evento asociado: RH
- F4: desviación positiva del límite m . Evento asociado: m-
- F5: desviación negativa del límite m . Evento asociado: m+

En la figura 3 se muestra el modelo de eventos discretos $\tilde{G} = (\tilde{X}, \tilde{\Sigma}, \tilde{\delta}, \tilde{x}_0)$ del sistema a diagnosticar.

Este modelo contempla tanto los estados de funcionamiento normal como los estados de fallo. Mediante líneas discontinuas se identifican las transiciones inobservables. En la tabla 1 se describe la situación del sistema en cada uno de los estados discretos definidos.

A partir del modelo \tilde{G} se obtiene el modelo G . Se considera que únicamente se mide la temperatura del horno para realizar las tareas de diagnóstico. La región alcanzable por la señal de medida en cada uno de los estados se describe en la tabla 1.

El modelo G obtenido siguiendo los pasos especificados en el punto 2 se detalla en la figura 4. Debido a los cambios de la región alcanzable por la señal de medida de la temperatura entre estados, algunas de las transiciones que eran inobservables en el modelo \tilde{G} son observables en el modelo G mediante la inserción de estados x_{new} . Sin embargo, las transiciones de fallo asociadas con el evento inobservable $m+$ siguen siendo inobservables.

Partiendo del modelo G , y siguiendo los pasos de diseño propuestos en el punto 2 se obtiene el diagnosticador de fallos de la figura 5. El diagnosticador se ejecuta de forma concurrente con el sistema a diagnosticar y realiza una estimación del estado discreto del sistema a partir de la medida de la temperatura y la observación de los eventos observables. Se puede comprobar que el fallo F4 no se puede detectar con certeza, ya que los estados del diagnosticador que contienen dicha etiqueta siempre van asociados con estados de funcionamiento normal. En estos casos hay una incertidumbre.

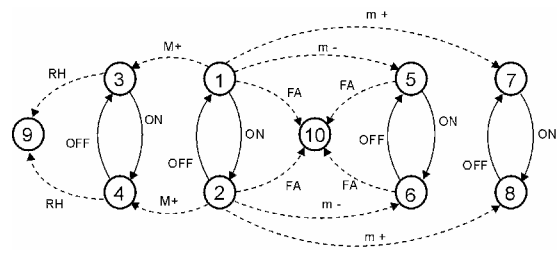


Figura 3: Modelo $\tilde{G} = (\tilde{X}, \tilde{\Sigma}, \tilde{\delta}, \tilde{x}_0)$ del sistema de control de temperatura.

Lo mismo ocurre con el fallo F5. Se trata de un sistema F_1 -diagnosticable, F_2 -diagnosticable y F_3 -diagnosticable, ya que posee estados F_1 -ciertos, F_2 -ciertos y F_3 -ciertos. Sin embargo, este sistema no es diagnosticable ya que no posee estados F_4 -ciertos y

F_5 -ciertos. En el caso de no ser válido este diagnosticador por no detectar con certeza estos fallos, se debe volver a aplicar la metodología propuesta considerando un nuevo vector de señales de medidas.

Tabla 1: Estados discretos del modelo y regiones alcanzables por la señal de medida de temperatura

Situación	Estado	Regiones s_x
Horno enfriándose en funcionamiento normal	1	$S_1 = \{x \mid x \in [m, M]\}$
Horno calentándose en funcionamiento normal	2	$S_2 = \{x \mid x \in [m, M]\}$
Horno enfriándose con desviación positiva de M	3	$S_3 = \{x \mid x \in [m, M + DM]\}$
Horno calentándose con desviación positiva de M	4	$S_4 = \{x \mid x \in [m, M + DM]\}$
Horno enfriándose con desviación negativa de m	5	$S_5 = \{x \mid x \in [m - dn, M]\}$
Horno calentándose con desviación negativa de m	6	$S_6 = \{x \mid x \in [m - dn, M]\}$
Horno enfriándose con desviación positiva de m	7	$S_7 = \{x \mid x \in [m, M]\}$
Horno calentándose con desviación positiva de m	8	$S_8 = \{x \mid x \in [m, M]\}$
Rotura del horno por sobrecalentamiento	9	$S_9 = \{x \mid x \in [0, M + DM]\}$
Fallo del actuador	10	$S_{10} = \{x \mid x \in [0, M]\}$

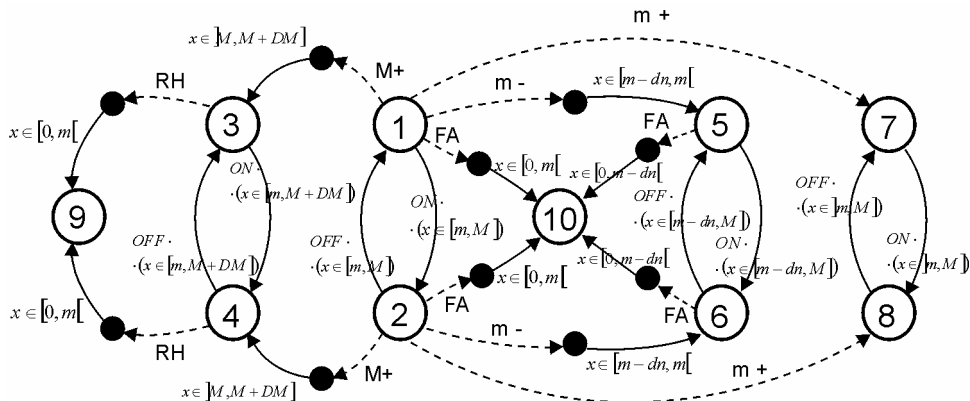


Figura 4: Modelo $G = (X, \Sigma, S, \delta, x_0)$ del sistema de control de temperatura.

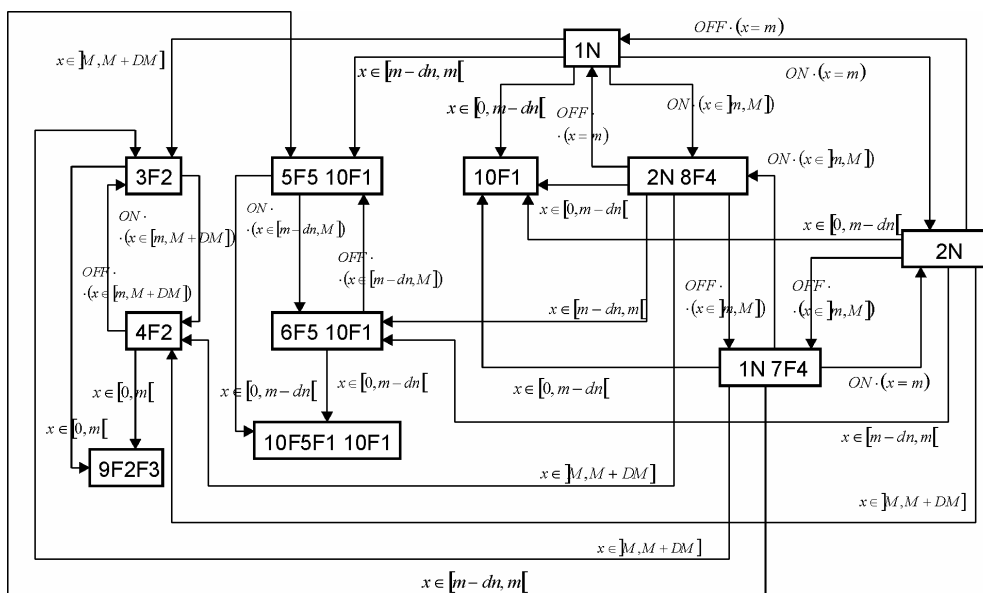


Figura 5: Diagnosticador de fallos

6 CONCLUSIONES

En los trabajos precedentes relativos al diseño de diagnosticadores de fallos basados en modelos de eventos discretos, para realizar las tareas de diagnóstico se utilizan medidas del sistema a diagnosticar que toman valores discretos. En este artículo se ha presentado una propuesta que se encuentra a medio camino entre los sistemas de eventos discretos y los sistemas híbridos. Se propone una metodología para el diseño de diagnosticadores de fallos utilizando señales de medida que toman valores continuos, que se basa en la identificación de la región del espacio de estados alcanzable por el vector de señales de medidas continuas en cada uno de los estados del sistema de eventos discretos a diagnosticar.

El diseño del diagnosticador se realiza analizando dicha información, y teniendo en cuenta que distintos estados discretos pueden tener asociadas regiones no disjuntas. Mediante una aplicación particular se ha comprobado la validez de la metodología presentada.

El diseño de diagnosticadores de fallos utilizando medidas discretas se puede considerar como un caso particular del diseño de diagnosticadores utilizando medidas continuas. También cabe la posibilidad de aplicar esta metodología para sistemas modelados mediante el autómata híbrido, con la condición de que las transiciones entre los estados discretos dependan únicamente de eventos discretos. Asimismo, también es posible obtener el modelo discreto del sistema a diagnosticar a partir de los modelos de eventos discretos de cada uno de los subsistemas que lo componen mediante el operador de composición síncrona.

Agradecimientos

Este trabajo ha sido financiado por el Programa Nacional de Diseño y Producción Industrial (Plan Nacional de I+D+I), DPI2003-03691.

Referencias

- [1] Alur, R., T. A. Henzinger, G. Lafferriere y G. P. Pappas (2000). Discrete abstraction of hybrid systems. In: *Proc. of the IEEE*, vol. 88, no. 7, pp. 971-984.
- [2] Correcher, A., E. García, F. Morant, R. Blasco, E. Quiles y V. Mascarós (2002). Diagnóstico de fallos intermitentes basado en modelos de eventos discretos. *XXIII Jornadas de Automática*, Sta. Cruz de Tenerife (España).
- [3] García, E. (2000). Descomposición modular de diagnosticadores de fallos basados en modelos de eventos discretos. Tesis doctoral. Universidad Politécnica de Valencia.
- [4] García, E., F. Morant, E. Quiles, R. Blasco, A. Correcher (2002). Centralized modular diagnosis and the phenomenon of coupling. *Workshop On Discrete Event Systems WODES'02*, Zaragoza (España).
- [5] Koutsoukos, X., F. Zhao, H. Haussecker, J. Reich, P. Cheung (2001). Fault Modeling for Monitoring and Diagnosis of Sensor-Rich Hybrid Systems. *Proceedings of the 40th IEEE Conference on Decision and Control*, pp. 793-801, Orlando.
- [6] McIlraith, S., G. Biswas, D. Clancy y V. Gupta (2000). Hybrid Systems Diagnosis. *Proceedings of Hybrid Systems: Computation and Control*, Lecture Notes in Computer Science, Springer-Verlag, pp. 282-295.
- [7] Sampath, M., R. Sengupta, S. Lafortune, K. Sinnamohidee and D. Teneketzis (1995). Diagnosability of discrete event systems. *IEEE Trans. on Automat. Control*, vol. 40, no. 9, pp. 1555-1575.
- [8] Sampath, M., R. Sengupta, S. Lafortune, K. Sinnamohidee and D. Teneketzis (1996). Failure diagnosis using discrete event models. *IEEE Trans. on Control Systems*, vol. 4, no. 2, pp. 105-124.