ScienceDirect
Disponible en www.sciencedirect.com
Revista Iberoamericana de Automática e Informática industrial 11 (2014) 191–201
www.elsevier.es/RIAI

Diagnóstico de Sistemas de Eventos Discretos Controlados: Un Enfoque Basado en Crónicas y Análisis Modular Usando Modelos de Autómatas

Olga González-Miranda[a], Mariela Cerrada-Lozada[b,*]

[a] *Postgrado en Ingeniería de Control y Automatización, Facultad de Ingeniería, Universidad de Los Andes, Mérida, Venezuela.*
[b] *Departamento de Sistemas de Control, CEMISID, Facultad de Ingeniería, Universidad de Los Andes, Mérida, Venezuela.*

Resumen

Debido a la complejidad de los procesos industriales, se necesitan diagnosticadores más sencillos y eficientes con reducción en las dimensiones de sus modelos. El diagnóstico modular ha mostrado ser eficiente en la reducción de la complejidad asociada a los sistemas de eventos discretos. Este trabajo propone un enfoque de diagnóstico basado en crónicas y análisis modular temporizado. Cada falla se asocia a un conjunto de crónicas, y cada crónica reconoce una firma de la falla, la cual es obtenida a partir de diagnosticadores de estado, modelados con autómatas de estado finito, y definidos para cada módulo del proceso. De esta manera se crea una base de crónicas modulares que luego son manipuladas a través de un protocolo de coordinación que se ejecuta en línea. El desempeño de este enfoque ha sido probado en un caso de estudio industrial relativo a una clase de sistema hidráulico, obteniendo resultados adecuados.

Palabras Clave:
Sistemas de eventos discretos, diagnóstico de fallas, diagnosticabilidad, crónicas, diagnóstico modular, firmas de falla.

1. Introducción

Los procesos de producción altamente automatizados pueden considerarse como sistemas de alta dimensión en cuanto a la cantidad de variables tratadas, y de alto nivel de dependencia o interconexión entre sus componentes. Este tipo de sistemas ha generado un reto importante para el tratamiento de los sistemas de ingeniería, por cuanto pueden dar lugar a una descomposición en subsistemas que, desde la perspectiva del control, tienen que considerar la comunicación entre los sensores, los actuadores y los controladores con sus subsistemas vecinos, Jamshidi (2010). En el caso de los sistemas de manufactura, donde pueden existir dinámicas determinadas por eventos discretos, si se utilizan autómatas como formalismo de modelado, las dimensiones de tales modelos pueden resultar intratables para su análisis en tiempo real, particularmente cuando se trata de detectar y diagnosticar fallas en actuadores y sensores.

Debido a la complejidad en la construcción de diagnosticadores centralizados basados en autómatas de estado finito, como el propuesto en Sampath et al. (1996), para sistemas de eventos discretos, se han desarrollado enfoques modulares que son computacionalmente tratables para el análisis de las propiedades de diagnosticabilidad de los sistemas, como los discutidos en Debouk et al. (2000) y Wang et al. (2007). En estos enfoques se construyen múltiples diagnosticadores locales, uno para cada subsistema considerado. Los enfoques modulares se han centrado principalmente en el problema de coordinación entre los diagnosticadores locales, proponiendo protocolos de coordinación para explotar la información diagnóstica que éstos proveen. En Contant et al. (2006) se revisan diferentes aspectos del enfoque modular tales como la arquitectura clásica, las condiciones y propiedades de la diagnosticabilidad modular, así como algoritmos para su comprobación.

Las hipótesis teóricas sobre las condiciones de diagnosticabilidad supuestas en Sampath et al. (1996) no siempre se cumplen en sistemas industriales reales, donde se necesita un análisis de diagnóstico que considere aspectos temporales. En Ferrarini et al. (2008) se presenta un enfoque pragmático de diagnóstico de fallas en un caso real de aplicación, donde las hipótesis teóricas supuestas en Sampath et al. (1996) no se cumplen. Este enfoque se basa en el uso de estados transitorios y análisis temporizado, en los modelos de autómatas, que permiten obtener información diagnóstica útil para los operadores, sin requerir de un modelo temporal explícito. En Cerrada et al. (2010) se propone una descomposición modular simple, donde cada módulo es visto como un subsistema controlado, se diseñan diagnosticadores locales para cada módulo y el diagnóstico se realiza por medio de reglas de coordinación que combinan

*Autor en correspondencia
Correos electrónicos: ogonzalez@ula.ve (Olga González-Miranda), cerradam@ula.ve (Mariela Cerrada-Lozada)

http://dx.doi.org/10.1016/j.riai.2014.02.003

la información de cada diagnosticador local, usando un análisis temporizado como el propuesto en Ferrarini et al. (2008).

Por otro lado, un formalismo usado para la monitorización en línea, especialmente por la comunidad de inteligencia artificial, es el formalismo de crónicas. Una crónica es un conjunto de eventos con algunas restricciones temporales entre sus tiempos de ocurrencia, que describe una situación a identificar en el contexto de diagnóstico, Dousson et al. (1993). En este enfoque, cada falla está usualmente asociada a un conjunto de crónicas, y cada crónica reconoce una firma (*signature*) de la falla. La firma de una falla es la asociación de la falla con una secuencia de eventos observables. Un enfoque de monitorización basado en crónicas es presentado en Cordier et al. (2007a), para el diagnósico de fallas en servicios web. El enfoque determina si una falla ha ocurrido o no, en la ejecución de un flujo de trabajo, a través del reconocimiento de crónicas predefinidas. En Pencolé y Subias (2009) se da una definición de las propiedades de diagnosticabilidad que establecen el desempeño del algoritmo basado en crónicas presentado en Cordier et al. (2007a).

El protocolo de coordinación presentado en Cerrada et al. (2010) realiza un análisis en línea de la información proveniente de diagnosticadores locales, lo que requiere de tiempo para lograr una conclusión útil en tiempo real, particularmente cuando el interés es detectar fallas en actuadores y sensores. Esta limitación ha motivado a los autores a extender dicha propuesta con el uso de crónicas para la monitorización en tiempo real.

En este trabajo se propone un enfoque de diagnóstico basado en el reconocimiento de crónicas asociadas a módulos del sistema bajo estudio, introduciendo el concepto de *crónica modular*; los modelos de las crónicas modulares están asociados a firmas de falla, las cuales son obtenidas a partir de los diagnosticadores locales generados con modelos de autómatas de estado finito. Las instancias de estos modelos de crónicas, esto es, la *base de crónicas*, se obtiene a partir de las características temporales de dichos autómatas diagnosticadores. Se propone un protocolo de coordinación que manipula las crónicas modulares para obtener el diagnóstico global.

El enfoque propuesto es aplicado a un subsistema electrohidráulico, que forma parte de un caso real de un sistema de manufactura, donde el interés es detectar y diagnosticar fallas en sus sensores y actuadores. Este tipo de sistema de eventos discretos es bastante común en procesos industriales donde, generalmente, los sensores y actuadores pueden modelarse como componentes de estado binario.

Este trabajo esta organizado como sigue. En la sección 1 se presenta una revisión de las referencias que han motivado este trabajo. En la sección 2 se revisan los fundamentos teóricos que sirven de base para la propuesta aquí desarrollada. Las secciones 3, 4 y 5 presentan las contribuciones de este trabajo, esto es, la obtención de conjuntos abarcadores de fallas, la obtención de crónicas para conjuntos abarcadores y el sistema de diagnóstico modular con el protocolo de coordinación propuesto, todo ello usando modelos formales basados en autómatas de estado finito. Finalmente, se presenta el caso de estudio en la sección 6 y las conclusiones en la sección 7.

2. Preliminares

Esta sección presenta los conceptos teóricos fundamentales asociados a la propuesta de este trabajo. Los detalles sobre estos fundamentos ya han sido tratados en Cordier et al. (2007b), Pencolé y Subias (2009), Ferrarini et al. (2008) y Cerrada et al. (2010).

2.1. Macrofallas y Conjunto Abarcador

El conjunto de las posibles fallas de un sistema está compuesto por n fallas básicas, $\mathcal{F} = \{f_1, \ldots, f_n\}$, y $f_0 = \{normal\}$ denota la ausencia de cualquier falla de $\mathcal{F}$, Cordier et al. (2007b).

En Pucel et al. (2008), la definición de diagnosticabilidad está basada en el concepto de *macrofalla*, que no es más que un conjunto de fallas básicas. Basado en la idea de que no todos los pares de fallas necesitan ser discriminables, las fallas que no necesitan ser discriminadas una de otra, son unidas en una macrofalla.

Definición 2.1. *Una* macrofalla F_j *es un conjunto de fallas,* $F_j \subseteq \mathcal{F}$*, con* $F_j \neq \emptyset$*. Si* F_j *está presente en el sistema, significa que una de las fallas básicas* $f_i \in F_j$ *está presente en el sistema.*

En este enfoque sólo se consideran *conjuntos abarcadores* de macrofallas, es decir, conjuntos de macrofallas, donde cada falla pertenece a una macrofalla. En consecuencia, siempre hay por lo menos una macrofalla presente, cualquiera que sea el estado del sistema.

Definición 2.2. *Un conjunto de macrofallas* $E(\mathcal{F})$ *es un conjunto abarcador de* $\mathcal{F}$ *si y sólo si* $\forall f_i \in \mathcal{F}$, $\exists F_j \in E(\mathcal{F})$ *tal que* $f_i \in F_j$.

El lenguaje L_{f_i} de la falla básica f_i, es el sub-lenguaje del sistema que contiene todas las secuencias en las cuales se encuentra f_i. Dentro de las palabras de L_{f_i} nos interesan aquellas que se observan en un tiempo arbitrariamente largo, ésto es, las que terminan en un ciclo infinito, las cuales se definen como palabras maximales, y forman el lenguaje maximal de la falla $L_{f_i}^{max}$.

Consideremos ahora la *firma* de una falla. Sea r una secuencia de eventos, las observaciones del sistema, OBS, son el conjunto de todas las secuencias $r_{OBS} = P_{OBS}(r)$, donde P_{OBS} es el operador de proyección sobre los eventos observables, Pencolé y Subias (2009).

Definición 2.3. *La firma elemental de una falla básica* $Sig(f_i)$ *es la proyección de* $L_{f_i}^{max}$ *sobre el conjunto de eventos observables:*

$$Sig(f_i) = P_{OBS}(L_{f_i}^{max}) \subseteq OBS$$

La observación de una firma elemental σ denota que la macrofalla F_j puede estar presente en el sistema. La presencia de F_j no es cierta, dado que es posible que σ sea también la firma elemental de otra macrofalla $F_{j'}$, Cordier et al. (2007b).

La observación de una firma σ que caracteriza a F_j, asegura que una de las $f_i \in F_j$ ha ocurrido, y otra $f_k \notin F_j$ no ha ocurrido. Luego, una firma característica de F_j se define de la siguiente manera:

Definición 2.4. *Una firma característica de una macrofalla $cSig(F_j)$ es un conjunto de observaciones que permite asegurarse con certeza de que la macrofalla F_j está presente:*

$$cSig(F_j) \subseteq \left(\bigcup_{f_i \in F_j} (Sig(f_i)) \setminus \bigcup_{f_k \notin F_j} (Sig(f_k)) \right)$$

Clásicamente, la diagnosticabilidad está formalmente definida sobre una partición de las fallas básicas del sistema, Sampath et al. (1996). En Cordier et al. (2007b) se plantea una extensión de la definición de diagnosticabilidad a un conjunto abarcador de macrofallas $E(\mathcal{F}) = \{F_1, \ldots, F_m\}$.

Definición 2.5. *Un conjunto abarcador de macrofallas $E(\mathcal{F})$ es diagnosticable si y sólo si, existe un conjunto de firmas características para estas macrofallas que forman una partición de OBS^{max}. Es decir:*

1. $\bigcup_{i=1}^{m} cSig(F_i) = OBS^{max}$;
2. $\forall i, j, i \neq j, cSig(F_i) \cap cSig(F_j) = \emptyset$.

2.2. Crónicas

En este trabajo se utiliza el formalismo de crónicas propuesto por Dousson (ver Dousson et al. (1993)), cuyas definiciones básicas de Evento y Crónica se presentan en esta sección. En este formalismo, ?*var* significa que *var* es una variable.

Evento. Un *evento* es un par $(E, ?t)$, donde E es un tipo de evento y $?t$ es el tiempo de ocurrencia del evento. Una *instancia de un evento* es un evento, cuyas variables y tiempo han sido instanciados.

Crónica. Un *modelo de crónica* c es un par $(\mathcal{S}, \mathcal{T})$ donde $\mathcal{S}$ es un conjunto de eventos y $\mathcal{T}$ un conjunto de restricciones temporales entre ellos.

Un modelo de crónica $c = (\mathcal{S}, \mathcal{T})$ es reconocido en una secuencia σ si:

1. Existe para todo evento $(e_i, ?t_i) \in \mathcal{S} = \{(e_1, ?t_1), \ldots, (e_n, ?t_n)\}$, una instancia de evento (e_i, t'_i) en σ;
2. Las restricciones $\{?t_1 = t'_1, \ldots, ?t_n = t'_n\} \cup \mathcal{T}$ se satisfacen.

Una crónica es instanciada cuando se instancian todos y cada uno de sus eventos y se cumplen las restricciones de $\mathcal{T}$, Pencolé y Subias (2009).

El *lenguaje de reconocimiento* $L(c, OBS)$ de una crónica es el conjunto de observaciones $\sigma \in OBS$ tal que el modelo de crónica c es reconocido en la secuencia observable σ. Un modelo de crónica asociado a una falla se denota $c(f)$, la cual caracteriza a f si y sólo si $L(c(f), OBS) \subseteq cSig(f) \subseteq Sig(f)$. Si $c(f)$ caracteriza a f, significa que la ocurrencia de f es cierta, Pencolé y Subias (2009).

Finalmente, sea $L \subseteq OBS$ un conjunto de observaciones, una crónica c cubre a L si y sólo si $L \subseteq L(c, OBS)$. Un conjunto de crónicas $c_1, \ldots, c_n$ cubre a L si y sólo si $L \subseteq \bigcup_{i=1}^{n} L(c_i, OBS)$. Sea f una falla, un conjunto de crónicas $c_1, \ldots, c_n$ cubre a f si y sólo si cubre a $Sig(f)$. Una vez que un conjunto de crónicas cubre una falla f, sabemos que si la falla f ocurre, una de las crónicas $c_1, \ldots, c_n$ será reconocida.

Propiedad 2.1. *Sea f una falla en un flujo de eventos del sistema de eventos discretos S, si existe un conjunto de crónicas $C(f) = \{c_1(f), \ldots, c_n(f)\}$ tal que:*

1. *$C(f)$ cubre a f;*
2. *$\forall j \in \{1, \ldots, n\}$, $c_j(f)$ caracteriza a f;*

entonces f es diagnosticable en el flujo de eventos del sistema S, Pencolé y Subias (2009).

2.3. Estado transitorio y análisis temporizado

El enfoque de diagnóstico de fallas en Ferrarini et al. (2008) considera el comportamiento dinámico entre los eventos (relaciones de causa-efecto) mediante la introducción de estados transitorios en el modelo de autómata del proceso. El estado transitorio modela la dinámica asociada con la transición física de los componentes del sistema (sensores y actuadores) y evita la construcción de un modelo de tiempo explícito. El principal aporte de este enfoque de modelado es que permite introducir el concepto de *timeout* y *estado de equilibrio*, con el fin de mejorar la ambigüedad y la incertidumbre en el análisis de diagnóstico cuando las propiedades clásicas de diagnosticabilidad no se cumplen, permitiendo extraer más información de un sistema no diagnosticable.

2.3.1. Estado transitorio

Sean dos estados x_1 y x_2 relacionados por un evento-causa σ, generando un evento-efecto físico explícito. Un estado transitorio entre x_1 y x_2 es definido por un nuevo estado $x_t \in X$ y nuevo evento $\varepsilon_t \in (\Sigma_{uc} \cup \Sigma_{uo})$, tal que $\delta(x_t, \varepsilon_t) = x_2$ y $\delta(x_1, \sigma) = x_t$, ésto es:

$$\begin{aligned} X_t \quad = \quad & \{x \subset X / \forall x \in X_t \exists \varepsilon_t \in (\Sigma_{uc} \cup \Sigma_{uo}) : \\ & \delta(x, \varepsilon_t) \quad \text{está definido}\} \end{aligned} \tag{1}$$

En la Fig. 1 se ilustra el modelo de un estado transitorio, el cual sigue estableciendo una relación causal, debido a la ocurrencia de eventos, entre los estados del sistema (state-event, como se conoce en inglés).

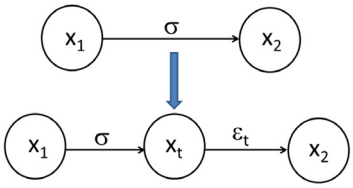

Figura 1: Estado transitorio

2.3.2. Análisis temporizado pasivo para el diagnóstico de fallas

Para llevar a cabo el análisis propuesto en Ferrarini et al. (2008), se toman en cuenta las siguientes suposiciones:

(A1) Sea $c \in \Sigma_c$ un evento controlable. La dinámica nominal del sistema se supone ejecutada correctamente si luego del evento c, los eventos observables esperados ocurren dentro de un período de tiempo T_{max} (condición *timeout*).

(A2) Sea $o \in \Sigma_o$ un evento observable. El sistema se supone en estado de equilibrio si luego del último evento o, no son producidos eventos observables sucesivos dentro del período T_{max}.

Luego, el análisis temporizado se establece como sigue, Cerrada et al. (2010):

Sea G_d el diagnosticador del sistema S definido como el autómata $G_d = (Q_d, \Sigma_o, \delta_d, q_0)$, y sea q_d un estado de G_d definido como el conjunto $q_d = \{(x_1, l_1), \ldots, (x_m, l_m)\}$ donde $x_i \in X$ y $l_i \in \Delta$, siendo Δ un conjunto de etiquetas de falla. Entonces:

Definición 2.6. *El estado de equilibrio del diagnosticador es definido como el conjunto* $q_{eq} \subset q_d \in Q_d$ *tal que* $q_{eq} = \{(x_i, l_i) / x_i \notin X_t\}$.

Definición 2.7. *Sea* $q_{eq\_j} \subset q_j$ *el estado de equilibrio actual del diagnosticador* G_d *y sea un evento observable* $o \in \Sigma_o$. *El estado de equilibrio sucesivo* q_{eq_j+} *de* G_d *es definido como el conjunto compuesto por el alcance debido al evento o, dado por* $S(x, o) = \{\delta(x, \sigma o), \sigma \in (\Sigma_{uo} \cap \Sigma_{uc})^*\}$. *Nótese que* $q_{eq\_j+} \subset q_{j+} \in Q_d$, *donde* q_{j+} *es el estado sucesivo de* G_d *alcanzado desde* q_j *debido al evento o.*

Definición 2.8. *Bajo el análisis temporizado, el estado de equilibrio* $q_{eq\_j+} \subset q_{j+} \in Q_d$ *se dice* F_i-cierto *si* $\forall (x, l) \in q_{eq\_j+}$, $F_i \in l$.

3. Obtención de conjuntos abarcadores de fallas a partir de diagnosticadores de estados

La diagnosticabilidad basada en crónicas queda establecida si es posible asociar con certeza, una crónica del sistema a la firma de una falla, de allí surge el interés primario en construir las firmas de las fallas para luego obtener las crónicas asociadas a ellas. En los trabajos referidos previamente, tanto los modelos de crónicas como sus instancias son obtenidos a partir de conocimiento experto, y no a partir de procedimientos sistemáticos usando modelos formales para sistemas de eventos discretos.

La metodología aquí planteada logra la construcción de las firmas de las fallas a partir del modelo del autómata y se basa en el hecho de tener la proyección observable del lenguaje del sistema en un diagnosticador de estados (ver Cassandras y Lafortune (2008)), luego las firmas de todas las fallas básicas se encuentran en el autómata diagnosticador con una partición de fallas básicas. Nos interesa el diagnosticador construido con una partición de fallas básicas a fin de obtener las firmas elementales.

Proposición 3.1. *Sea* $Sig(f_i) = P_{OBS}(L_{f_i}^{max}) = L_{OBS-f_i}^{max} \subseteq OBS$ *y sea q un estado del diagnosticador. Entonces:*

$L_{OBS-f_i} = \bigcup L_{OBS}(q)$, $\forall q \mid f_i \in l_i$ *para algún* $(x_i, l_i) \in q$ *y* $q \in$ *ciclo.*

Se consideran los estados q que pertenecen a un ciclo, ya que nos interesa el lenguaje maximal de la falla obtenido a partir de los ciclos que se forman en el diagnosticador. Debido a que el lenguaje observable $L_{OBS}(q)$ es obtenido para estados q que forman un ciclo en el diagnosticador, entonces $L_{OBS-f_i} = L_{OBS-f_i}^{max}$.

3.1. Metodología para la obtención de L_{OBS-f_i} a partir del modelo temporizado

Debido a las características particulares del modelado temporizado, se establece la siguiente metodología para la obtención de firmas elementales, en base a la Proposición 3.1:

1. Obtener el estado de equilibrio del diagnosticador según la Definición 2.6.
2. Identificar en el diagnosticador, los estados que formen un ciclo tal que $f_i \in l_i$ para algún $(x_i, l_i) \in q$, es decir, los estados que formen un ciclo f_i-cierto o un ciclo f_i-indeterminado (según Sampath et al. (1996)).
3. Obtener el lenguaje observable de cada estado que pertenece al ciclo: $L_{OBS}(q)$, $q \in$ ciclo.
4. Obtener la unión de los lenguajes observables de todos los estados que pertenecen al ciclo, ésto es, $\bigcup L_{OBS}(q)$, $\forall q \in$ ciclo.
5. Obtener la unión de los lenguajes observables de todos los ciclos con f_i. Este conjunto constituye la firma $Sig(f_i)$.

Si un ciclo es no f_i-indeterminado y contiene otras fallas f_j (incluyendo la ausencia de falla f_0), la firma de la falla f_i no se obtiene en este ciclo sino la de f_j. Este hecho esta asociado a la relación entre la diagnosticabilidad basada en observadores de estado establecida en Sampath et al. (1996) y la definición de firma de falla.

Ejemplo. Consideremos el sistema de la Fig. 2, donde σ_{f1} es un evento de falla. El autómata G' se presenta en la Fig. 3 y su diagnosticador en la Fig. 4.

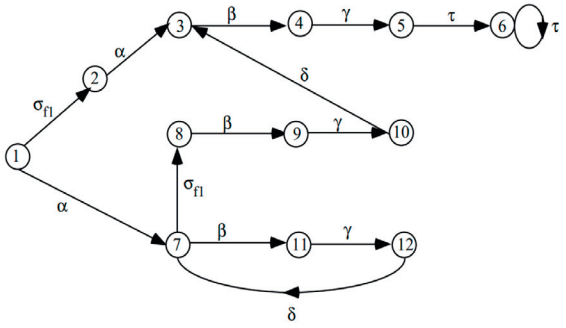

Figura 2: El sistema G, Sampath et al. (1996)

Las etiquetas $F1$ y N están en un ciclo y siendo un ciclo no $F1$-indeterminado, entonces:

$$Sig(F1) = \alpha(\beta\gamma\delta)^*\beta\gamma\tau\tau^\infty$$

$$Sig(N) = \alpha(\beta\gamma\delta)^\infty, \alpha\beta(\gamma\delta\beta)^\infty, \alpha\beta\gamma(\delta\beta\gamma)^\infty$$

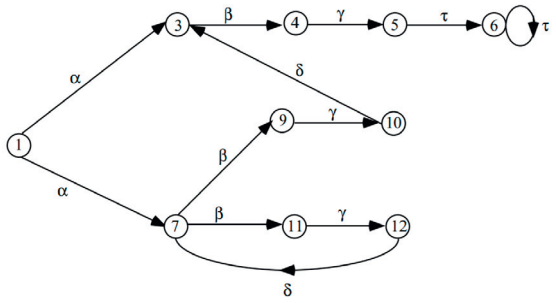

Figura 3: El autómata G´, Sampath et al. (1996)

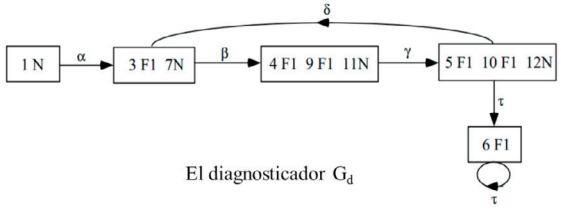

Figura 4: Diagnosticador con ciclo no indeterminado, Sampath et al. (1996)

Para un ciclo $F1$-indeterminado, $Sig(N) \subset Sig(F1)$.

Esta metodología para la obtención de firmas de falla propuesta en esta trabajo es la base para la definición de crónicas asociadas con las fallas. El lenguaje de la crónica debe contener las firma $Sig(f)$ y esta debe estar contenida en la firma característica $cSig(f)$ para que el sistema sea diagnosticable.

3.2. *Metodología para la obtención de un conjunto abarcador diagnosticable*

A partir del conocimiento de las firmas elementales, según lo descrito en la sección 3.1, se propone a continuación la metodología para la obtención de un conjunto abarcador diagnosticable:

1. Encontrar las firmas elementales de las fallas básicas del sistema, siguiendo la metodología propuesta en la sección 3.1.
2. Escoger un conjunto abarcador de macrofallas (Definición 2.2), siguiendo el siguiente criterio basado en la estructura del diagnosticador de estados:
   Sea q un estado de un ciclo f_i-indeterminado, tal que $f_i \in l_i$ y $f_j \in l_j$, con $f_i, f_j \neq f_0$, para algún $(x_i, l_i) \in q$ y $(x_j, l_j) \in q$, definir un conjunto abarcador $E(\mathcal{F})$ que contenga la macrofalla $F_k = \{f_i, f_j\}$.
3. Obtener las firmas características (Definición 2.4) para cada macrofalla que pertenece al conjunto abarcador, considerando el conjunto más grande de firmas características de F_j, ésto es $cSig(F_j) = (\bigcup_{f_i \in F_j} (Sig(f_i)) \setminus \bigcup_{f_k \notin F_j} (Sig(f_k)))$.
4. Verificar las condiciones para la diagnosticabilidad del conjunto abarcador de macrofallas, según la Definición 2.5:
   a) Si la condición 1 de la Definición 2.5 no se cumple, entonces el sistema *no* es diagnosticable.
   b) Si la condición 2 de la Definición 2.5 no se cumple, entonces considerar para aquellas macrofallas F_j, tales que $cSig(F_j) \supset cSig(F_k)$, $j \neq k$, una firma característica $\widehat{cSig}(F_j) \subset cSig(F_j)$, con $\widehat{cSig}(F_j) = \left(cSig(F_j) \setminus cSig(F_k)\right)$, y regresar al paso 4.
   c) Si las dos condiciones de la Definición 2.5 se cumplen, entonces el sistema es diagnosticable.

El paso (4.b) es justificado porque cualquier subconjunto de un conjunto de firmas características también constituye una firma característica. La elección de un conjunto abarcador diagnosticable puede tener varios criterios, dependiendo de cuáles son los tipos de falla que pueden ser agrupados en una macrofalla, donde la identificación de la ocurrencia de alguna de las fallas del conjunto es suficiente. La contraparte es la diagnosticabilidad del conjunto abarcador de macrofallas escogido. Luego, buscando un equilibrio en el criterio de elección, la decisión se basa en la estructura del diagnosticador de estados. Por otro lado, a fin de garantizar que el sistema sea detectable, el estado *normal* etiquetado como f_0 no debe ser agrupado en una macrofalla.

Ejemplo. Consideremos el modelo basado en autómata de la Fig. 5, que describe a un sistema de eventos discretos, y su diagnosticador en la Fig. 6.

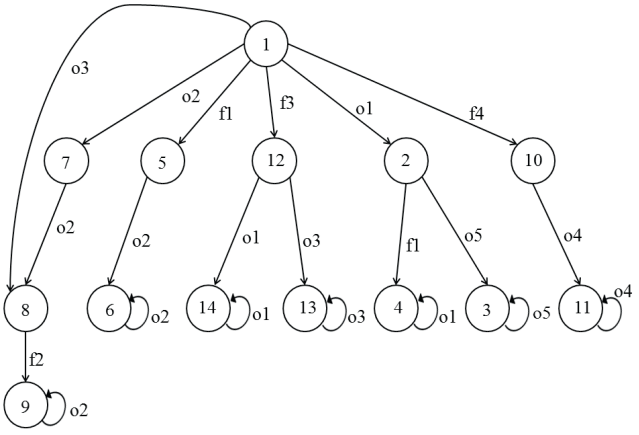

Figura 5: Autómata de un sistema de eventos discretos, Cordier et al. (2007b)

Las firmas de cada falla según la metodología de la sección 3.1 son:

$$
\begin{aligned}
Sig(f_0) &= L_{OBS-f_0} = \{o_1 o_5^{\infty}\} \\
Sig(f_1) &= L_{OBS-f_1} = \{o_1^{\infty}, o_2^{\infty}\} \\
Sig(f_2) &= L_{OBS-f_2} = \{o_2^{\infty}, o_3 o_2^{\infty}\} \\
Sig(f_3) &= L_{OBS-f_3} = \{o_3^{\infty}, o_1^{\infty}\} \\
Sig(f_4) &= L_{OBS-f_4} = \{o_4^{\infty}\} \\
OBS^{max} &= \{o_1 o_5^{\infty}, o_1^{\infty}, o_2^{\infty}, o_3 o_2^{\infty}, o_3^{\infty}, o_4^{\infty}\}
\end{aligned}
$$

Según el criterio del paso (2) de la metodología de la sección 3.2, se define a partir del diagnosticador el conjunto abarcador:

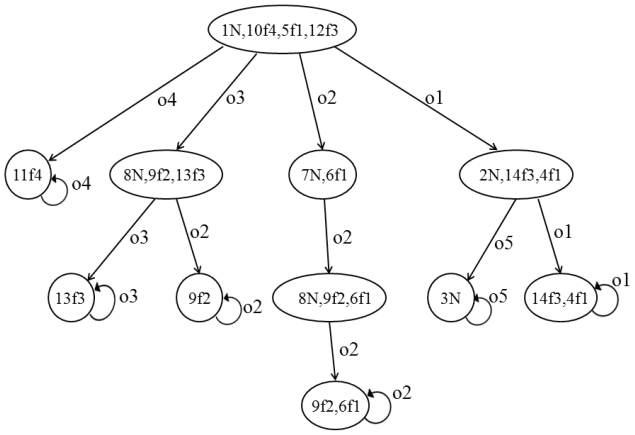

Figura 6: Autómata diagnosticador del sistema de la Fig. 5

$$E(\mathcal{F}) = \{\{f_0\}, \{f_1, f_2\}, \{f_2\}, \{f_1, f_3\}, \{f_3\}, \{f_4\}\}$$

donde las macrofallas se denotan como $F_0 = \{f_0\}$, $F_1 = \{f_1, f_2\}$, $F_2 = \{f_2\}$, $F_3 = \{f_1, f_3\}$, $F_4 = \{f_3\}$, $F_5 = \{f_4\}$. Luego tenemos:

$$\begin{aligned}
cSig(F_0) &\subseteq \left(\{o_1 o_5^{\infty}\}\right)\\
cSig(F_1) &\subseteq (\{o_2^{\infty}, o_3 o_2^{\infty}\})\\
cSig(F_2) &\subseteq (\{o_3 o_2^{\infty}\})\\
cSig(F_3) &\subseteq \left(\{o_1^{\infty}, o_3^{\infty}\}\right)\\
cSig(F_4) &\subseteq \left(\{o_3^{\infty}\}\right)\\
cSig(F_5) &\subseteq (\{o_4^{\infty}\})
\end{aligned}$$

Para este conjunto de firmas características, el conjunto abarcador no es diagnosticable según las condiciones de la Definición 2.5, sin embargo, aún es posible encontrar conjuntos $\widehat{cSig}(F_j)$, según lo indicado en el paso (4) de la metodología de la sección 3.2. En efecto:

$$\begin{aligned}
\widehat{cSig}(F_1) &\subset cSig(F_1)\\
&= (cSig(F_1) \setminus cSig(F_2))\\
&= (\{o_2^{\infty}\})\\
\widehat{cSig}(F_3) &\subset cSig(F_3)\\
&= (cSig(F_3) \setminus cSig(F_4))\\
&= (\{o_1^{\infty}\})
\end{aligned}$$

De esta manera:

- Existe un conjunto de firmas características que forman una partición de OBS^{max}.
- El conjunto $\widehat{PSig} = \{\{o_1 o_5^{\infty}\}, \{o_2^{\infty}\}, \{o_3 o_2^{\infty}\}, \{o_1^{\infty}\}, \{o_3^{\infty}\}, \{o_4^{\infty}\}\}$ es una partición de firmas elementales, tal que cualquier observación $\sigma \in cSig(F_j)$ garantiza que F_j está presente.
- El conjunto abarcador es diagnosticable.

4. Obtención de crónicas para el conjunto abarcador diagnosticable en el enfoque temporizado

El modelo de la crónica se construye a partir de cada firma del conjunto abarcador diagnosticable obtenido en la sección 3.2, añadiendo las restricciones temporales derivadas del propio lenguaje o del conocimiento previo. Para la clase de sistemas que se describen en la Sección 2.3, las restricciones temporales se derivan de la condición *timeout* que tendrá asociado un evento *STOP* en el diagnosticador, explícitamente o implícitamente, según sea la sucesión de eventos observables. El evento observable artificial STOP modela la ocurrencia de un *no evento* en el sistema real.

Dependiendo de la condición *timeout*, se pueden instanciar diferentes modelos de crónicas para la misma secuencia de eventos, diferenciados por las restricciones temporales entre los eventos. Es decir, podemos tener una crónica con una secuencia *abc*, donde todos los eventos ocurran dentro de T_{max}, asociada a una falla f_i, y tener otra crónica con la misma secuencia de eventos pero con un *timeout* luego de cada evento, asociada a otra falla f_j.

4.1. Base de crónicas explícitas

Primeramente, se obtienen los modelos de crónica a partir de cada firma de una macrofalla, considerando, en el lenguaje de la firma, la aparición explícita del evento ficticio *STOP*, ésto es, la ocurrencia de una condición *timeout*. Por ejemplo, dada la firma $\{a, STOP, b, STOP^{\infty}\}$, asociada a una macrofalla $\{F_j\}$, el modelo de crónica correspondiente sería: $C_1(F_j) = (\mathcal{S}_1, \mathcal{T}_1)$, con $\mathcal{S}_1 = \{(a, ?t_1), (STOP, ?t_2), (b, ?t_3), (STOP, ?t_4)\}$ y $\mathcal{T}_1 = \{0 < ?t_2 - ?t_1 \leq T_{max}, ?t_3 > ?t_1 + T_{max}, 0 < ?t_4 - ?t_3 \leq T_{max}\}$.

Esta crónica representa el hecho de que habiendo ocurrido el evento a, no ocurre ningún otro evento observable dentro de un período de tiempo T_{max}, previamente definido, el evento b ocurre en cualquier tiempo mayor que $?t_1 + T_{max}$ y ningún evento observable ocurre dentro de un nuevo período de tiempo T_{max} después de ocurrir el evento b. Así, si la crónica $C_1(F_j)$ es reconocida, el sistema dará como diagnóstico la macrofalla F_j.

Todos los modelos de crónica obtenidos de esta manera, son crónicas de interés y por lo tanto conforman la base de crónicas explícita del sistema.

4.2. Extensión de la base de crónicas

En una segunda etapa, se debe extender la base de crónicas tomando en cuenta que pueden existir situaciones de *timeout* que no están evidenciadas explícitamente en las firmas porque no aparece el evento *STOP* explícitamente en el diagnosticador.

Ésto significa que si una crónica $C_1(F_j) = (\mathcal{S}_1, \mathcal{T}_1)$ con $\mathcal{S}_1 = \{(a, ?t_1), (b, ?t_2)\}$, siendo a y b eventos observables con restricciones de tiempo $\mathcal{T}_1$, tiene una condición de *timeout* implícita entre la sucesión de eventos *ab*, entonces se definirá otra crónica adicional $C_2 = (\mathcal{S}_2, \mathcal{T}_2)$ donde $\mathcal{T}_2$ describirá las nuevas restricciones temporales y $\mathcal{S}_2 = \{(a, ?t_1), (STOP, ?t_2), (b, ?t_3)\}$.

La información de si existe o no una condición de *timeout* implícita se obtiene directamente del diagnosticador, detectando las sucesiones de un par de eventos observables (diferentes

de *STOP*) que tienen asociados estados que permitan la condición de *timeout*, definiendo primeramente los estados *candidatos*:

Definición 4.1. *El conjunto de los estados candidatos donde puede haber un evento STOP para la firma* $Sig(f_i)$ *es definido como* $Q^{cand} = \{q_d \in Q_d^{vivo} : \delta_d^{vivo}(q_{d\_i}, o_i) = q_d \text{ y } \delta_d^{vivo}(q_d, o_j) = q_{d\_j}\}$ *a lo largo de la traza* $Sig(f_i)$*, donde* q_{d_i}*,* q_{d_j} *son estados del diagnosticador* G_d^{vivo}*, y* $o_i, o_j \in \Sigma_o$*, son dos eventos observables, siendo* $o_i, o_j \neq STOP$*.*

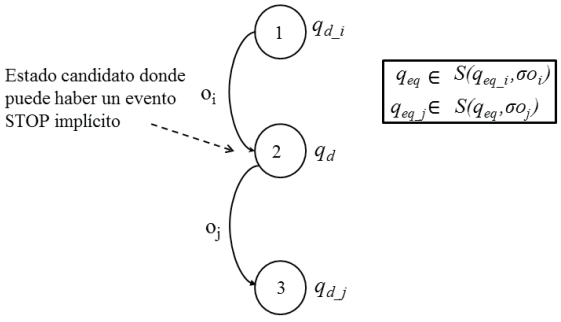

Figura 7: Sucesión de eventos observables que puede asociarse a un evento *stop*

La Fig. 7 ilustra la definición 4.1. De estos estados candidatos se deben descartar aquellos en los cuales, si existe una condición *timeout* que define el estado de equilibrio $q_{eq} \subset q_d \in Q^{cand}$ según la Definición 2.6, el alcance S debido al evento observable siguiente o_j no está definido. Entonces:

Definición 4.2. *Sea* $q_{eq\_i} \subset q_{d\_i}$ *un estado de equilibrio. El conjunto de los estados donde existe un evento* STOP *implícito para la firma* $Sig(f_i)$ *está formado por el conjunto* $Q = \{q_d \in Q^{cand}$ *tal que* $q_{eq} \subset q_d \in Q^{cand}$ *y* $q_{eq\_j} \subset q_{d\_j}$ *están definidos a partir de* $q_{eq\_i}\}$.

En la Definición 4.2, el estado de equilibrio es considerado como en la Definición 2.7. Luego, q_{eq} y q_{eq_j} son estados de equilibrio para la sucesión de eventos o_i, o_j sobre la traza $Sig(f_i)$.

De esta manera, la base de crónicas es actualizada con las nuevas secuencias temporales, que no provienen directamente del lenguaje del diagnosticador, sino que son derivadas de un análisis temporizado posterior sobre las trazas observables (firmas) obtenidas.

5. Diagnóstico modular basado en crónicas y analisis temporizado

En este trabajo se propone una arquitectura de diagnóstico basado en el reconocimiento de crónicas modulares, definidas a continuación:

Definición 5.1. *Una crónica modular es una crónica que modela la sucesión de eventos temporales de un módulo asociado a un sistema.*

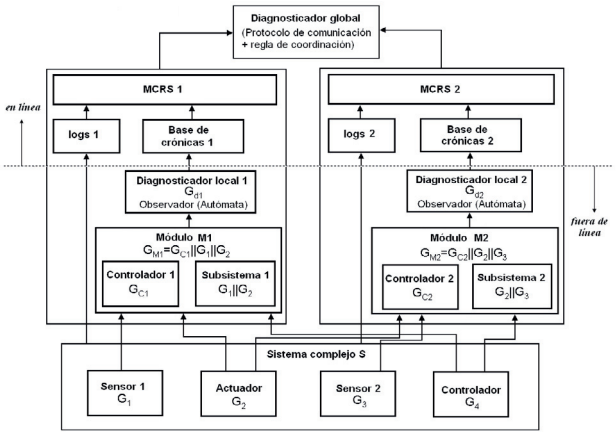

Figura 8: Arquitectura modular basada en crónicas

En este sentido, cada módulo definido para un sistema complejo tendrá asociado su conjunto de crónicas modulares, y caracteriza el comportamiento del módulo en un contexto dado. La Fig. 8 muestra la arquitectura modular basada en crónicas propuesta en este trabajo, la cual está inspirada en la arquitectura modular presentada en Cerrada et al. (2010), y en la arquitectura de diagnóstico de Cordier et al. (2007a). El sistema está compuesto por un diagnosticador global y los módulos locales, cada uno compuesto por: *(i)* el propio módulo, definido como en Cerrada et al. (2010); *(ii)* un diagnosticador de estados modular construído como en Sampath et al. (1996); *(iii)* una base de crónicas modulares, generada fuera de línea a partir de cada diagnosticador modular, siguiendo el procedimiento de la sección 4; *(iv)* los *logs* generados en tiempo real por el proceso (eventos observables); *(v)* un Sistema de Reconocimiento de Crónicas Modulares (*MCRS*-siglas en inglés); *(vi)* un diagnosticador global encargado de producir el diagnóstico global, a través de un protocolo de comunicación que se ejecuta en línea.

5.1. Protocolo de comunicación

La información diagnóstica local está dada por las crónicas modulares reconocidas. Cada MCRS, utiliza el *log* de eventos producidos en tiempo real (flujo de eventos) para instanciar los modelos de crónicas modulares previamente creados y que se encuentran en la base modular de crónicas.

Cuando una crónica modular c_{k_i} es reconocida por el *MCRS* i, con $i = 1, 2$, $k = 1, \ldots, n$, éste transmite al supervisor el diagnóstico local, dado por la macrofalla asociada a la crónica reconocida c_{k_i}. Si el *MCRS* j, $j = 1, 2$, $j \neq i$, no transmite ninguna información, el supervisor supone que es $\{N\}$ o la última macrofalla reconocida.

Las fallas candidatas globales que proveen de información diagnóstica global están dadas por el conjunto $F_C = \{\hat{f}_1, \hat{f}_2, \ldots, \hat{f}_n\}$, donde las fallas $\hat{f}_i$ provienen de aplicar la siguiente función de mezcla para cada par f_k, f_l, con $f_k \in F_k$ y $f_l \in F_l$, definida

como sigue:

$$merg(f_k, f_l) = \begin{cases} f_k \wedge f_l & \text{si} \quad \exists f_{ci}/(f_{ci} \in f_k), (f_{ci} \in f_l) \\ f_k & \text{si} \quad f_l = \{N\} \\ f_l & \text{si} \quad f_k = \{N\} \\ \text{indefinida} & \text{en} \quad \text{otro caso} \end{cases}$$

donde, f_k, f_l son fallas múltiples, y f_{ci} es una falla del componente común.

El supervisor realiza el diagnóstico global fusionando los diagnósticos locales usando dicha función de mezcla. Se asume que F_k y F_l provienen de módulos diferentes. Si las macrofallas F_k y F_l no poseen una falla en común (del componente común), entonces la función de mezcla no está definida.

6. Caso de estudio

En esta sección se considera un sistema de componentes electro-hidráulicos que se usan para mover actuadores que bloquean y desbloquean una mesa giratoria (RT-*rotary table*). El sistema RT forma parte de uno de los componentes del susbistema de carga de piezas, que es bastante común en sistemas de manufactura dedicados a tareas de ensamblaje.

El sistema bajo estudio está compuesto por una válvula eléctrica de apertura/cierre (YV9) y sensores de presión (SP9 y SP10) con los valores 1/0. Cuando el comando de apertura, $YV9\_0$, se da, la válvula va al estado de abierto, el sensor de baja presión, SP10, va a 0 y el de alta presión, SP9, va a 1. Esta transición debe ocurrir dentro de un tiempo máximo de T_{max} = 5 seg. Los autómatas que modelan el sistema se muestran en la Fig. 9 y la Fig. 10. Los eventos de falla de la válvula son atascada abierta (SO-*stuck open*) y atascada cerrada (SC-*stuck closed*), y las fallas $g0$ y $g1$ llevan al sensor SP9 permanentemente atascado en 0 o en 1, respectivamente. Los estados de la válvula y del sensor, insertados antes de llegar a la configuración siguiente son estados transitorios. El sensor SP10 funciona de manera dual y su modelo se denota como G_3, con las fallas $G0$ and $G1$. La partición de falla es definida como $F_1 = \{g0\}$, $F_2 = \{g1\}$, $F_3 = \{G0\}$, $F_4 = \{G1\}$, $F_5 = \{SO\}$ y $F_6 = \{SC\}$. $F_0 = \{N\}$ representa el comportamiento normal del sistema.

El autómata centralizado de este sistema incluye más de 500 estados y de 1400 transiciones, lo cual requiere, por un lado, un importante esfuerzo para la construcción de la base de crónicas en cuanto la cantidad de variables a considerar y sus instancias y, por el otro lado, un esfuerzo computacional considerable para la implantación en tiempo real del sistema de reconocimiento de crónicas. Luego, se justifica el uso del enfoque modular para este sistema, permitiendo hacer un diagnóstico útil en sistemas de automatización industrial como éste, a partir de bases de crónicas modulares relativamente simples.

La estructura modular propuesta es de dos módulos. El módulo M_1 compuesto por los componentes YV9 y SP9, y el módulo M_2 por los componentes YV9 y SP10; cada módulo puede *observar* una parte del sistema y por lo tanto puede detectar las fallas correspondientes. El módulo M_1 puede detectar las fallas $F_1 = \{g0\}$, $F_2 = \{g1\}$, $F_5 = \{SO\}$ y $F_6 = \{SC\}$, y el módulo M_2 puede detectar las fallas $F_3 = \{G0\}$, $F_4 = \{G1\}$, $F_5 = \{SO\}$ y

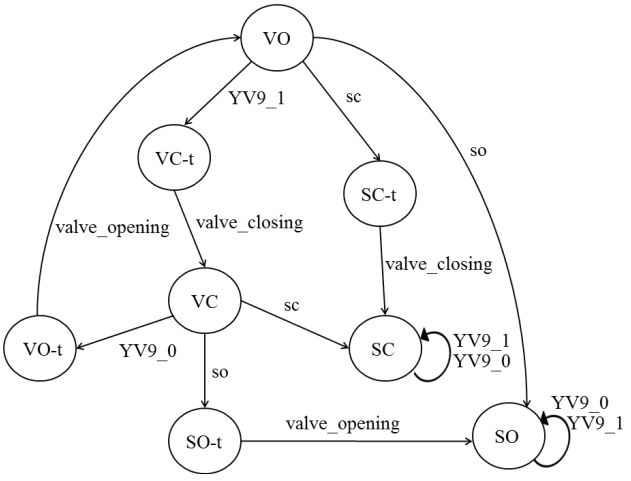

Figura 9: Modelo de la válvula YV9 (G_1)

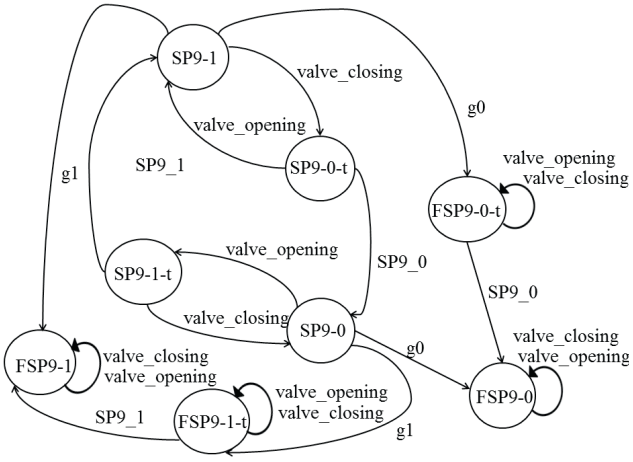

Figura 10: Modelo del sensor SP9 (G_2)

$F_6 = \{SC\}$. Debido a que ambos módulos comparten un componente común, consistente con la descomposición modular propuesta, ambos módulos poseen las fallas del elemento común dentro de su conjunto de fallas.

La inclusión del evento ficticio ó no evento *Stop* se hace en cada controlador modular. En la Fig. 11 se presenta el controlador G_{c1} para el módulo M_1, para el módulo M_2 el controlador se concibe de manera análoga.

Los diagnosticadores modulares, G_{d1} y G_{d2}, a partir de los cuales se obtienen las bases modulares de crónicas, se muestran en la Fig. 12 y en la Fig. 13.

Se aplicó la metodología de la sección 3.1 para encontrar las firmas de falla de cada módulo. Por ejemplo, para la falla múltiple $F1F5$ del módulo M_1 se encontró el siguiente conjunto $Sig(F1F5)$:

$\{STOP^*, YV9\_1, SP9\_0, STOP^*, YV9\_0, STOP^\infty$;
$STOP^*, SP9\_0, STOP^\infty$;
$STOP^*, YV9\_1, SP9\_0, STOP^*, SP9\_1, SP9\_0, STOP^\infty$;

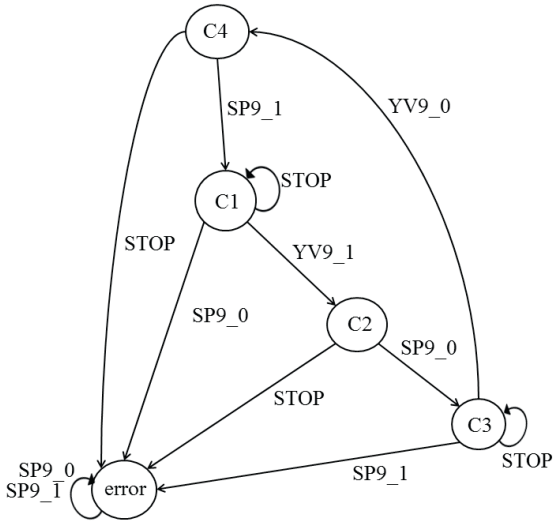

Figura 11: Controlador modular G_{c1}

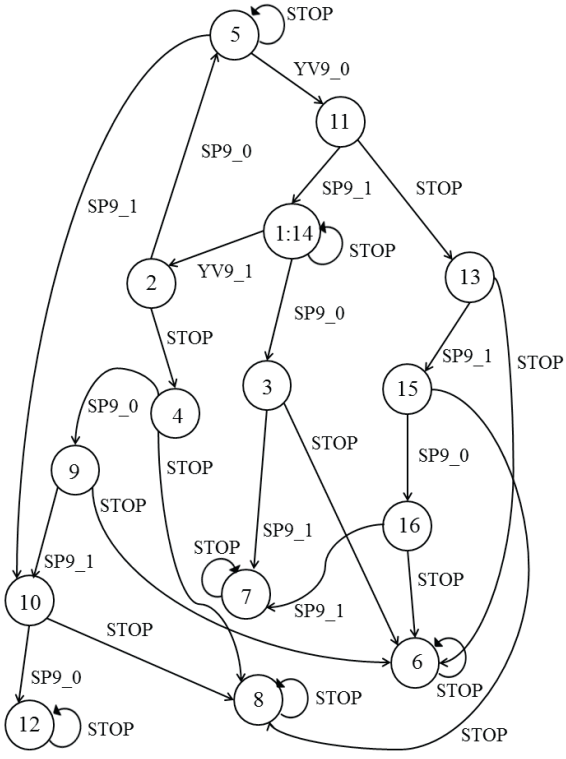

Figura 12: Diagnosticador modular G_{d1}

$STOP^*, YV9\_1, STOP, SP9\_0, SP9\_1, SP9\_0, STOP^\infty$;
$STOP^*, YV9\_1, STOP, SP9\_0, STOP^\infty$;
$STOP^*, YV9\_1, SP9\_0, STOP^*, YV9\_0, STOP, SP9\_1,$
$SP9\_0, STOP^\infty$ }

Luego se aplicó la metodología de la sección 3.2 para encontrar las firmas características que conducen a un conjunto abarcador diagnosticable. Para la falla arriba detallada se tiene que:

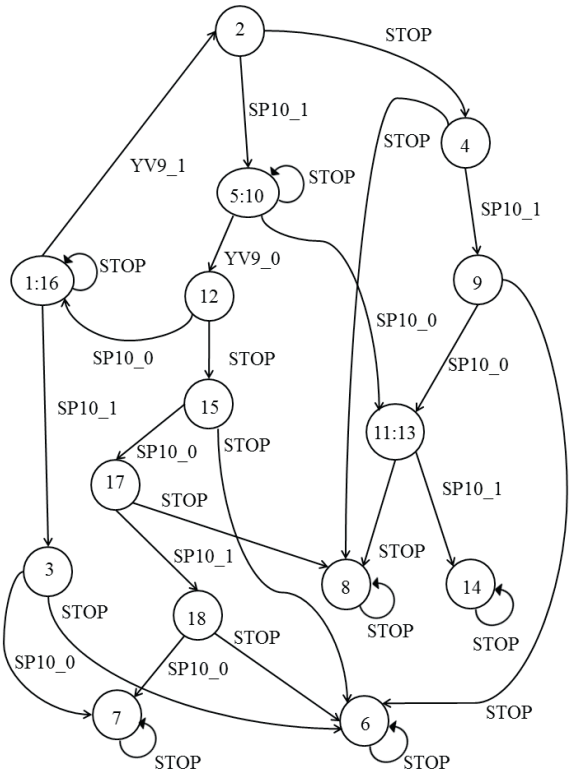

Figura 13: Diagnosticador modular G_{d2}

$$cSig(\hat{F}_1) \subseteq ((Sig(F1F5)) \setminus (Sig(F1F6) \bigcup Sig(F2F5) \bigcup Sig(F2F6) \bigcup Sig(F_0)))$$

$$cSig(\hat{F}_1) \subseteq (\{STOP^*, YV9\_1, SP9\_0, STOP^*, SP9\_1, SP9\_0, STOP^\infty; STOP^*, YV9\_1, STOP, SP9\_0, SP9\_1, SP9\_0, STOP^\infty\})$$

Haciendo el estudio exhaustivo, se definieron los conjuntos abarcadores diagnosticables $E(\mathcal{F}) = \{\hat{F}_0, \hat{F}_1, \hat{F}_2, \hat{F}_3, \hat{F}_4\}$, para cada módulo. Para M_1, $\hat{F}_0 = \{F_0\}$, $\hat{F}_1 = \{F1F5\}$, $\hat{F}_2 = \{F1F5, F1F6\}$, $\hat{F}_3 = \{F2F6\}$, y $\hat{F}_4 = \{F2F5, F2F6\}$. Análogamente, para M_2 se define $E_2(\mathcal{F})$ con $\tilde{F}_0 = \{F_0\}$, $\tilde{F}_1 = \{F3F6\}$, $\tilde{F}_2 = \{F3F5, F3F6\}$, $\tilde{F}_3 = \{F4F5\}$, y $\tilde{F}_4 = \{F4F5, F4F6\}$. F_0 denota la firma en ausencia de falla. Para estos conjuntos abarcadores, y estudiando la secuencia de eventos contenidos en las firmas características de cada macrofalla, se definieron las crónicas para cada una de ellas. Por ejemplo, para la secuencia $STOP, YV9\_1, STOP, SP9\_0, SP9\_1, SP9\_0, STOP$ asociada a la macrofalla $\{F1F5\}$ del módulo M_1, se obtiene la crónica $C(\{F1F5\})$ con:

$$\mathcal{S}_1 = \{(STOP, ?t_1), (YV9\_1, ?t_2), (STOP, ?t_3), (SP9\_0, ?t_4), (SP9\_1, ?t_5), (SP9\_0, ?t_6), (STOP, ?t_7)\}$$

$$\mathcal{T}_1 = \{?t_1 < ?t_2, ?t_2 < ?t_3, ?t_3 < ?t_4, ?t_4 < ?t_5, ?t_5 < ?t_6, ?t_6 < ?t_7, 0 < ?t_3 - ?t_1 \leq T_{max}, ?t_4 > ?t_1 + T_{max}, 0 < ?t_7 - ?t_4 \leq T_{max}\}$$

Finalmente, se obtuvo una base de crónicas extendida de 23 crónicas para cada módulo, que cubren todas las posibles sucesiones de eventos. Ésto representa una ventaja en comparación con las dimensiones del sistema centralizado.

A fin de ilustrar la ejecución del sistema de reconocimiento de crónicas modulares, se dan a continuación dos ejemplos de flujos de eventos diferentes, a partir del estado inicial que considera la válvula abierta.

6.1. Flujo de eventos 1

Suponga que el evento controlable $YV9\_1$ es dado, desde el estado inicial. El tiempo T_{max} expira sin que se observen eventos provenientes de los sensores. Ahora se observa el evento $SP9\_0$ y el tiempo T_{max} expira de nuevo. Finalmente se observa el evento $SP10\_1$. En este caso, el flujo de eventos se corresponde con el ciclo nominal pero el vencimiento de T_{max} entre la ocurrencia de los eventos observables esperados indica que una situación de falla esta ocurriendo. Este flujo de eventos se corresponde con las siguientes tres sucesiones temporales diferentes:

1. $STOP$, $YV9\_1$, $STOP$.
2. $STOP$, $YV9\_1$, $STOP$, $SP9\_0$, $STOP$.
3. $STOP$, $YV9\_1$, $STOP$, $SP9\_0$, $STOP$, $SP10\_1$, $STOP$.

Cada una de dichas secuencias temporales reconoce una crónica modular, asociada a una macrofalla definida, las cuales se muestran en la Tabla 1.

Tabla 1: Diagnóstico modular basado en reconocimiento de crónicas. Caso 1.

	Módulo 1 Macrofalla	Módulo 2 Macrofalla	Diagnóstico Global
1	$\{F2F5, F2F6\}$	$\{F3F5, F3F6\}$	$\{F2F3F5, F2F3F6\}$
2	$\{F1F5, F1F6\}$	$\{F3F5, F3F6\}$	$\{F1F3F5, F1F3F6\}$
3	$\{F1F5, F1F6\}$	$\{F4F5, F4F6\}$	$\{F1F4F5, F1F4F6\}$

A modo explicativo, cuando se ha alcanzado la secuencia 3, el módulo M_1 reconoce la crónica C_{9_1}: ($\mathcal{S}_{9\_1}$ = {($YV9\_1$, $?t_1$), ($STOP$, $?t_2$),($SP9\_0$, $?t_3$), ($STOP$, $?t_4$)}, con $\mathcal{T}_{9\_1}$ = {$0 < ?t_2 - ?t_1 \leq T_{max}$, $?t_3 > ?t_1 + T_{max}$, $0 < ?t_4 - ?t_3 \leq T_{max}$, $?t_1 < ?t_2 < ?t_3 < ?t_4$}), asociada a la macrofalla $\{F1F5, F1F6\}$. El módulo M_2 reconoce la crónica C_{20_2}: ($\mathcal{S}_{20\_2}$ = {($YV9\_1$, $?t_1$), ($STOP$, $?t_2$), ($SP10\_1$, $?t_3$), ($STOP$, $?t_4$)}, con $\mathcal{T}_{20\_2}$ = {$0 < ?t_2 - ?t_1 \leq T_{max}$, $?t_3 > ?t_1 + T_{max}$, $0 < ?t_4 - ?t_3 \leq T_{max}$, $?t_1 < ?t_2 < ?t_3 < ?t_4$}), asociada a la macrofalla $\{F4F5, F4F6\}$. Al aplicar la función de mezcla, el diagnosticador global aísla la macrofalla $\{F1F4F5, F1F4F6\}$, lo cual da como cierta la ocurrencia de las fallas $g0$ y $G1$, y como incierta la ocurrencia de SO ó SC. Este resultado puede verificarse a partir del diagnosticador centralizado.

6.2. Flujo de eventos 2

Suponga que el sistema está en el estado inicial, y sin darse el comando $YV9\_1$, se observa el evento inesperado $SP10\_1$, expira el tiempo T_{max} y posteriormente el evento $SP9\_0$ ocurre. Finalmente suponga que $SP9\_1$ ocurre después de expirar nuevamente T_{max}. En este caso, ambos módulos se encuentran fuera del ciclo nominal de operación. El flujo de eventos se corresponde con las siguientes tres sucesiones temporales diferentes:

1. $STOP$, $SP10\_1$, $STOP$.
2. $STOP$, $SP10\_1$, $STOP$, $SP9\_0$, $STOP$.
3. $STOP$, $SP10\_1$, $STOP$, $SP9\_0$, $STOP$, $SP9\_1$, $STOP$.

Las macrofallas reconocidas para cada una de las secuencias temporales se muestran en la Tabla 2.

Tabla 2: Diagnóstico modular basado en reconocimiento de crónicas. Caso 2.

	Módulo 1 Macrofalla	Módulo 2 Macrofalla	Diagnóstico Global
1	$\{N\}$	$\{F4F5, F4F6\}$	$\{F4F5, F4F6\}$
2	$\{F1F5, F1F6\}$	$\{F4F5, F4F6\}$	$\{F1F4F5, F1F4F6\}$
3	$\{F2F6\}$	$\{F4F5, F4F6\}$	$\{F2F4F6\}$

Cuando ocurre la primera secuencia, el módulo M_1 no ha salido de su ciclo nominal puesto que al no ocurrir ningún evento controlable, el sensor $SP9$ no debe emitir ningún cambio en su valor nominal, es por ésto que M_1 reconoce la crónica asociada al estado normal N. Si en el sistema no ocurre otro evento, la aplicación de la función de mezcla indica que la falla $F4$ ha ocurrido, es decir, $G1$ es cierta. Una vez que ha ocurrido la tercera secuencia, el módulo M_1 reconoce la crónica C_{13_1}: ($\mathcal{S}_{13\_1}$ = {($SP9\_0$,$?t_1$), ($STOP$,$?t_2$), ($SP9\_1$,$?t_3$), ($STOP$,$?t_4$)}, con $\mathcal{T}_{13\_1}$ = {$?t_1 < ?t_2 < ?t_3 < ?t_4$, $0 < ?t_2 - ?t_1 \leq T_{max}$, $?t_3 > ?t_1 + T_{max}$, $0 < ?t_4 - ?t_3 \leq T_{max}$}), asociada a la macrofalla $\{F2F6\}$. Por su parte, el módulo M_2 reconoce la crónica C_{19_2}: ($\mathcal{S}_{19\_2}$ = {($SP10\_1$,$?t_1$), ($STOP$,$?t_2$)}, con $\mathcal{T}_{19\_2}$ = {$0 < ?t_2 - ?t_1 \leq T_{max}$}), asociada a la macrofalla $\{F4F5, F4F6\}$. Así, al aplicar la función de mezcla sobre las macrofallas $\{F2F6\}$ y $\{F4F5, F4F6\}$, se obtiene como diagnóstico global $\{F2F4F6\}$. Luego, la ocurrencia de $g1$, $G1$ y SC es cierta. Este resultado puede verificarse a partir del diagnosticador centralizado.

7. Conclusión

Este trabajo propone un enfoque modular temporizado basado en crónicas para el diagnóstico de fallas. Las principales contribuciones son la proposición de una metodología para obtener las firmas de falla a partir del modelo de falla contenido en un diagnosticador de estados, una metodología para encontrar un conjunto abarcador de fallas diagnosticable, un procedimiento sistemático para la obtención de crónicas a partir de firmas de falla basado en un modelo temporizado, y un protocolo de comunicación que permite hacer un diagnóstico global a partir de la información local, todo ello enmarcado en una

arquitectura de diagnóstico modular. El protocolo de comunicación puede ser fácilmente implementado en línea. Asimismo, el enfoque propuesto es aplicable a casos reales de sistemas de automatización industrial.

El caso de estudio analizado muestra que el diagnóstico obtenido depende de la secuencia de eventos observados, incluido el no-evento *stop*, por tanto la observación de un nuevo evento, adicional al flujo de eventos ya ocurrido puede cambiar completamente el resultado diagnóstico del momento. Ésto sugiere la inclusión de esquemas de diagnóstico activos para verificar que, en efecto, ningún otro evento observable diferente del no-evento *stop*, puede ocurrir.

Como trabajos futuros, se proponen la implementación del sistema de reconocimiento de crónicas modulares y la construcción automática de las crónicas, bajo las consideraciones hechas en este trabajo, usando técnicas de aprendizaje o de minería de datos.

English Summary

Diagnosis of Controlled Discrete-Event Systems: An Approach Based on Chronicles and Modular Analysis by Using Automata Models.

Abstract

Nowadays industrial process systems are becoming more complex and it is needed simpler and efficient diagnosers by decreasing the dimension of their models. Modular diagnosis has proved to be very efficient in order to reduce the complexity asociated to discrete event systems. This work proposes a diagnostic approach based on chronicles and modular temporized analysis. Each fault is associated with a set of chronicles and each chronicle recognizes fault signature which is obtained from the state diagnoser associated to the finite state automata defined for each process module. A base of modular chronicles is created, which are manipulated through a coordination protocol that runs online in order to produce the global diagnosis. The performance of the proposed approach is tested on a industrial case of study and adequate results are reached.

Keywords:

Discrete-event systems, fault diagnosis, diagnosability, chronicles, modular diagnosis, fault signatures.

Agradecimientos

Este trabajo ha sido financiado por el proyecto CDCHT-ULA I-1237-10-02-AA.

Referencias

Cassandras, C. G., Lafortune, S., 2008. Introduction to Discrete Event Systems, 2nd Edition. Springer, New York, USA.

Cerrada, M., Ferrarini, L., Dedé, A., Julio 2010. Modular fault diagnosis using temporized analisys for a class of discrete event systems. In: 12th LSS Large Scale Systems: Theory and Applications Simposium. Villeneuve d'Ascq. France.

Contant, O., Lafortune, S., Teneketzis, D., 2006. Diagnosability of discrete event systems with modular structure. Discrete Event Dynamic Systems 16 (1), 9–37.

Cordier, M., Guillou, X. L., Robin, S., Rozé, L., Vidal, T., Mayo 29-31 2007a. Distributed chronicles for on-line diagnosis of web services. In: The 18^{th} International Workshop on Principles of Diagnosis (DX-07). Nashville, TN, USA, pp. 37–44.

Cordier, M., Pencolé, Y., Travé-Massuyés, L., Vidal, T., 2007b. Self-healability = diagnosability + repairability. In: The 18^{th} International Workshop on Principles of Diagnosis (DX-07). Nashville, TN, USA, pp. 251–258.

Debouk, R., Lafortune, S., Teneketzis, D., 2000. Coordinated descentralized protocols for failure diagnosis of discrete event systems. Discrete Event Dynamic Systems 10 (1-2), 33–86.

Dousson, C., Gaborit, P., Ghallab, M., 1993. Situation recognition: Representation and algorithms. In: Proceedings of the 13^{th} IJCAI. Vol. 1. Chambéry, France, pp. 166–172.

Ferrarini, L., Brusa, R., Veber, C., 2008. A pragmatic approach to fault diagnosis in hydraulic circuits for automated machining: a case study. In: IEEE CASE 2008, the 4^{th} annual IEEE Conference on Automation Science and Engineering. Washington DC, USA.

Jamshidi, M., Julio 2010. From large-scale systems to system of systems: Control challenges for the 21st century. In: 12th LSS Large Scale Systems: Theory and Applications Simposium. Villeneuve d'Ascq. France.

Pencolé, Y., Subias, A., 2009. A chronicle-based diagnosability approach for discrete timed-event systems: Application to web-services. Journal of Universal Computer Science 15 (17), 3246–3272.

Pucel, X., Travé-Massuyés, L., Pencolé, Y., Julio 21-25 2008. Another point of view on diagnosability. In: 4^{th} European Starting AI Researcher Symposium (Stairs'2008). Patras, Grecia.

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., Teneketzis, D., 1996. Failure diagnosis using discrete-event models. IEEE Transactions on Control Systems Technology 4 (2), 105–124.

Wang, Y., Yoo, T., Lafortune, S., 2007. Diagnosis of discrete event systems using decentralized architectures. Discrete Event Dynamic Systems 17 (2), 233–263.