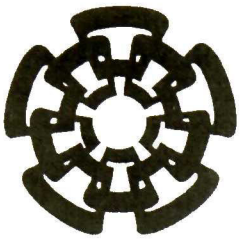
xx(178569.1)



Centro de Investigación y de Estudios Avanzados del I.P.N.
Unidad Guadalajara

Diagnóstico de faltas en sistemas de eventos discretos temporizados

Tesis que presenta:

Elías Hernández Flores

para obtener el grado de:

Maestro en Ciencias

en la especialidad de:

Ingeniería Eléctrica

Directores de Tesis

Dr. Luis Ernesto López Mellado
Dr. Antonio Ramírez Treviño

Guadalajara, Jalisco, Octubre de 2008.

Agradecimientos

A mis abuelos Antonio y Jesús por ser mi inspiración para seguir estudiando.

A mi madre, por su apoyo incondicional y sus consejos siempre atinados.

A Yesenia por su amor incondicional y estar conmigo en los buenos y malos momentos.

A mis amigos por los buenos momentos que he pasado en su compañía y sus valiosos consejos.

A mis asesores de tesis porque, con su disposición e invaluable experiencia contribuyeron en mi formación.

Diagnóstico de Faltas en Sistemas de Eventos Discretos Temporizados

Resumen

Se aborda el problema del diagnóstico de faltas permanentes en sistemas de eventos discretos (SED) y sistemas de eventos discretos temporizados (SEDT) en modelados con redes de Petri interpretadas (RPI) y con RPI temporizadas (RPIT) respectivamente.

Se define la propiedad de T-diagnosticabilidad en términos de RPIT y se propone una caracterización para redes de Petri que cumplen con ésta propiedad.

Además se extiende el concepto de diagnosticabilidad entrada-salida para aplicarse en modelos de RPIT; se propone una caracterización de RPIT que cumplen esta propiedad y se determina la relación que existe entre T-diagnosticabilidad y diagnosticabilidad entrada-salida.

Se muestra que la condición de evento-detectabilidad es una restricción importante que afecta tanto a la caracterización de la diagnosticabilidad entrada-salida propuesta en trabajos previos, como a la caracterización de T-diagnosticabilidad introducida en esta tesis.

Se proponen caracterizaciones y esquemas de diagnóstico para RPI con comportamiento de ME y GM que son diagnosticables entrada-salida en las cuales se relaja la condición de evento-detectabilidad.

Fault Diagnosis in Timed Discrete Event Systems

Abstract

This thesis addresses the problem of fault diagnosis in discrete event systems (DES) and timed discrete event systems (TDES) in models of interpreted Petri nets (IPN) and timed interpreted Petri nets (TIPN) respectively.

The T-diagnosability property of the TIPN is defined and then a characterization for TIPN models owning this property is proposed.

Furthermore input-output diagnosability concept is extended to the TIPN; a characterization of input-output diagnosable TIPN models is then proposed and the relationship between T-diagnosability and input-output diagnosability is analyzed.

It is showed that the event-detectability condition is an important constraint on both diagnosability characterizations; then news characterizations and diagnoser schemes are proposed for state machines and marked graphs subclasses, which are not event detectable.

Índice general

Índice de figuras

Introducción

Hasta el momento el hombre no ha creado un sistema exento de fallas. Las fallas son consecuencia de faltas internas las cuales provocan que un sistema funcione de una forma no deseada, originando un aumento en el costo de operación y la disminución de la seguridad; de aquí la importancia de contar con métodos de detección oportuna de faltas, que permitan incrementar la seguridad, la confiabilidad y el rendimiento del sistema.

A medida que se crean sistemas cada vez más grandes y complejos, se incrementa la probabilidad de que ocurran faltas y la dificultad para detectar las mismas. Por esto, el diagnóstico de faltas es un problema que se ha venido abordando en las últimas décadas, desde diferentes enfoques y con múltiples herramientas de modelado.

En el área de sistemas de eventos discretos (SED) el enfoque basado en los modelos ha sido adoptado por varios grupos de investigación; en este enfoque se han propuesto técnicas de diagnóstico donde prevalecen dos formalismo de modelado: los autómatas finitos (AF) y las redes de Petri (RP).

Entre los trabajos representativos del enfoque basado en AF se encuentran por un lado el propuesto en **[Sampath95]** donde un AF no determinista que describe el comportamiento normal y con faltas (representadas por eventos incontrolables) es procesado a través de alcanzabilidad para determinar la diagnosticabilidad y para obtener un diagnosticador. Por otro lado **[Hashtrudi05]** en se trata el problema de diagnóstico en sistemas SED temporizados (SEDT) a través del análisis del modelo expresado en AF temporizados. El principal problema común de estos enfoques reside en la talla de los modelos cuando son expresados como AF.

Los trabajos que utilizan RP para expresar sus modelos se benefician de la compacidad al representar el funcionamiento de los sistemas en especial cuando se trata con procesos concurrentes. Algunos trabajos como **[Genc05]**, **[Lefevbre07]** y **[Ruiz-Beltran07]** emplean redes de Petri como formalismo de modelado; sin embargo, no todos aprovechan la base matemática para llevar a cabo el análisis, realizando el análisis por alcanzabilidad.

El enfoque adoptado por el grupo de trabajo en SED del Cinvestav Unidad Guadalajara para abordar el diagnóstico de faltas es también basado en modelos de RP interpretadas (RPI). Sin embargo las técnicas propuestas para la determinación de la diagnosticabilidad son estructurales con el fin de evitar el análisis de alcanzabilidad **[Alcaraz04]**, **[Ruiz-Beltran07]**.

En este trabajo se trata el problema de diagnóstico de fallas en línea basado en modelos de RPI temporizadas desde un enfoque estructural. Se trata de extender los resultados obtenidos en **[Ruiz-Beltran07]**, considerando la duración de las actividades en el modelo y de estudiar la posibilidad de relajar la condición de evento-detectabilidad; lo que permitiría aplicar este método de análisis a una clase más amplia de modelos. A continuación se plantean los problemas tratados en esta tesis.

Problema 1: Sea (Q, M0) una RPI que representa un SED donde pueden ocurrir faltas permanentes de bloqueo. Entonces después de la ocurrencia de cualquier falta se debe cumplir que, con la entrada, la salida y el conocimiento de las actividades del sistema, se determine la ocurrencia de cualquier falta de manera única en un número de pasos finito.

Problema 2: Sea (E, M0) una RPI que representa un SED donde se conoce la duración de las actividades y pueden ocurrir faltas permanentes de bloqueo. Entonces después de la ocurrencia de cualquier falta se debe cumplir que con la entrada del sistema, la salida y el conocimiento de la duración de las actividades del sistema, se determine que falta ocurrió en un tiempo finito.

Así, los objetivos planteados en esta tesis son los siguientes:

- Extender resultados previos sobre diagnóstico de SED manejados por eventos donde se trata con faltas permanentes de bloqueo modelados con RPI.
- Considerar la duración de las actividades para ayudar en el proceso de diagnóstico.
- Definir y caracterizar la propiedad de diagnosticabilidad para SEDT.
- Proponer algoritmos eficientes para verificar la propiedad de diagnosticabilidad.
- Proponer esquemas de diagnóstico en línea.

El presente documento está organizado como sigue. En el Capítulo 1 se resumen los conceptos básicos acerca de sistemas de eventos discretos (SED) y redes de Petri (RP) En el Capítulo 2 se introducen conceptos relacionados con el diagnóstico de fallas en SED y se da una reseña de los trabajos que se relacionan con el diagnóstico de faltas. El Capítulo 3 trata el diagnóstico en línea en SEDT. El capítulo 4 trata el problema de diagnóstico de faltas en SED. Finalmente se dan comentarios sobre el trabajo realizado y las perspectivas de se plantean algunos aspectos importantes que se dejan como trabajo futuro.

CAPíTULO 1

Modelado de SED.

RESUMEN. *En este capítulo se definen los sistemas de eventos discretos (SED) y los sistemas de eventos discretos temporizados (SEDT); además se definen las RPI y las RPIT, las cuales son herramientas de modelado de SED y SEDT respectivamente.*

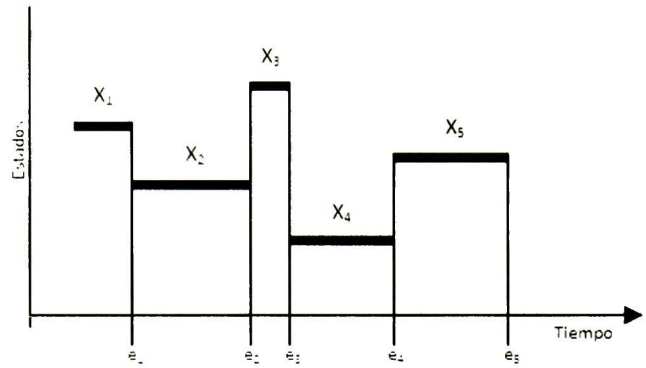


FIGURA 1.1.1. Sistema de eventos discretos.

1.1. Sistemas de eventos discretos

Existe una gran cantidad de sistemas de eventos discretos (SED), por ejemplo las redes de computadoras, sistemas de producción automatizada y sistemas de control. Estos se caracterizan porque su estado cambia de manera instantánea en una base de tiempo continua debido a la ocurrencia de algún evento. Los SED son sistemas dinámicos que tiene un espacio de estados numerable aunque posiblemente infinito.

DEFINICIÓN 1. *Un* sistema de eventos discretos *SED es un sistema de estados discretos manejados por eventos, de tal forma que, su evolución depende enteramente de la ocurrencia de eventos discretos asíncronos en el tiempo* **[Christos93]**.

Es posible "discretizar" un sistema continuo y tratarlo como un sistema de eventos discretos.

En la figura 1.1.1 se muestra un esquema que representa un sistema de eventos discretos en los que X_1 es el estado inicial del sistema y $e_1, e_2, e_3, e_4, e_5, e_6...$ son los eventos que hacen que el sistema cambie su estado. Sabemos que cada uno de estos eventos se da en alguna fecha, pero este no está determinado en el modelo.

1.2. Sistemas de eventos discretos temporizados

Cuando un SED se modela es posible adoptar dos enfoques:

- *El modelo no representa el tiempo:* Los eventos del sistema se dan como una secuencia de eventos $e_1, e_2, e_3, ...$, sin información sobre el tiempo en que ocurrieron estos. En este caso, dado un estado inicial se puede determinar las posibles secuencias de eventos, es decir, con este modelo se pueden contestar preguntas del tipo: ¿Puede un estado particular ser alcanzado?

  El modelo representa el tiempo: Los eventos del sistema se dan como una secuencia de eventos temporizada $(e_1, \tau_1), (e_2, \tau_2), ...$, en los que se sabe la fecha en la que ocurrió un evento. Es decir se pueden contestar preguntas como ¿Cuánto tiempo permanece el sistema en un estado particular? o ¿Cuándo se ejecutará un evento particular? o ¿Cuándo se alcanzará un estado particular? **[Christos93]**.

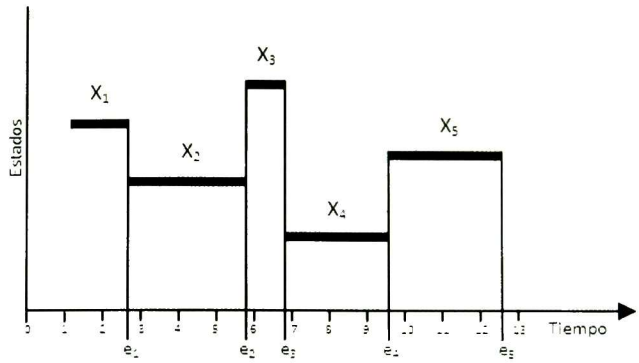


FIGURA 1.2.1. Sistema de eventos discretos temporizados.

Cuando hablamos de un sistema de eventos discretos temporizados nos estamos refiriendo a un sistema de eventos discretos en el que se toma en cuenta la duración de las actividades o el tiempo en que ocurren los eventos.

DEFINICIÓN 2. *Un* sistema de eventos discretos temporizado *(SEDT) es un sistema de eventos discretos en el que se conoce el tiempo que permanece el sistema en cada uno de los estados.*

En la figura 1.2.1 se muestra un esquema que representa un SEDT en los que se conoce el tiempo en que se ejecuta cada uno de los eventos y por lo tanto se sabe cuanto tiempo permanece el sistema en un estado determinado.

En esta tesis se usa tanto el enfoque temporizado como el no temporizado. La representación de los modelos se hace por medio de redes de Petri, las cuales se describen en la siguiente sección.

1.3. Conceptos básicos sobre redes de Petri.

A continuación se definen algunas clases de Redes de Petri y algunos conceptos relacionados con las redes de Petri usados en esta tesis.

1.3.1. Redes de Petri.

Una red de Petri (RP) es un grafo bipartido, compuesto por dos tipo de nodos: lugares y transiciones, y arcos que relacionan nodos de diferente tipo. Enseguida se da una definición formal.

DEFINICIÓN 3. *Un estructura N de un RP es un grafo bipartido representado por la 4-tupla* N=(P,T,I,O) *donde:*

- $P = \{p_1, p_2, ..., p_n\}$ es un conjunto finito de vértices llamados lugares.
- $T = \{t_1, t_2, ..., t_m\}$ es un conjunto finito de vértices llamados transiciones.
- $I : P \times T \longrightarrow \mathbb{Z}^+$ es un función que representa el peso de los arcos que van de los lugares a las transiciones.
- $O : P \times T \longrightarrow \mathbb{Z}^+$ es un función que representa el peso de los arcos que van de las transiciones a los lugares.

Donde $\mathbb{Z}^+$es el conjunto de enteros no negativos.

Gráficamente los lugares son representados por círculos, las transiciones por rectángulos y los arcos por flechas. El símbolo $\bullet t_j$ denota el conjunto de lugares p_i tales que $I(p_i, t_j) \neq 0$ y $t_j\bullet$ denota el conjunto de lugares p_i tal que $O(p_i, t_j) \neq 0$, de manera similar $\bullet p_i$ denota el conjunto de transiciones t_j tales que $O(p_i, t_j) \neq 0$ y $p_j\bullet$ el conjunto de transiciones t_j tales que $I(p_i, t_j) \neq 0$.

La matriz de pre-incidencia de N es $C^- = [c_{ij}^-]$, donde $[c_{ij}^-] = I(p_i, t_j)$; la matriz de post-incidencia de N es $C^+ = [c_{ij}^+]$, donde $[c_{ij}^+] = O(p_i, t_j)$; la matriz de incidencia de N es $C = C^+ - C^-$

DEFINICIÓN 4. *La función de marcado $M : P \longrightarrow \mathbb{N} \cup \{0\}$ representa el número de marcas (dibujados como puntos) en cada lugar de N. donde $\mathbb{N}$ representa el conjunto de los números naturales.*

El marcado generalmente se representa como un vector de n entradas, donde n es el número de lugares.

DEFINICIÓN 5. *Un red de Petri (RP) se compone del par (N, M_0), donde N es la estructura de la RP y M_0 es la distribución de marcas inicial.*

Una transición $t_i \in T$ está *habilitada* en un marcado M si y solo si $\forall p_j \in \bullet t_i : M(p_j) \geq I(p_j, t_i)$. Una transición habilitada $t_i \in T$ se puede disparar y su disparo alcanza un nuevo marcado M_{k+1}. M_{k+1} se calcula con la ecuación (1.3.1) llamada *ecuación de marcado.*

$$M_{k+1} = M_k + C \cdot \vec{v_i}, \tag{1.3.1}$$

donde $\vec{v_i}$ es un vector de m-entradas, tal que $\vec{v_i}(i) = 1$, y $\vec{v_i}(j) = 0$ para $i \neq j$.

EJEMPLO 1. *En la figura 1.3.1 se muestra una RP (N, M_0), en la que N está compuesta por $P = \{p_1, p_2, p_3, p_4, p_5\}$, $T = \{t_1, t_2, t_3, t_4, t_5\}$ y las funciones $I : P \times T \longrightarrow \mathbb{Z}^+$. $O : P \times T \longrightarrow \mathbb{Z}^+$ se representan por medio de la matriz de incidencia $C = C^+ - C^-$ de la ecuación (1.3.2). M_0 se muestra en la ecuación (1.3.3). Para la transición t_1 se tiene que el conjunto de pre-incidencia es $\bullet t_1 = \{p_1\}$ y el conjunto de post-incidencia es $t_1\bullet = \{p_2, p_3\}$. Para el lugar p_2 se tiene que conjunto de pre-incidencia es $\bullet p_2 = \{t_1, t_5\}$ y el conjunto de post-incidencia es $p_2\bullet = \{t_2\}$.*

$$\begin{bmatrix} -1 & 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 1 & -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{1.3.2}$$

$$M_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix}^T \tag{1.3.3}$$

M_0 habilita la transición t_1; si se dispara t_1 el nuevo marcado alcanzado M_1 es:

$$M_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} -1 & 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

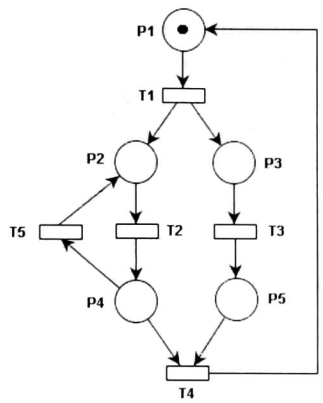


FIGURA 1.3.1. Red de Petri.

En M_1 las transiciones habilitadas son t_2 y t_3. Si se dispara la transición t_2 el nuevo marcado alcanzado M_2 será:

$$M_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} -1 & 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

DEFINICIÓN 6. *Se dice que dos transiciones t_i, t_j están en* conflicto estructural *si $\bullet t_i = \bullet t_j \neq 0$.*

DEFINICIÓN 7. *Una* secuencia de disparo *en (N, M_0) es una secuencia de transiciones $\sigma = t_i t_j ... t_k$ tal que $M_0 \longrightarrow_{t_i} M_1 \longrightarrow_{t_j} ... M_w \longrightarrow_{t_k} ....$ Donde $M_k \longrightarrow_t M_{k+1}$ indica que se alcanza el marcado M_{k+1} con el disparo de la transición t_i habilitada en el marcado M_k.*

DEFINICIÓN 8. *Sea $\sigma = t_i t_j t_k ...$ una secuencia de disparo. El vector de Parikh $\vec{\sigma}$ es una función $\vec{\sigma} : T \longrightarrow (\mathbb{Z}^+)^m$ que $\vec{\sigma}$ mapea cada transición $t \in T$ con el número de ocurrencias de t en σ.*

DEFINICIÓN 9. *El conjunto de todas las secuencias de disparo σ posibles desde M_0 es llamado* lenguaje de disparo *$L(N, M_0) = \{\sigma | \sigma = t_i t_j ... t_k$ tal que $M_0 \longrightarrow_{t_i} M_1 \longrightarrow_{t_j} ... M_w \longrightarrow_{t_k} ...\}$*

DEFINICIÓN 10. *El* conjunto de alcanzabilidad *de una RP, $R(N, M_0)$, es el conjunto de todos los marcados alcanzables a partir de M_0, mediante el disparo de transiciones habilitadas.*

DEFINICIÓN 11. *Una RP (N, M_0) es viva si $\forall M_i \in R(N, M_0)$ y $\forall t \in T$ se cumple que $\exists M_j$ tal que $M_i \longrightarrow_\sigma M_j \longrightarrow_t$.*

DEFINICIÓN 12. *Una RP (N, M_0) es k-acotada si $\forall M_i \in R(N, M_0)$ y $\forall p \in P$, $M(p) \leq k$. Si la RP es 1-acotada también es llamada segura o binaria.*

DEFINICIÓN 13. *Sea C la matriz de incidencia de RP (N, M_0). Un* T-semiflujo X_i *de* (N, M_0) *es una solución de valores racionales semi-positivos de la ecuación $CX_i = 0$. El soporte del T-semiflujo X_i es el conjunto $||X_i|| = \{t_j | X_i(t_j) \neq 0\}$.*

DEFINICIÓN 14. *Sea C la matriz de incidencia de RP (N, M_0). Un* P-semiflujo Y *de* (N, M_0) *es una solución de valores racionales semi-positivos de la ecuación $Y^T C = 0$. El soporte del P-semiflujo Y_i es el conjunto $||Y_i|| = \{p_j | Y_i(p_j) \neq 0\}$.*

DEFINICIÓN 15. *Sea X_i un T-semiflujo de la RP (N, M_0) y $||X_i||$ el soporte de X_i, entonces la subred inducida por X_i es $TC_i = (P_i = \cup p_r \in \bullet t_k, p_l \in t_k \bullet, t_k \in ||X_i||, T_i = ||X_i||, I_i, O_i)$, el cual es llamado* T-componente *inducido por X_i.*

DEFINICIÓN 16. *Sea Y_i un P-semiflujo de la RP (N, M_0) y $||Y_i||$ el soporte de Y_i, entonces la subred inducida por Y_i es $PC_i = (P_i = ||Y_i||, T_i = \cup t_k \in \bullet p_j, t_l \in p_j \bullet, p_j \in ||Y_i||, I_i, O_i)$, el cual es llamado* P-componente *inducido por Y_i.*

DEFINICIÓN 17. *Un* sifón *es un subconjunto de lugares $S = \{p_1, ..., p_s\} \subseteq P$ de una RP tal que $\bullet S \subseteq S \bullet$.*

DEFINICIÓN 18. *Una RP (N, M_0) es una máquina de estados (ME) si $\forall t_i \in T, |\bullet t_i| = 1 = |t_i \bullet|$.*

DEFINICIÓN 19. *Una RP (N, M_0) es una grafo marcado (GM) si $\forall p_i \in P, | \bullet p_i| = 1 = |p_i \bullet|$.*

1.3.2. Redes de Petri interpretadas.

Una extensión de las RP que asocia símbolos a los elementos de la RP son las *redes de Petri interpretadas* (RPI). Así una RPI tiene la posibilidad de modelar las entradas y salidas de un sistema.

DEFINICIÓN 20. *Un RPI* **[Meda98]** *es una 4-tupla $Q = (N, \Sigma, \lambda, \varphi)$ donde:*

- $N = (N, M_0)$ es una RP como se definió antes.
- $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_r\}$ es el alfabeto de entrada de la RP, donde α_i es i-ésimo símbolo de entrada del alfabeto.
  $\lambda : T \longrightarrow \Sigma \cup \{\varepsilon\}$ es la función de etiquetado de transiciones, con la siguiente restricción: $\forall t_j, t_k \in T$, $j \neq k$, si $\forall p_i I(p_i, t_j) = I(p_i, t_k) \neq 0$ y $\lambda(t_j) \neq \varepsilon$, $\lambda(t_k) \neq \varepsilon$, entonces $\lambda(t_j) \neq \lambda(t_k)$. En este caso ε representa un evento interno del sistema.
- Existe una matriz φ de dimensiones $q \times n$, tal que $y_k = \varphi M_k$ es el mapeo del marcado M_k en un vector de observación q-dimensional. La columna $\varphi(\bullet, i)$ es el vector elemental e_h si el lugar p_i tiene asociado el sensor h; o el vector nulo si p_i no tiene asociado ningún sensor.

Una transición habilitada t_j, etiquetada con $\lambda(t_j) \neq \varepsilon$ (transición manipulable) debe dispararse cuando $\lambda(t_j)$ es activado. Una transición t_j, etiquetada con $\lambda(t_j) = \varepsilon$ (transición no manipulable) se puede disparar si está habilitada, el tiempo en el que se puede disparar una transición no manipulable está dentro del intervalo $[0, \infty]$ a partir del instante en que se habilita.

La *ecuación de estado* de una RPI es igual que en una RP. El vector de observación y_k que se obtiene al alcanzar el marcado M_k se da en la ecuación (1.3.4).

(1.3.4) $$y_k = \varphi M_k$$

DEFINICIÓN 21. *Si $\lambda(t_i) \neq \varepsilon$ se dice que la transición t_i es* manipulable. *De otra forma es* no manipulable. *Se denota por T^{ε} al conjunto de transiciones no manipulables.*

Lugares y transiciones medibles.

DEFINICIÓN 22. *Si $\varphi(\bullet, i)$ no es un vector nulo se dice que p_i es un lugar* medible. *De otra forma es* no medible.

DEFINICIÓN 23. *Una transición t_i es medible si $\varphi C(\bullet, t_i)$ es diferente del vector nulo. De otra forma es* no medible. *Se denota por T^m al conjunto de transiciones medibles.*

DEFINICIÓN 24. *Una transición t_i es evento-detectable* **[Rivera05]** *si es posible inferir el disparo de t_i, inmediatamente después de que este se da, a partir de la entrada y salida del modelo de RP.*

En **[Rivera05]** se propone la caracterización siguiente para RPI que son evento-detectables.

LEMMA 1.3.1. *Una RPI viva dada por (Q, M_0) es evento-detectable si y sólo si*

$\forall t_i, t_j \in T$ tal que $\lambda(t_i) = \lambda(t_j)$ ó $\lambda(t_i) = \varepsilon$ se cumple que $\varphi C(\bullet, t_i) \neq \varphi C(\bullet, t_j)$,
$\forall t_k \in T$ se cumple que $\varphi C(\bullet, t_k) \neq 0$

Secuencias y lenguajes.

DEFINICIÓN 25. *Una secuencia de símbolos de entrada-salida de (Q, M_0) es una secuencia $\omega = (\alpha_0, y_0)(\alpha_1, y_1)...(\alpha_n, y_n)$, donde $\alpha_j \in \Sigma \cup \{\varepsilon\}$ y α_{i+1} es la entrada de la RPI cuando el vector de observación cambia de y_i a y_{i+1}. y_i puede ser igual a y_{i+1}, es decir, es posible que la entrada α_{i+1} no produzca cambio en la salida.*

DEFINICIÓN 26. *Sea (Q, M_0) una RPI. El conjunto $\Lambda(Q, M_0) = \{\omega | \omega$ es una secuencia de símbolos de entrada-salida$\}$ denota el conjunto de todas las secuencias de símbolos de entrada-salida de (Q, M_0). El conjunto de todas las secuencias de entrada-salida de una longitud mayor a k se denotan por $\Lambda^k(Q, M_0)$, es decir, $\Lambda^k(Q, M_0) = \{\omega \in \Lambda(Q, M_0) || \omega | \geq k\}$.*

DEFINICIÓN 27. *Si $\omega = (\alpha_0, y_0)(\alpha_1, y_1)...(\alpha_n, y_n)$ es una secuencia de símbolos de entrada-salida. Una secuencia disparo $\sigma \in L(Q, M_0)$ que genera ω es denotado por σ_ω. El conjunto de todas las secuencias de disparo que generan la palabra ω es definido como $\Omega(\omega) = \{\sigma | \sigma \in L(Q, M_0) \wedge$ el disparo de σ produce $\omega\}$.*

DEFINICIÓN 28. *El conjunto de todas las secuencias de símbolos de entrada-salida que llevan a marcados de bloqueo se denota por $\Lambda_B(Q, M_0)$, es decir, $\Lambda_B(Q, M_0) = \{\omega \in \Lambda(Q, M_0) | \exists \sigma \in \Omega(\omega)$ tal que $M_0 \longrightarrow_\sigma M_j$ y $M_j \longrightarrow_{t_i}$ no está definido para alguna transición$\}$.*

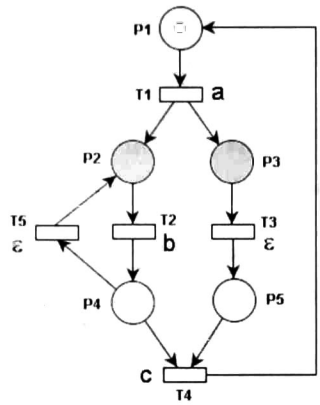


FIGURA 1.3.2. Red de Petri interpretada.

DEFINICIÓN 29. *Sea* $\omega = (\alpha_0, y_0)(\alpha_1, y_1)...(\alpha_n, y_n) \in \Lambda(Q, M_0)$ *una secuencia de símbolos de entrada-salida. El conjunto de secuencias de marcados correspondientes a* ω *es definido como* $S_\omega = \{M_0 M_1 ... M_k | M_i \in R(Q, M_0) \wedge M_0 \longrightarrow_{t_i} M_1 \longrightarrow_{t_j} ... \longrightarrow_{t_m} M_k \wedge \sigma_\omega = t_i t_j ... t_m \in \Omega(\omega)\}$.

DEFINICIÓN 30. *Si* $\omega = (\alpha_j, y_j)(\alpha_{j+1}, y_{j+1})...(\alpha_{j+n}, y_{j+n})$ *es una secuencia de símbolos de entrada-salida. La secuencia de salida correspondiente a* ω *es una secuencia* $\Theta_\omega = \{y_i, y_{i+1}, y_{i+2}...\}$ *donde* $y_j \in \Theta_\omega$ *y* $y_{j+1} \in \Theta_\omega$ *si y sólo si* $y_j \neq y_{j+1}$.

EJEMPLO 2. *En la figura 1.3.2 se muestra una RPI donde* $\Sigma = \{a, b, c\}$ *y* $\lambda(t_1) = a$, $\lambda(t_2) = b$, $\lambda(t_3) = \varepsilon$, $\lambda(t_4) = c$, $\lambda(t_5) = \varepsilon$, *la matriz* φ *correspondiente es la siguiente*

$$\varphi = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

los lugares p_1, p_4, p_5 *son* medibles *y los lugares* p_2, p_3 *son* no medibles; *en la matriz* φC *se puede ver que las transiciones* t_1, t_4, t_5 *son evento-detectables, mientras que las transiciones* t_2, t_3 *no lo son; todas las transiciones son medibles.*

$$\varphi C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 & 1 & 0 \\ 1 & -1 & -1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 1 & -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & -2 & -1 \end{bmatrix}$$

1.3.3. Redes de Petri interpretadas temporizadas.

A continuación se definen las redes de Petri llamadas *redes de Petri interpretadas temporizadas* (RPIT), las cuales son una variante de las RPI con una constante d_i asociado a cada lugar p_i. d_i representa el tiempo que tarda en ejecutarse el proceso representado por p_i.

DEFINICIÓN 31. *Una RPIT es una 2-tupla* (E, M_0) *donde:*

E es una RPI.

- $D : P \longrightarrow \mathbb{R}^+ - \{0\}$ es una función que asigna a cada lugar p_i un retardo d_i.

DEFINICIÓN 32. *La función λ de Q se redefine de la siguiente manera $\lambda : T \longrightarrow \Sigma \cup \{\varepsilon, \varepsilon\iota\}$, donde $\varepsilon\iota$ es el evento* siempre cierto, *con las siguientes restricciones,*

- $\forall t_j, t_k \in T$, $j \neq k$, si $\bullet t_j = \bullet t_k \neq \emptyset$ y $\lambda(t_j) = \lambda(t_k)$ entonces $\lambda(t_j) = \lambda(t_k) = \varepsilon \vee \lambda(t_j) = \lambda(t_k) = \varepsilon\iota$.
  $\forall t_i$ si $\lambda(t_i) = \varepsilon\iota$ entonces $\nexists t_k, \bullet t_i = \bullet t_k \neq \emptyset \wedge (\lambda(t_k) = a \vee \lambda(t_k) = \varepsilon)$ donde $a \in \Sigma$.

Las reglas de disparo son las siguientes:

Una transición habilitada t_j, etiquetada con $\lambda(t_j) \neq \varepsilon$ y $\lambda(t_j) \neq \varepsilon\iota$ (transición manipulable) debe dispararse cuando $\lambda(t_j)$ es activado.
Una transición t_j, etiquetada con $\lambda(t_j) = \varepsilon$ (transición no manipulable) se puede disparar si está habilitada,

- Una transición habilitada t_j, etiquetada con $\lambda(t_j) = \varepsilon\iota$ si se dispara entonces su disparo es inmediatamente después de la habilitación.

La ecuación de estado para un RPIT es igual a la expresada en la ecuación (1.3.1) para RP. Sin embargo, la condición de habilitación de las transiciones cambia; cuando se crea una marca en un lugar p_i deben transcurrir $D(p_i)$ unidades de tiempo antes que la marca esté disponible para habilitar una transición. Se puede expresar el marcado M_k de una RPIT como la suma $M_k = M_{kn} + M_{ka}$, donde M_{kn} representa el número de marcas en cada lugar p_i que aún no cumplen el retraso $D(p_i)$, y M_{ka} representa el número de marcas en cada lugar p_i que cumplieron con el retraso. Cuando una marca cumple su retardo pasa de M_{kn} a M_{ka}. Formalmente una transición t_j está habilitada en M_k si y sólo si $\forall p_i \in P$, $M_{ka}(p_i) \geq I(p_i, t_j)$. Cuando una transición habilitada t_j se dispara se alcanza un nuevo marcado M_{k+1} denotado por $M_k \longrightarrow_{t_j} M_{k+1}$.

EJEMPLO 3. *Retomando el ejemplo anterior en la figura 1.3.3 se muestra una RPIT con los siguientes retardos asignados a cada lugar. $D(p_1) = 1$, $D(p_2) = 1$, $D(p_3) = 2$, $D(p_4) = 1$ y $D(p_5) = 1$. La función λ se define de la siguiente forma. $\lambda(t_1) = a$, $\lambda(t_2) = b$, $\lambda(t_3) = c$, $\lambda(t_4) = \varepsilon\iota$, $\lambda(t_5) = \varepsilon$.*

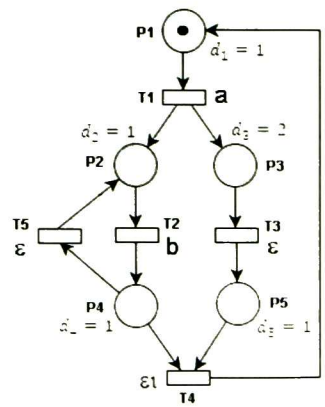


FIGURA 1.3.3. Red de Petri interpretada temporizada.

DEFINICIÓN 33. *Una* secuencia temporizada de disparos de transiciones *de una RPIT* (E, M_0) *es una secuencia de transiciones* $\sigma_\tau = (t_i, \tau_i)(t_j, \tau_j)...(t_k, \tau_k)...$ *tal que* $M_0 \longrightarrow_{t_i} M_1 \longrightarrow_{t_j} M_2... \longrightarrow_{t_k} M_w...$ *donde* τ_i *es el tiempo en el que se dispara* t_i.

Una secuencia σ es una secuencia σ_τ en la que no se considera el tiempo de disparo de las transiciones.

DEFINICIÓN 34. *Sea* $\sigma_\tau = (t_i, \tau_i)(t_j, \tau_j)...(t_k, \tau_k)...$ *una secuencia de disparos de transiciones. El vector de Parikh* $\overrightarrow{\sigma} : T \longrightarrow (\mathbb{Z}^+)^m$ *de* σ_τ *mapea cada* $t \in T$ *con el número de ocurrencias de* t *en* σ_τ.

CAPíTULO 2

Diagnóstico de faltas en SED

RESUMEN. *En este capítulo, se definen conceptos básicos sobre el diagnóstico de faltas, se propone una clasificación de faltas según su efecto y su duración en el sistema. Además, se revisan brevemente algunos trabajos relacionados con el diagnóstico en línea basado en modelos.*

2.1. Conceptos básicos sobre diagnóstico de faltas

2.1.1. Tipos de faltas.

Falta. Es el cambio inesperado del funcionamiento del sistema, es decir, cuando el sistema se comporta de una manera no deseada aunque esto no provoque necesariamente una falla [**Chen99**].

Las faltas pueden provocar un bajo desempeño del sistema, provocando que los costos se eleven, o que lleven a situaciones de riesgo para el sistema y para las personas que los manejan. Cuando el funcionamiento inesperado del sistema conduce a situaciones peligrosas decimos que se trata de una falla. En adelante, sólo nos referiremos a faltas, ya que esto abarca también el concepto de la falla.

Error. Es la diferencia entre el comportamiento especificado y el comportamiento real del sistema [**Jalote94**].

Tomando en cuenta la duración de las faltas en el sistema estas se puede clasificar como permanentes o intermitentes; tomando en cuenta el efecto que producen en el sistema, las faltas se pueden clasificar como bloqueantes o no bloqueantes. En seguida se definen estos tipos de faltas.

Faltas permanentes. Una vez que se presentan en el sistema no desaparecen por si solas, por lo que la recuperación de este tipo de faltas debe hacerse de manera externa. Note que este tipo de faltas no necesariamente bloquean el sistema.

Faltas intermitentes. Sus efectos sobre el sistema son los mismos que las faltas permanentes, pero una vez que aparecen en el sistema, pueden desaparecer sin la intervención de un sistema de recuperación. A menudo la frecuencia de estas faltas va en aumento hasta convertirse en una falta permanente, esto depende del origen de la falta. En ocasiones la falta es producida debido al efecto de algún agente externo, por lo que si este agente externo desaparece, la falta desaparecerá con el, cuando la falta es debida a un desgaste gradual de los componentes entonces es probables que esta falta evolucione a una falta permanente si no se repara el componente a tiempo [**Correcher05**].

Faltas bloqueantes. Cuando una falta bloqueante se presenta en el sistema provoca que el sistema no pueda continuar con sus actividades. Puede ser que el sistema se bloquee total o parcialmente.

Faltas no bloqueantes. Cuando una falta no bloqueante se presenta en un sistema no provoca que éste suspenda sus actividades, sino que puede continuar funcionando de manera errónea.

Los tipos de faltas clasificadas anteriormente pueden tener repercusiones temporales, es decir, pueden cambiar la fecha en que inician o termina las actividades; si esto sucede con respecto a las acciones observables entonces es posible usar el tiempo como un parámetro adicional para hacer más eficiente el proceso de diagnóstico.

2.1.2. Diagnóstico de faltas.

Diagnóstico de faltas. Es el proceso de detectar, aislar e identificar una falta.

Como se ve, el proceso de diagnóstico de una falta está compuesto por tres etapas, la detección de la falta, el aislamiento y la identificación de la misma.

Detección. Consiste en determinar las faltas presentes en el sistema.

En esta etapa del diagnóstico no se conoce el tipo de falta que ocurrió en el sistema ni su localización, únicamente se sabe que una falta ocurrió.

Aislamiento. Consiste en determinar la localización de la falta.

En la etapa de aislamiento se conoce que existe una falta, y se conoce su localización, la tercera etapa consiste en determinar el tipo de falta.

Identificación. Consiste en identificar el tipo, tamaño o naturaleza de la falta ocurrida en el sistema.

Diagnosticabilidad. Cuando en un sistema es posible detectar, aislar e identificar una falta en un tiempo finito, se dice que esta falta es diagnosticable; si esto se cumple para toda falta se dice que el sistema es diagnosticable o tiene la propiedad de diagnosticabilidad.

Diagnóstico basado en modelos. Es la detección, aislamiento e identificación de faltas en los componentes del sistema por medio de la comparación de las mediciones disponibles de un sistema con información a priori representada por un modelo matemático del sistema.

En el diagnóstico basado en modelos, las faltas son detectadas por medio de la diferencia entre las observaciones del sistema y el estimado de las observaciones hecho por medio del modelo matemático, a esta diferencia se le conoce como *residuo*. Para que cada una de las faltas sea diagnosticable es necesario que el error producido por cada falta genere un residuo diferente, es decir, debe ser posible asociar de manera única cada observación anormal con algún tipo de falta.

El **diagnóstico en línea** es un concepto ampliamente relacionado con el diagnóstico basado en modelos, en el cual el diagnóstico se realiza mientras el sistema está en operación.

En la figura 2.1.1 se muestra un esquema que representa la estructura del diagnóstico de faltas en línea basado en modelos.

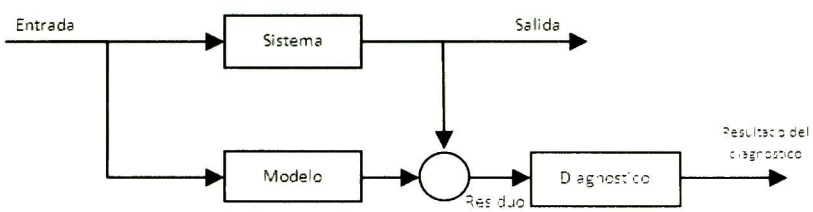


FIGURA 2.1.1. Esquema de diagnóstico en línea basado en modelos.

En la siguiente sección se describen brevemente algunos de los trabajos relacionados con el diagnóstico de faltas.

2.2. Trabajo relacionado.

En esta sección se resumen algunos trabajos publicados que tratan sobre el diagnóstico en línea basado en modelos. Estos trabajos se han clasificado de acuerdo al formalismo utilizado para modelar el sistema: autómatas finitos o redes de Petri.

2.2.1. Diagnóstico basado en modelos de autómatas finitos.

En **[Sampath95]** se trata el problema de diagnóstico de faltas mediante un enfoque que se basa en el estudio del lenguaje de salida generado por un sistema; este lenguaje se representa por medio de un autómata no determinista. A partir del modelo del sistema se construye un autómata finito determinista llamado diagnosticador, en el que se verifica la existencia de ciclos Fi-indeterminados. Éstos representan un conjunto de secuencias infinitas de eventos que producen la misma secuencia de salida, tal que el conjunto contiene secuencias con falta y secuencias sin falta.

En **[Hashtrudi05]** y **[Pan06]** se trata el problema de diagnóstico en línea de sistemas de eventos discretos temporizados, modelados con autómatas de Moore. El tiempo es representado por eventos llamados "ticks" Se define time-diagnosability. Un falta permanente es diagnosticable si existe un entero $Ti \geq 0$ tal que la falta puede ser detectada y aislada en a lo más Ti "ticks" Se dan condiciones necesarias y suficientes para que un autómata de Moore sea time-diagnosability, además se propone la construcción de un diagnosticador. Sin embargo el método que se sigue para la construcción del diagnosticador es exponencial.

En **[Debouk00]** se aborda el problema de diagnóstico de SED con información descentralizada. Se extiende la noción de diagnosticabilidad de sistemas centralizados para una arquitectura coordinada descentralizada. Existen varios subsistemas; para cada subsistema se diseña un diagnosticador local el cual envía información a un coordinador encargado de determinar la ocurrencia de una falta por medio se ciertas reglas definidas.

2.2.2. Diagnóstico en modelos de redes de Petri.

En **[Genc05]** se trata el problema de diagnóstico en línea de sistemas distribuidos modelados con redes de Petri. Se propone un algoritmo capaz de detectar y aislar las faltas ocurridas. El algoritmo se aplica a submodelos que comparten lugares y no comparten transiciones. Este algoritmo recopila información y la combina para recuperar el estado global del sistema y determinar si alguna falta ocurrió. Para hacer el analisis se extiende al grafo de alcanzabilidad de la RP y se usa el método propuesto por **[Sampath95]**, lo que hace que su complejidad sea exponencial.

En **[Lefevbre07]** se trata el problema de diagnóstico en sistemas modelados con redes de Petri. Se calcula el conjunto de lugares observables y se determina si con las observaciones proporcionadas por este conjunto es posible determinar el disparo de un conjunto de transiciones que representan faltas, esta noción es equivalente a la noción de evento-detectabilidad usada en **[Ruiz-Beltran07]**. Además se dan condiciones necesarias y suficientes para que una red de Petri sea diagnosticable. Estas condiciones se basan en las relaciones causales y los caminos dirigidos que parten de una transición de falta.

En **[Ruiz-Beltran07]** se propone una metodología para modelar faltas permanentes y se define formalmente la propiedad de *diagnosticabilidad entrada-salida* de un SED modelado mediante una RPI. Además se dan condiciones necesarias para que una RPI sea diagnosticable y se propone un esquema diagnosticador. A continuación se describe brevemente este trabajo, para más detalles ver **[Ruiz-Beltran07]**.

Modelado de faltas.

Las faltas se modelan por medio de lugares y transiciones agregados al modelo que representa funcionamiento normal del sistema (Q^N, M_0^N), de acuerdo al procedimiento del agoritmo 1.

El conjunto de lugares y transiciones agregados siguiendo este procedimiento se denota por P^F y T^F respectivamente.

Algoritmo 1 Modelado de faltas permanentes en RPI.

Entrada:
(Q^N, M_0^N). RPI que representa el funcionamiento normal del sistema.
P^R Conjunto de lugares apartir de los cuales puede ocurrir una falta.
Salida:
(Q, M_0). RPI que representa tanto el funcionamiento normal como el de falta.

1. Para cada lugar p_i^N que representa una operación a partir de la cual puede ocurrir una falta permanente, agregar una transición no manipulable t_f, un lugar de falta p_j^F, y los arcos $I(p_i^N, t_f)$ y $O(p_j^F, t_f)$.
2. Para cada lugar p_i agregado en el paso anterior hacer $\varphi(\bullet, p_i) = \varphi(\bullet, p_j)$, donde $p_j \in \bullet\bullet p_i$.
3. Para cada transición t_i agregada en el paso 1, hacer $\lambda(t_i) = \varepsilon$.

Se denota por (Q, M_0) a la RPI que representa tanto el funcionamiento normal como el de falta. (Q^N, M_0^N) indica el funcionamiento normal del sistema, es decir sin considerar T^F y P^F P^N es el conjunto de lugares que pertenecen a (Q^N, M_0^N) y T^N es el conjunto de transiciones que pertenecen a (Q^N, M_0^N). El conjunto de *lugares de riesgo* P^R está compuesto por los lugares p_i tal que $p_i \in \bullet T^F$ El conjunto de transiciones *post-riesgo* $T^R = \{P^R \bullet \cap T^N\}$.

La definición de diagnosticabilidad propuesta es la siguiente.

DEFINICIÓN 35. *Una RPI dada por* (Q, M_0) *es* diagnosticable entrada-salida *en* $k < \infty$ *pasos si y sólo si usando cualquier palabra* $\omega \in \Lambda^k(Q, M_f) \cup \Lambda_B(Q, M_f)$, *la información de* C, φ, λ *de* (Q, M_0) *son suficientes para distinguir la presencia de faltas en el SED.*

Donde $\Lambda^k(Q, M_f)$ denota el conjunto de todas las secuencias de entrada-salida de un tamaño mayor a k iniciando en el marcado de falla M_f y $\Lambda_B(Q, M_f)$ denota el conjunto de todas las secuencias de símbolos de entrada-salida que llevan a marcados de bloqueo iniciando en el marcado de falla M_f.

El siguiente teorema propuesto en **[Ruiz-Beltran07]** establece condiciones suficientes para que una RPI sea diagnosticable entrada-salida.

TEOREMA 1. *Sea* (Q, M_0) *una RPI con faltas permanentes, donde* (Q^N, M_0^N) *es una RPI segura, viva y evento-detectable. Si*

1. $\forall t_i \in T^R, \forall t_j \in T^N$ donde $t_i \neq t_j, D_H(t_i, t_j < \infty)$,
2. $\forall t_k \in T^R, {}^\bullet(t_k) = \{p_i^N\}$ debe cumplirse que $|\bullet(t_k)| = 1$ y $\lambda(t_k) \neq \varepsilon$

entonces (Q, M_0) es diagnosticable entrada-salida.

Donde D_H es la distancia relativa máxima como se define a continuación.

La distancia relativa $D_R(t_i, t_j)$ es el número de disparos de t_i cuando una marca se retiene en $\bullet t_j$. La distancia relativa máxima $D_H(t_i, t_j)$ en entre t_i y t_j es $max\{DR(t_i, t_j), DR(t_j, t_i)\}$.

La demostración se puede encontrar en **[Ruiz-Beltran07]**

EJEMPLO 4. *Considere la figura 2.2.1 donde las transiciones* t_6 *y* t_7 *representan faltas permanentes que bloquean el sistema. Cuando se alcanza un marcado donde una falta puede ocurrir, es decir se marca un lugar de riesgo, en este caso* p_3 *o* p_6, *entonces según la definición 35, en un número finito de pasos se deberá disparar la transición de post-riesgo* t_5 *o* t_3. *Cuando se marca* p_3 *entonces en un número finito de eventos el sistema sólo tendrá habilitada la transición* t_5

suponiendo que no ocurrió t_6 por lo que $\lambda(t_5)$ se deberá dar al sistema. Con la entrada $\lambda(t_5)$, se puede determinar si la transición de falta t_6 se disparó por medio del cambio producido en la salida según φ. Puesto que el sistema es evento-detectable se garantiza que el disparo de t_5 producirá algún cambio y que este cambio no se confunde con el cambio producido por el disparo de otra transición en el sistema. Si este cambio no se produce entonces se sabe que una falta ocurrió. Note que esto no sucede cuando se dispara t_7, el sistema puede disparar las transiciones t_5, t_4 indefinidamente por lo que la entrada $\lambda(t_3)$ puede no darse nunca y por lo tanto nunca saber si t_7 se disparó; cuando esto sucede se dice que t_3 y t_4 tienen una distancia relativa infinita, lo mismo que t_3 y t_5.

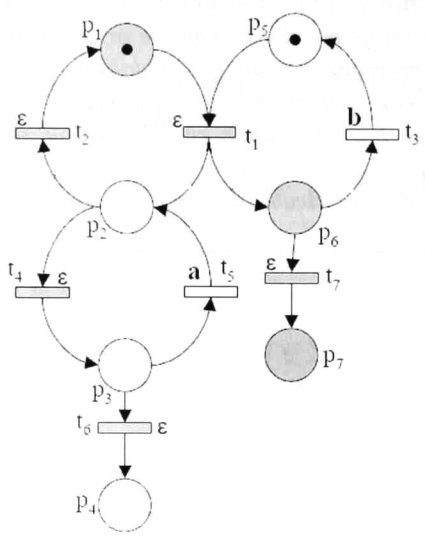


FIGURA 2.2.1. Diagnosticabilidad de faltas permanentes **[Ruiz-Beltran07]**.

CAPíTULO 3

Diagnosticabilidad de RPIT.

RESUMEN. *Este capítulo trata el problema del diagnóstico de faltas permanentes en modelos de redes de Petri interpretadas temporizadas. Se propone un método de modelado de faltas permanentes en RPIT, se define formalmente la diagnosticabilidad en RPIT y se propone una caracterización de RPIT que cumplen con esta propiedad. Además, se muestra como es posible extender el concepto de diagnosticabilidad entrada-salida en RPI propuesto en* **[Ruiz-Beltran07]** *para ser aplicado en RPIT. Por último se hace una comparación entre el concepto de diagnosticabilidad propuesto en este capítulo y la diagnosticabilidad entrada-salida.*

3.1. Modelado de faltas permanentes bloqueantes

Existen varios trabajos que abordan el problema de diagnóstico en sistemas de eventos discretos temporizados **[Tripakis02, Pan06, Jiroveanu06]**. Sin embargo, los algoritmos propuestos para verificar la propiedad de diagnosticabilidad son ineficientes para modelos grandes.

En esta sección se propone una extensión al método de modelado presentado en el capítulo anterior, para representar faltas permanentes en RPIT. Básicamente, la diferencia radica en que, en una RPIT no existen transiciones t_i, t_j tales $\lambda(t_i) = \varepsilon\iota$ y $\lambda(t_j) \neq \varepsilon\iota$ y $\bullet t_i = \bullet t_j \neq \emptyset$, por lo que es necesario tomar en cuenta esto en el modelado de las faltas.

El algoritmo 2 propone el método de modelado de faltas.

Algoritmo 2 Modelado de faltas.

Entrada:
(E^N, M_0^N). RPIT que describe el funcionamiento normal del sistema.
P^R Conjunto de lugares de riesgo de (E^N, M_0^N).
Salida:
(E, M_0). (E^N, M_0^N) con lugares y transiciones agregados que describe el funcionamiento normal y de falta del sistema.

---

1. Para todo lugar de riesgo $p_i \in P^R$ hacer.
   a) Agregar una transición t_f.
   b) Si existe $t_j \in p_i\bullet$ tal que $\lambda(t_j) = \varepsilon$ o $\lambda(t_j) \in \Sigma$, entonces hacer $\lambda(t_f) = \varepsilon$.
   c) Si existe $t_j \in p_i\bullet$ tal que $\lambda(t_j) = \varepsilon\iota$, entonces hacer $\lambda(t_f) = \varepsilon\iota$.
   d) Agregar un lugar p_f.
      1) Hacer $D(p_f) = 1$.
   e) Agregar los arcos $I(p_i, t_f)$ y $O(p_f, t_f)$.

El modelo obtenido siguiendo los pasos del algoritmo 2 representa tanto el funcionamiento normal, como el de falta del sistema. El conjunto de lugares y el conjunto de transiciones agregados en el algoritmo 2 se denota por P^F y T^F respectivamente.

(E, M_0) describe tanto el funcionamiento normal como el de falta. (E^N, M_0^N) indica el funcionamiento normal del sistema, es decir sin considerar T^F y P^F P^N es el conjunto de lugares que pertenecen a (E^N, M_0^N) y T^N es el conjunto de transiciones que pertenecen a (E^N, M_0^N). El conjunto de *lugares de riesgo* P^R está compuesto por los lugares p_i tal que $p_i \in \bullet T^F$ El conjunto de transiciones post-riesgo es $T^R = P^R \bullet \cap T^N$

El ejemplo siguiente muestra el seguimiento del algoritmo 2 para obtener un modelo que representa las posibles faltas.

EJEMPLO 5. *En la figura 3.1.1 se muestra un RPIT simple* (E^N, M_0^N), *donde* $\lambda(t_1) = \varepsilon$, $\lambda(t_2) = a_2$, $\lambda(t_3) = a_3$, $\lambda(t_4) = \varepsilon$, $\lambda(t_5) = \varepsilon\iota$, $\lambda(t_6) = a_6$ *y* $\lambda(t_7) = a$. *La función D se define así:* $\forall p_i D(p_i) = 1$. *La matriz* φ *asociada se muestra en la ecuación (3.1.1). Si los lugares* p_6 *y* p_7 *representan operaciones a partir de las cuales puede ocurrir una falta, entonces* $P^R = \{p_6, p_7\}$. *Siguiendo los pasos del algoritmo 2 se obtiene el modelo* (E, M_0) *de la firuga 3.1.2 que representa tanto el funcionamiento normal como el de falta. El conjunto de transiciones de falta es* $T^F = \{t_8, t_9\}$ *y el conjutno de transiciones post-riesgo es* $T^R = \{t_5, t_7\}$.

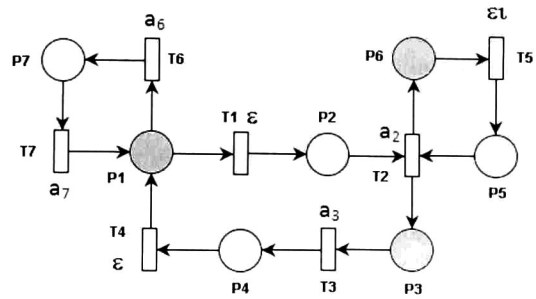


FIGURA 3.1.1. Modelo de RPIT.

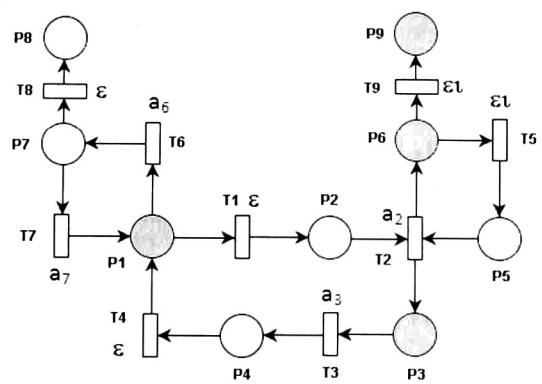


FIGURA 3.1.2. Modelo de RPIT con comportamiento de falta.

(3.1.1)
$$\varphi = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

3.2. T-diagnosticabilidad

Cuando en una RPIT con faltas permanentes modeladas como se muestra en la sección anterior es posible inferir la presencia de cualquier falta en un tiempo finito después de que ésta se produce, decimos que esta RPIT es diagnosticable. Este concepto se define formalmente a continuación.

DEFINICIÓN 36. *Un RPIT* (E, M_0) *es* T-diagnosticable *si y solo si, en un tiempo* $\tau < \infty$ *después de la ocurrencia de cualquier falta, es posible determinar la presencia de ésta basados en la información de* C, φ, λ, D *de* (E, M_0).

Como se ve en la definición anterior, T-diagnosticabilidad exige que en un tiempo finito se determine la presencia de cualquier falta; no toma en cuenta el número de eventos que pueden ocurrir después de una falta, como lo hace la diagnosticabilidad entrada-salida, en secciones siguientes se hace una comparación entre estos dos conceptos.

Antes de proponer una caracterización veamos un ejemplo.

EJEMPLO 6. *Retomando la RPIT de la figura 3.1.2. Supongamos que se alcanza un marcado* $M_k = [\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ ]$ *a partir del cual la transición de falta* t_9 *se puede disparar. Puesto que* $D(p_6) = 1$ *y* $\lambda(t_5) = \varepsilon\iota$*, entonces sabemos que* t_5 *se deberá disparar después de una unidad de tiempo sino ocurre* t_9*; puesto que* t_5 *es evento-detectable, entonces su disparo puede ser verificado. Si el disparo de* t_5 *se da sabemos que* t_9 *no ocurrió. Veamos ahora el caso de la falta* t_8*. Supongamos que se alcanza un marcado* $M_k = [\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ ]$ *donde* t_8 *puede ocurrir. Puesto que* $D(p_7) = 1$ *y* $\lambda(t_7) = a_7$*, sabemos que después de una unidad de tiempo la transición* t_7 *estará habilitada si no se produce* t_8*, sin embargo no sabemos el tiempo en el que se dará la entrada "*a_7*" por lo que no podemos saber en un tiempo finito si la transición* t_8 *se disparó.*

3.3. Caracterización de T-diagnosticabilidad

A continuación se propone una caracterización de RPIT que cumplen con la propiedad de T-diagnosticabilidad.

El siguiente teorema establece condiciones suficientes para una RPIT sea T-Diagnosticabilidad.

TEOREMA 2. *Sea* (E, M_0) *una RPIT con faltas permanentes, donde* (E^N, M_0^N) *es una RPI segura, viva y evento-detectable. Si* $\forall t_k \in T^R$*, se cumple que* $|\bullet t_k| = 1$ *y* $\lambda(t_k) = \varepsilon\iota$*, entonces* (E, M_0) *es T-diagnosticable.*

DEMOSTRACIÓN. Puesto que (E^N, M_0^N) es viva, entonces es viva por lugares **[Desel95]** es decir, $\forall p_i \in P^N$ donde $p_i \bullet \cap T^F \neq 0$ existe un marcado $M_s \in R(E^N, M_0^N)$ tal que $M_s(p_i) > 1$ (Específicamente $M_s(p_i) = 1$ puesto la red es segura). Por tanto existe una secuencia de transiciones σ_k tal que $M_0 \longrightarrow_{\sigma_k} M_k$ y $M_k(p_i) = 1$ donde $t_k \in p_i \bullet \cap T^N$ y $p_i \in P^R$ En M_k la transición de falta permanente $t_f \in (p_i) \bullet \cap T^F$ puede ser disparada y puesto que $\lambda(t_k) = \varepsilon\iota$ el disparo de t_k depende sólo del tiempo que dura la actividad p_i, entonces al término del tiempo $D(p_i)$, t_k se deberá disparar, en este momento dos casos pueden presentarse.

a) Si t_k se dispara, entonces un nuevo marcado M_x se alcanza, y debido a que la RPI es evento-detectable, entonces una nuevo vector de observación φM_x se alcanza, dado que $\varphi M_x \neq \varphi M_w$ el disparo de t_k puede ser detectado y se concluye que t_f no ocurrió. Donde $M_w \in R(E^N, M_k^N)$ tal que $M_w(p_i) = 1$.

b) Si t_f se dispara entonces la RPI alcanza un marcado de falta M_f, tal que M_f no habilita t_k y el marcado no evoluciona a M_x cuando el tiempo de disparo de t_k ha transcurrido. Por lo que no existe ningún cambio en el vector de observación φM_w con lo que se detecta la falta. Donde $M_w \in R(E^N, M_k^N)$ tal que $M_w(p_i) = 1$. □

Es fácil comprobar si las condiciones del teorema se cumplen en una RPIT. Además, el esquema diagnosticador propuesto en **[Ruiz-Beltran07]** se puede usar sin mayores cambios.

En las secciones siguientes se extiende el concepto de diagnosticabilidad entrada-salida a RPIT y se propone una caracterización de esta propiedad. Además se muestra la relación que existe entre T-diagnosticailidad y diagnosticabilidad entrada-salida.

3.4. Diagnosticabilidad entrada-salida en RPIT

Por comodidad reescribimos la definición de diagnosticabilidad entrada-salida presentada en el capítulo anterior en la siguiente definición. Vemos que aunque ésta está definida en términos de RPI, no es difícil reformularla en términos de RPIT.

DEFINICIÓN 37. *Una RPI dada por* (Q, M_0) *es* diagnosticable entrada-salida *en* $k < \infty$ *pasos si y sólo si usando cualquier palabra* $\omega \in \Lambda^k(Q, M_f) \cup \Lambda_B(Q, M_f)$, *la información de* C, φ, λ *de* (Q, M_0) *son suficientes para distinguir la presencia de faltas en el SED.*

Debido a que $\Lambda^k(Q, M_f)$ y $\Lambda_B(Q, M_f)$ se pueden aplicar directamente a RPIT, podemos definir el concepto de diagnosticabilidad entrada-salida para RPIT de la siguiente forma.

DEFINICIÓN 38. *Una RPI dada por* (E, M_0) *es* diagnosticable entrada-salida *en* $k < \infty$ *pasos si y sólo si usando cualquier palabra* $\omega \in \Lambda^k(E, M_f) \cup \Lambda_B(E, M_f)$, *la información de* C, φ, λ, D *de* (E, M_0) *son suficientes para distinguir la presencia de faltas en el SEDT.*

Observe que esta definición toma en cuenta la información que proporciona la función D para poder determinar si alguna falta ocurrió, lo que representa más información al momento de deducir la ocurrencia de una falta. A continuación se propone una caracterización para RPIT que son diagnosticables entrada-salida.

3.5. Caracterización de diagnosticabilidad entrada-salida en RPIT

Intuitivamente, si consideramos cualquier modelo de RPIT con comportamiento de falta y si sabemos que las transiciones post-riesgo se deben disparar en algún momento y éstas son evento-detectables, entonces podremos saber si cualquier falta ocurrió; a continuación se explica con detalle esto.

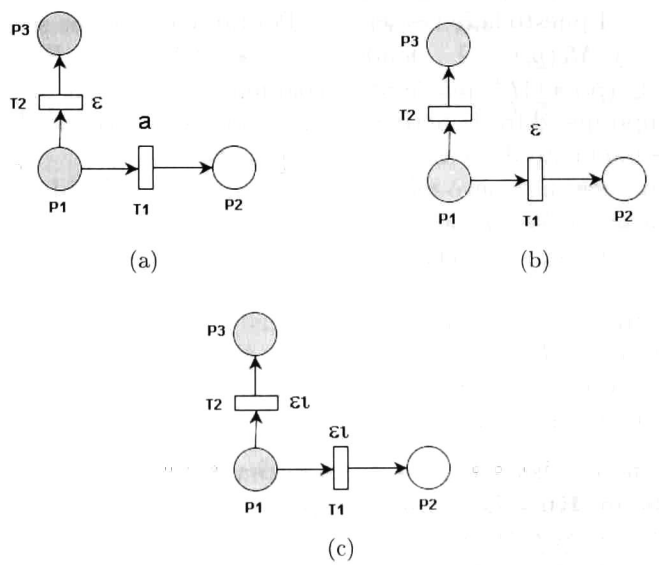


FIGURA 3.5.1. Situaciones de riesgo en una RPIT.

Considerando la figura 3.5.1.a que representa una sección de una RPIT en la que p_1 es un lugar de riesgo, t_2 es una falta, t_1 es una transición post-riesgo y p_2 es un lugar medible. Cuando una marca llega al lugar p_1 ésta no habilita alguna transición hasta que transcurren $D(p_1)$ unidades de tiempo. Una vez que transcurre este tiempo, las transiciones t_1 y t_2 están habilitadas. Para asegurar la diagnosticabilidad de la falta t_2 es necesario asegurar que la entrada "a" se dará al sistema; es posible asegurar esto si la distancia relativa máxima D_H entre t_1 y el resto de las transiciones es finita. En el caso de la figura 3.5.1.b, una vez que las transiciones t_1 y t_2 están habilitadas, aun cuando la distancia relativa máxima entre t_1 y el resto de las transiciones sea finita, no es posible determinar si t_1 no sea ha disparado o ya no se disparará debido a que ocurrió t_2, por lo que no es posible saber si t_2 se disparó. En el caso de la figura 3.5.1.c, cuando una marca se produce en p_1 se sabe que en $D(p_1)$ unidades de tiempo se deberá disparar t_1, si esto no ocurre será debido a que t_2 se disparó.

DEFINICIÓN 39. *$T^{a\varepsilon}$ es el conjunto de transiciones t tales que $\lambda(t) \neq \varepsilon\iota$.*

El teorema siguiente establecen condiciones suficientes para que una RPIT sea diagnosticable entrada-salida.

TEOREMA 3. *Sea (E, M_0) una RPIT con faltas permanentes, donde (E^N, M_0^N) es una RPIT segura, viva y evento-detectable. Si*

1. $\forall t_i \in T^R \cap T^{a\varepsilon}$ $\forall t_j \in T^N$ donde $t_i \neq t_j, D_H(t_i, t_j < \infty)$,
2. $\forall t_k \in T^R, {}^\bullet(t_k) = \{p_i^N\}$ debe cumplirse que $|\bullet(t_k)| = 1$ y $\lambda(t_k) \neq \varepsilon$

entonces (Q, M_0) es diagnosticable entrada-salida.

DEMOSTRACIÓN. La demostración de que las faltas $t_f \in (\bullet\bullet(T^R \cap T^{a\varepsilon})) \cap T^F$ son diagnosticables es igual a la demostración del teorema . La demostración de que las faltas $t_f \in (\bullet\bullet(T^R - T^{a\varepsilon})) \cap T^F$ son diagnosticables entrada-salida es inmediata de la definición de RPIT, ya que una vez que alcanza un marcado de riesgo p_i y transcurre el tiempo $D(p_i)$ se habilitan tanto las transiciones $p_i \bullet \cap T^N$ como la transición $p_i \bullet \cap T^R$ y alguna de éstas se debe disparar de inmediato. Si no ocurre una la falta $p_i \bullet \cap T^R$ entonces se debe disparar alguna transición que pertenece a $p_i \bullet \cap T^N$ y su disparo será detectado; si no se detecta el disparo de alguna transición que pertenece a $p_i \bullet \cap T^N$ se puede concluir que la transición de falta $p_i \bullet \cap T^R$ se disparó. □

En la siguiente sección se comparan los dos conceptos de diagnosticabilidad vistos en este capítulo.

3.6. Relación entre T-diagnosticabilidad y diagnosticabilidad entrada-salida

En esta sección veremos brevemente como se relacionan la T- Diagnosticabilidad y la diagnosticabilidad entrada-salida.

La T-diagnosticabilidad establece que en un tiempo finito debe ser posible determinar la presencia de cualquier falta, mientras que diagnosticabilidad entrada-salida establece que esto debe ocurrir en un número finito de pasos. A continuación se muestra esto con la ayuda de la RPIT de la figura 3.1.2.

Verificando la propiedad de T-diagnosticabilidad vemos que:

t_8 no es T-diagnosticable.
t_9 es T-diagnosticable.

Verificando la propiedad de diagnosticabilidad entrada-salida se tiene lo siguiente:

- t_8 Es diagnosticable entrada-salida.
- t_9 Es diagnosticable entrada-salida.

Vemos que t_8 no es T-diagnosticable pero si es diagnosticable entrada-salida, mientras que t_9 cumple ambas propiedades, es decir la RPIT de la figura 3.1.2 no es T-diagnosticable y es diagnosticable entrada-salida.

Basándonos en los teoremas anteriores en este capítulo y en este ejemplo podemos deducir que si una falta es T-diagnosticable entonces es diagnosticable entrada-salida. El corolario siguiente establece esto.

COROLARIO 3.6.1. *Sea una RPIT con faltas permanentes. Si una falta t_f es T-diagnosticable entonces t_f es diagnosticable entrada-salida.*

DEMOSTRACIÓN. De la definición de T-diagnosticabilidad se tiene que una falta t_f se debe detectar en un tiempo finito τ después que se presenta. Puesto que en una RPIT se cumple que $\forall p \in P, D(p) > 0$, entonces no puede ocurrir un número infinito de pasos en el lapso de tiempo que inicia cuando ocurre t_f y termina τ unidades de tiempo más tarde; esto cumple con la definición de diagnosticabilidad entrada-salida que establece que se debe ser capaz de determinar la presencia de cualquier falta en un número finito de pasos. □

Como se puede ver, el problema de verificar la propiedad de T-diagnosticabilidad cuando las transiciones post-riesgo son evento-detectables y se disparan en un tiempo finito no es complicado. Sin embargo, cuando la RPIT no es evento-detectable aún es posible verificar esta propiedad aunque el proceso resulta más complejo; esto también sucede cuando se intenta verificar diagnosticabilidad entrada-salida en una RPIT que no es evento-detectable. Intuitivamente, si se propone una caracterización que permita verificar polinomialmente la propiedad de diagnosticabilidad entrada-salida en RPI no evento-detectables, entonces verificar la propiedad de T-diagnosticabilidad es más sencillo. El capítulo siguiente estudia este nuevo planteamiento.

CAPíTULO 4

Diagnosticabilidad entrada-salida

RESUMEN. *En este capítulo, se trata el problema de diagnóstico de faltas permanentes en modelos de redes de Petri interpretadas que no cumplen con la propiedad de evento-detectabilidad.*

Se proponen caracterizaciones de diagnosticabilidad entrada-salida para ME y GM no evento-detectables.

4.1. RPI diagnosticables no evento-detectables.

Para verificar la diagnosticabilidad entrada-salida de un RPIT que no es evento-detectable es necesario analizar las secuencias de salida producidas, las cuales deben permitir saber cuándo se alcanzó un lugar de riesgo y garantizar que todas las secuencias de salida posibles a partir de un marcado de riesgo permitan determinar si ésta ocurrió, en un número de pasos finito.

Los siguientes ejemplos muestran dos casos de RPI no evento-detectables en los que es posible determinar la ocurrencia de las faltas.

EJEMPLO 7. *Considere la RPI de la figura 4.1.1 con* $\lambda(t_1) = a$, $\lambda(t_2) = b$, $\lambda(t_3) = c$, $\lambda(t_4) = d$, *y* $\lambda(t_5) = f_1$, *con* p_2 *como el único lugar medible. Si consideramos el marcado inicial* $M_0 = [\ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$, *con la secuencia de entrada "da" se deberá alcanzar el marcado* $M_0 = [\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ ]$ *y obtener una observación, si esto no ocurre será debido a que* f_1 *ocurrió, y por tanto el marcado de la red es* $M_k = [\ 0\ \ 0\ \ 0\ \ 0\ \ 1\ ]$. *Así es posible determinar la presencia de la falta sin necesidad de la condición de evento-detectabilidad.*

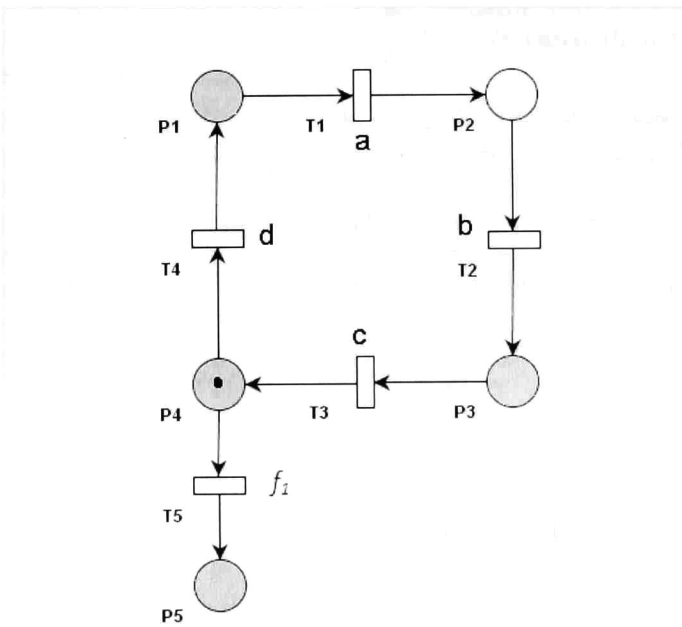


FIGURA 4.1.1. ME no evento-detectable diagnosticable entrada-salida.

EJEMPLO 8. *En la figura 4.1.2 se muestra un RPI en la que* $\lambda(t_i) = a_i$. *En un número de pasos finito después de que ocurre* t_9 *es posible determinar la presencia de la falta; esto se logra verificando el disparo de la transición medible* t_3 *tras dar la secuencia de entrada "*a_1a_3*" Lo mismo sucede con el lugar de riesgo* p_3, *la secuencia de entrada "*a_2a_6*" y el disparo de* t_6. *Las entradas* a_1, a_2, a_3, a_6 *se deben dar en un número de pasos finito ya que la distancia relativa máxima entre las transiciones* t_1, t_3, t_4, t_6 *es finita con respecto al cualquier otra transición.*

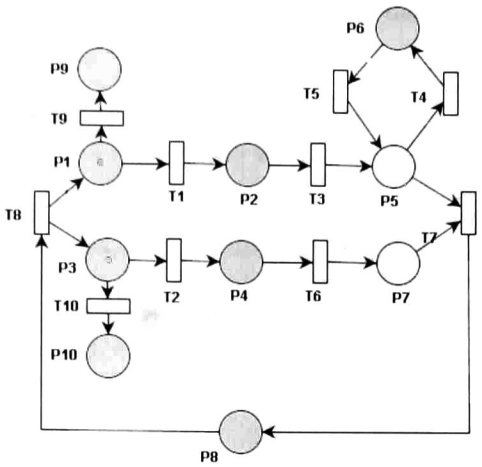


FIGURA 4.1.2. RPI no evento-detectable diagnosticable entrada-salida.

Como vemos en los ejemplos anteriores, una caracterización de RPI diagnosticables no evento-detectables tendría una aplicación mucho mayor, ya que no es necesario que las transiciones post-riesgo sean evento-detectables; sin embargo esto provoca que el análisis sea mucho más complejo. En las siguientes secciónes se proponen caracterizaciones de RPI con el comportamiento de ME y GM que son diagnosticables entrada-salida.

4.2. Diagnosticabilidad en ME

En esta sección se propone una caracterización para ME vivas y seguras diagnosticables entrada-salida en la que se ha relajado la condición de evento-detectabilidad para las transiciones post-riesgo. Esta caracterización sólo considera el caso cuando el disparo de las transiciones está *determinado*; a continuación se explica esto.

DEFINICIÓN 40. *Decimos que el disparo de una transición t_i está determinado en una ME, si el disparo de t_i no se confunde con el disparo de alguna otra transición, es decir*

- Si $\forall t_j \in T$ tal que $\lambda(t_j) = \varepsilon$ se cumple que $\varphi C(\bullet, t_j) \neq \mathbf{0}$.
- Si $\exists t_i, t_j$ tal que $\bullet t_i = \bullet t_j \neq \emptyset$ y $\lambda(t_i) = \lambda(t_j) = \varepsilon$ entonces $\varphi C(\bullet, t_i) \neq \varphi C(\bullet, t_j)$.

En la RPI de la figura 4.2.1.a, el disparo de t_1 y t_2 está totalmente determinado por la función λ, aún cuando la función φ no asigna sensores a ninguno de los lugares. En la figura 4.2.1.b, con la función φ como se muestra en la ecuación (4.2.1), el disparo de t_1 y t_2 está totalmente determinado por las observaciones producidas por cada una de las transiciones, ya que $\varphi C(\bullet, t_1) = \begin{bmatrix} 1 & 0 \end{bmatrix}^T$ y $\varphi C(\bullet, t_2) = \begin{bmatrix} 0 & 1 \end{bmatrix}^T$ por lo que $\varphi C(\bullet, t_1) \neq \varphi C(\bullet, t_2)$. En 4.2.1.c no es posible determinar el disparo de t_1 a menos que se dé la entrada "a" y no se obtenga la observación esperada.

$$\varphi = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.2.1}$$

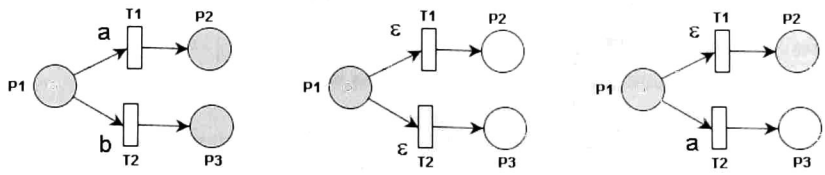


FIGURA 4.2.1. Detección de disparo de transiciones en conflicto estructural.

El ejemplo siguiente muestra qué pasa cuando existen transiciones en conflicto estructural que no están determinadas.

EJEMPLO 9. *Vea la RPI de la figura 4.2.2 donde las transiciones t_1 y t_2 no son manipulables. Los lugares sombreados son lugares no medibles. Con la secuencia de entrada "ac" a partir del estado actual, tres casos podrían ocurrir:*

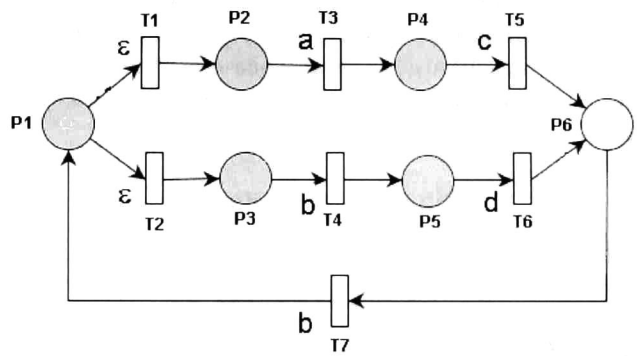


FIGURA 4.2.2. Disparo no determinado.

- t_1 se disparó antes de dar la entrada "ac" alcanzando el marcado $M = [\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ ]$. Con la entrada "$ac$" el sistema alcanza el nuevo estado $M = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ ]$
- t_2 se disparó antes de dar la entrada "ac" llevando al sistema al estado $M = [\ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ ]$. Con la entrada "$ac$" el sistema no evoluciona.
- No se disparó alguna de las transiciones t_1, t_2. Al dar la entrada "ac" el sistema no evoluciona.

Debido a que el disparo de las transiciones en *conflicto estructural* t_1, t_2 no se puede controlar o inferir a partir de las observaciones (no está determinado), no es posible saber el estado real del sistema, a menos que se den las entradas correspondientes a los posibles estados del sistema. En el ejemplo anterior se podría inferir el estado del sistema dando las secuencias de entrada "ac", "bd" y revisando las observaciones obtenidas. Sin embargo, en esta tesis no se hace alguna suposición sobre el módulo encargado de dar las entradas al sistema, y el proceso de diagnóstico se considera

pasivo. Por lo que solo se considera el caso cuando se sabe cuál transición en *conflicto estructural* se disparó.

4.2.1. Caracterización de diagnosticabilidad.

Intuitivamente, la ocurrencia de una falta se puede diagnosticar si ésta produce un cambio en la secuencia de observaciones, y dicho cambio no se confunde con la observación producida por otra falta o con el funcionamiento normal del sistema. Por ejemplo, si analizamos la RPI de la figura 4.2.3 con la función φ que se muestra en la ecuación (4.2.2) y M_0 como se muestra en la figura es posible detectar el disparo de t_1 o de t_4. Si se dispara t_1 entonces se alcanza un marcado M con $M(p_2) = 1$. El disparo de t_2 también es posible inferirlo a partir de las observaciones; cuando éste se da, se alcanza el marcado $M(p_3) = 1$, el cual marca un lugar de riesgo. Con la secuencia de entrada "ab" a partir del último marcado se podrá saber si la marca se "perdió" debido al disparo de t_{10} o en realidad se alcanzó el marcado $M(p_4) = 1$ al obtener la observación correspondiente al disparo de t_7. Algo similar sucede con la transición de falta t_9, ya que es posible saber si se diparó t_4 por medio de las observaciones; puesto que t_5 es manipulable, entonces con la entrada $\lambda(t_5)$ es posible vefiricar su disparo.

(4.2.2)
$$\varphi = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

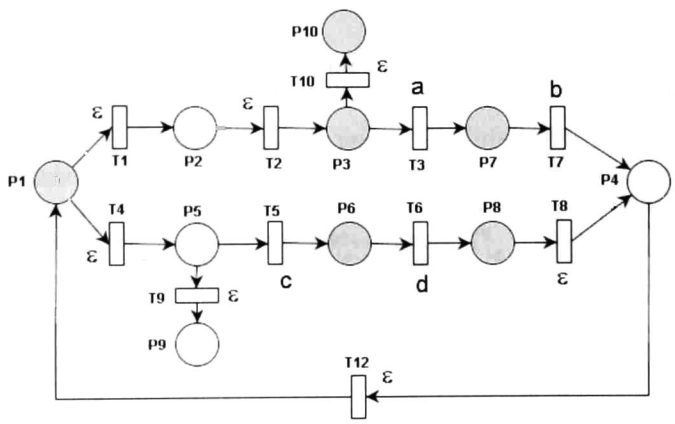
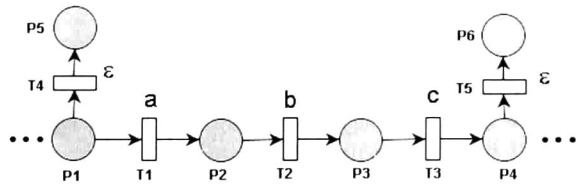
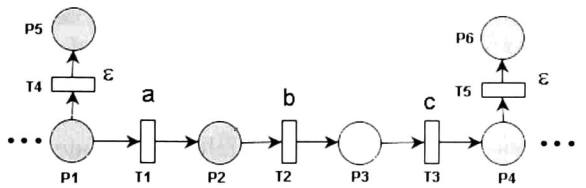


FIGURA 4.2.3. RPI Diagnosticable.

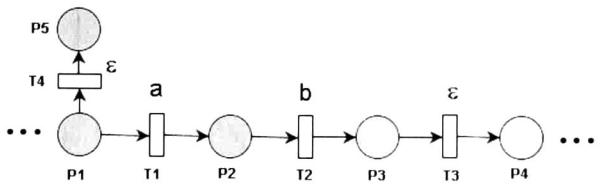
En la figura 4.2.3 se ve que no existen caminos dirigidos no observables entre los lugares de riesgo p_3 y p_5; esto permite aislar cada uno de las faltas asociadas a estos lugares de riesgo. Además, no existen caminos dirigidos no observables entre estos lugares de riesgo y alguna transición no manipulable o un T-semiflujo no observable, lo que garantiza que después de marcar un lugar de riesgo se deberá disparar una transición medible. Esto se puede observar mejor en la figura 4.2.4.



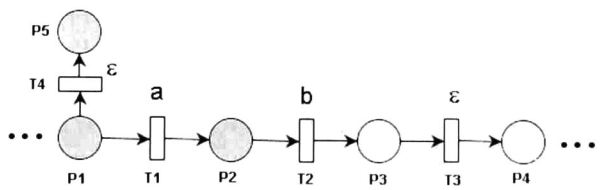
(a)



(b)



(c)



(d)

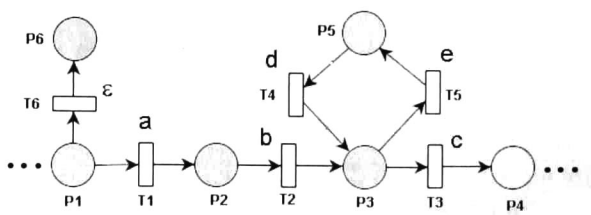


FIGURA 4.2.4. Caminos dirigidos.

En 4.2.4.a existe un camino dirigido $\rho = p_1t_1p_2t_2p_3t_3$ que va del lugar de riesgo p_1 al lugar de riesgo p_4. Este camino dirigido no contiene transiciones medibles, por lo que, si se dispara t_4 o t_5 no será posible determinar cuál de éstas se disparó.

- Si se considera 4.2.4.b el camino dirigido $\rho = p_1t_1p_2t_2p_3t_3$ contiene las transiciones medibles t_2 y t_3 por lo que, cuando se dé la secuencia de entrada "ab" a partir de un marcado $M(p_1) = 1$ se podrá determinar si t_4 se disparó considerando la observación producida por la entrada b.
- En 4.2.4.c se tiene el camino dirigido $\rho = p_1t_1p_2t_2p_3$ que va del lugar de riesgo p_1 a la transición no manipulable t_3, el cual no contiene transiciones medibles; a partir de un marcado $M(p_1) = 1$ si se da la entrada "ab" no es posible determinar en un tiempo finito si se disparó t_4 ya que el disparo de t_3 puede no darse en un tiempo finito debido a que no es manipulable.
- Considerando 4.2.4.d, existe el camino dirigido $\rho = p_1t_1p_2t_2p_3$ que va del lugar de riesgo p_1 a la transición no manipulable t_3; el camino dirigido contiene la transición medible t_2, con lo que al aplicar la entrada "ab" a partir del marcado $M(p_1) = 1$ es posible determinar si t_4 se disparó revisando la observación producida cuando se da la entrada b.
- En la figura 4.2.4.e existe el camino dirigido $\rho = p_1t_1p_2t_2p_3$ que va del lugar de riesgo p_1 al T-componente $||X_i||$ inducido por el T-semiflujo no observable compuesto por las transiciones t_4 y t_5, esto nos indica que "c" podría no darse cuando $M(p_3) = 1$ y en consecuencia no saber si t_6 se disparó.

De los escenarios anteriormente descritos podemos ver que es posible detectar que ocurrió una falta cuando existe un indicio de que el camino que se originà en un lugar de riesgo se está ejecutando.

En el teorema siguiente se contempla lo anterior para proponer una caracterización; antes se define un concepto usado en el teorema.

DEFINICIÓN 41. *Denotamos con $\rho_f(p_i)$ a un camino dirigido que inicia en un lugar de riesgo p_i y termina en el primer nodo n tal que $n\bullet$ es un lugar de riesgo o $\exists t_i \in n\bullet$ tal que $\lambda(t_i) = \varepsilon$.*

En el teorema siguiente se establece que si en un máquina de estados donde el disparo de las transiciones está determinado se cumple que, no existen T-semiflujos no observables y para todo lugar de riesgo no existe camino dirigido $\rho_f(p_i)$ sin transiciones medibles, entonces es posible detectar y aislar cualquier falta ocurrida en el sistema.

TEOREMA 4. *Sea (Q^N, M_0^N) una ME viva y segura con faltas permanentes, donde el disparo de las transiciones está determinado. Si*

- $\nexists X_i$ tal que $\forall t_i \in ||X_i||$, $\varphi C(\bullet, t_i) = 0$
- $\forall p_i \in P^R, \nexists \rho_f(p_i)$ tal que $\forall t_i \in \rho_f(p_i)$ se cumple que $\varphi C(\bullet, t_i) = 0$

entonces (Q, M_0) es diagnosticable entrada-salida.

DEMOSTRACIÓN. Puesto que el disparo de las transiciones está determinado entonces es posible saber en todo momento cual es el marcado del sistema cuando no se produce alguna falta. En particular se sabe cuando un lugar de riesgo fue marcado. Si se alcanza un marcado $M_k(p_i) = 1$ donde p_i es un lugar de riesgo, entonces tenemos dos casos posibles:

Caso 1. Se dispara la falta relacionada con el lugar p_i. Entonces un nuevo marcado $M_f(p_j) = 1$ es alcanzado. Donde $p_j = (p_i\bullet \cap T^F)\bullet$. Por lo que, las transiciones $t_j \in p_i\bullet \cap T^N$ no están habilitadas. Puesto que todo camino $\rho_f(p_i)$ contiene al menos una transición t_i tal que $\varphi C(\bullet, t_i) \neq 0$ y no existe

T-semiflujo no observable, entonces se deberán dar las entradas $\lambda(t_j)$ para todo $t_j \in \rho_f(p_i)$ para algún camino dirigido $\rho_f(p_i)$; cuando se da la entrada $\lambda(t_l)$ para $t_l \in \rho_f(p_i)$ tal que $\varphi C(\bullet, t_l) \neq 0$ entonces se tiene que la transición t_l no se dispara debido al disparo de $(p_i \bullet \cap T^F)$ por lo que no se producirá la observación esperada. Con lo que se concluye que $(p_i \bullet \cap T^F)$ se disparó.

Caso 2. No se dispara la falta relacionada con el lugar p_i. Entonces al dar las entradas correspondientes a una transición $t_l \in \rho_f(p_i)$ tal que $\varphi C(\bullet, t_l) \neq 0$ se producirá la observación esperada. Con lo que se concluye que $(p_i \bullet \cap T^F)$ no se disparó. □

Basado en este resultado, a continuación se presenta el algoritmo 3 para determinar la existencia de caminos dirigidos $\rho_f(p_i)$ que no contienen transiciones medibles.

Algoritmo 3 Determinar si existe $\rho_f(p_i)$ sin transiciones medibles para p_i de riesgo.

Entrada:
p_i Lugar de riesgo.
Salida:
Existe camino dirigido $\rho_f(p_i)$ sin transiciones medibles.

1. Sea Y_P un vector en $\{0,1\}^n$ (donde n es el número de lugares en (Q^N, M_0^N)), hacer $Y_P = \vec{0}$.
2. Para p_i, hacer $Y_P(i) = 1$.
3. $Y_T = Y_P^T C^-$
4. Repetir m veces (donde m es el número de transiciones en (Q^N, M_0^N)).
   a) Para todo $Y_T(i) \neq 0$ hacer
      1) Si $\lambda(t_i) = \varepsilon$ entonces "Existe camino dirigido $\rho_f(p_i)$ sin transiciones medibles"
      2) Si $t_i \bullet \cap P^R \neq 0$ y $\varphi C(\bullet, t_i) = 0$ entonces "Existe camino dirigido $\rho_f(p_i)$ sin transiciones medibles"
      3) Si $\varphi C(\bullet, t_i) \neq 0$ hacer $Y_T(i) = 0$
   b) Si $Y_T(i) = 0$ para toda t_i entonces.
      1) "No existe $\rho_f(p_i)$ sin transiciones medibles"
      2) Terminar.
   c) $Y_T = Y_T \cdot (C^{+T} \cdot C^-)$.

EJEMPLO 10. *Considere la RPI de la figura 4.2.5 con la función φ como se muestra en la ecuación (4.2.3) y $\lambda(t_8) = \varepsilon$, $\lambda(t_{13}) = \varepsilon$, $\lambda(t_{15}) = \varepsilon$ y $\lambda(t_i) = a_i$ para cualquier otra transición. El seguimiento de los pasos de este algoritmo para verificar la existencia de $\rho_f(p_i)$ no medibles en la RPI se muestra en el apendice A. Vemos que esta RPI no contiene $\rho_f(p_i)$ no medibles.*

$$\varphi = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4.2.3}$$

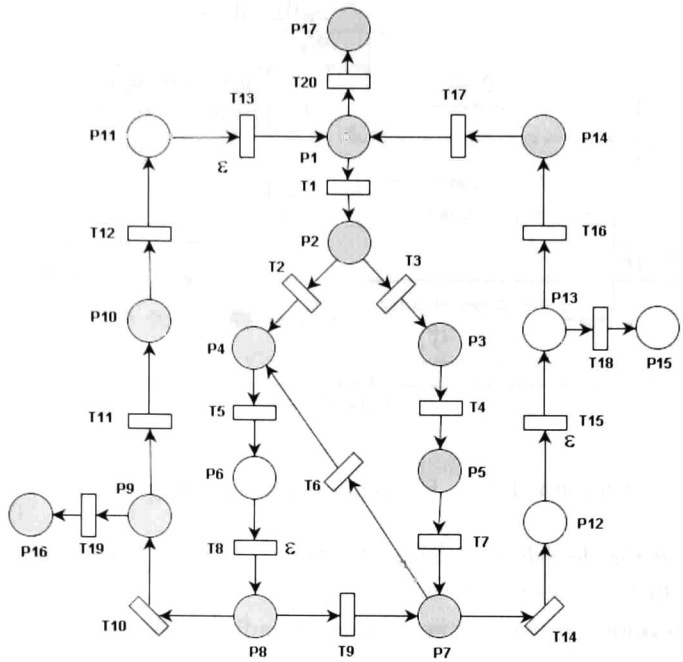


FIGURA 4.2.5. ME

En la siguiente sección se propone un esquema diagnosticador para ME diagnosticables.

4.2.2. Esquema de diagnóstico.

A continuación se propone un esquema diagnosticador para ME diagnosticables entrada-salida.

El esquema diagnosticador mostrado en la figura 4.2.6 está compuesto por:

- El *modelo del sistema* (Q, M_0)
- El *modelo diagnosticador* (Q^D, M_0^D)
- El módulo de *detección de eventos*
- El módulo *detección y localización* de faltas

El modelo del sistema representa tanto el funcionamiento normal como el de falta (Q, M_0). El modelo diagnosticador (Q^D, M_0^D) es el modelo normal del sistema (Q^N, M_0^N), donde la función λ se modifica de la siguiente manera. $\forall t_i$ tal que $\lambda(t_i) = \varepsilon$ en el (Q^N, M_0^N) hacer $\lambda(t_i) = a$ donde "a" no está asignada a otra transición. La función λ así modificada se denota por λ'. El marcado de (Q^D, M_0^D) de denota con M_k^D.

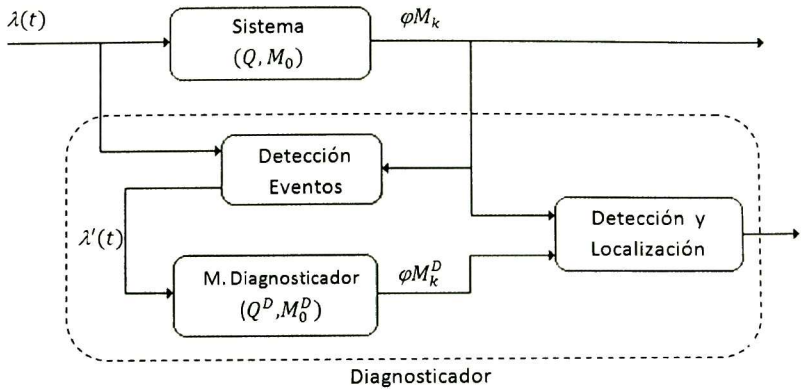


FIGURA 4.2.6. Esquema diagnosticador en ME.

El módulo de detección de eventos y el módulo de detección y localización son procedimientos basados en los algoritmos 4 y 5 respectivamente.

El módulo de detección de eventos se ejecuta cuando se da una nueva entrada a (Q, M_0) o cuando existe un cambio en la salida del sistema. Si se da una entrada al sistema ésta se da al modelo diagnosticador. Si existe un cambio en la salida del sistema y no se produjo una entrada se calcula la transición que puede producir este cambio en el modelo diagnosticador y está habilitada, y se da la entrada $\lambda'(t)$ correspondiente a la transición calculada. Esta estrategia se resume en el algoritmo siguiente.

Algoritmo 4 Detección de eventos en ME.

Entrada:
$\varphi(M_k)$-Vector de observación del sistema.
$\lambda(t)$- Símbolo de entrada.
Salida:
$\lambda'(t)$- Símbolo de entrada del modelo diagnosticador.

1. Si $\lambda(t)$ se da como entrada, entonces
   a) $\lambda'(t)$ tal que $\lambda'(t) = \lambda(t)$ se da como entrada a (Q^N, M_0^N).
2. Si $\varphi(M_k) - \varphi(M_{k-1}) \neq 0$ y no existe entrada el sistema.
   a) Dar la entrada $\lambda'(t_i)$ a (Q^D, M_0^D) tal que $\varphi(M_k) - \varphi(M_{k-1}) = \varphi C(\bullet, t_i)$ y t_i está habilitada en (Q^D, M_0^D).

El módulo de detección y localización de faltas se encarga de determinar la causa de la existencia de un error. Si un lugar de riesgo se marca, éste se guarda hasta determinar si ocurrió la falta asociada. Cuando se produce un cambio en el vector de observación del modelo diagnosticador se verifica la existencia de un error con respecto al vector de observación del sistema. En caso de no existir error se borra el lugar de riesgo de p. Si el error es diferente de cero se determina la existencia de una falta en el sistema.

Algoritmo 5 Detección y localización de faltas.

Entrada:
M_k^D Marcado del modelo diagnosticador
$\varphi(M_k^D)$ - Observación del modelo diagnosticador.
$\varphi(M_k)$ - Observación del sistema.
Salida:
t_f Falta ocurrida.
M Marcado de falta.

1. Si $M_k^D(p_i) = 1$ donde p_i es un lugar de riesgo.
   a) $p = p_i$
2. Si $\varphi(M_k^D) \neq \varphi(M_{k-1}^D)$ y $p = p_i$ para algún lugar de riesgo p_i
   a) $E_k = \varphi(M_k) - \varphi(M_k^D)$
   b) Si $E_k = 0$ entonces
      1) $p = \emptyset$
   c) Si $E_k \neq 0$
      1) $t_i \in p\bullet \cap T^F$ ocurrió y $M(t_i\bullet) = 1$ es el marcado de falta.

En el ejemplo siguiente se explica el funcionamiento del esquema diagnosticador.

EJEMPLO 11. *Considere la RPI de la figura 4.2.5; el funcionamiento del módulo de detección y localización de faltas es el siguiente. Considerando el caso cuando se da la secuencia de entrada "$a_1a_3a_4a_7a_{14}a_{16}$" al sistema y se produce la falta t_{18}. El marcado inicial de (Q, M_0) y (Q^D, M_0^D) es*

$$M_0 = [\ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_0^D = [\ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- Paso 1. Puesto que M_0^D marca el lugar de riesgo p_1 entonces $p = p_1$.
  Cuando se da la entrada a_1 al sistema, ésta también se da a (Q^D, M_0^D). Los marcados alcanzados son

$$M_1 = [\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_1^D = [\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

  El vector de observación $\varphi(M_0^D)$ es $[\ 0\ \ 0\ \ 0\ \ 0\ ]$ y $\varphi(M_1^D)$ es $[\ 0\ \ 0\ \ 0\ \ 0\ ]$ por lo que el paso 2 no se cumple.
  Con la entrada a_3, (Q, M_0) y (Q^D, M_0^D) alcanzan los marcados

$$M_2 = [\ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_2^D = [\ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- El vector de observación $\varphi(M_1^D)$ es $[\ 0\ \ 0\ \ 0\ \ 0\ ]$ y $\varphi(M_2^D)$ es $[\ 0\ \ 0\ \ 0\ \ 0\ ]$ por lo que el paso 2 no se cumple.
  Con la entrada a_4, (Q, M_0) y (Q^D, M_0^D) alcanzan los marcados

$$M_3 = [\ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_3^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- El vector de observación $\varphi(M_2^D)$ es $[\ 0\ \ 0\ \ 0\ \ 0\ ]$ y $\varphi(M_3^D)$ es $[\ 0\ \ 0\ \ 0\ \ 0\ ]$ por lo que el paso 2 no se cumple.

  Con la entrada a_7, (Q, M_0) y (Q^D, M_0^D) alcanzan los marcados

$$M_4 = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_4^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- El vector de observación $\varphi(M_3^D)$ es $[\ 0\ \ 0\ \ 0\ \ 0\ ]$ y $\varphi(M_4^D)$ es $[\ 0\ \ 0\ \ 0\ \ 0\ ]$ por lo que el paso 2 no se cumple.

  Con la entrada a_{14}, (Q, M_0) y (Q^D, M_0^D) alcanzan los marcados

$$M_5 = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_5^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ ]$$

  El vector de observación $\varphi(M_4^D)$ es $[\ 0\ \ 0\ \ 1\ \ 0\ ]$ y $\varphi(M_5^D)$ es $[\ 0\ \ 0\ \ 1\ \ 0\ ]$ y $p = p_1$ por lo que el paso 2 se cumple.

  - En 2.a se calcula el error. $E_k = \varphi(M_5^D) - \varphi(M_5) = [\ 0\ \ 0\ \ 1\ \ 0\ ] - [\ 0\ \ 0\ \ 1\ \ 0\ ] = 0$ por lo que $p = \emptyset$ (no se produjo t_{20}).

  Si se da la entrada a_{16} en este momento tanto, el sistema como el modelo diagnosticador permanecerán en el mismo estado debido a que aún no se detecta el disparo de t_{15} la cual es una transición no manipulable.

  Una vez que el disparo de t_{15} se produce en el sistema y es detectado por el módulo de detección de eventos, se alcanza el marcado

$$M_6 = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_6^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$$

  Paso 1. Puesto que M_6^D marca el lugar de riesgo p_{13} entonces $p = p_{13}$.

  En el estado actual del sistema suponemos que se dispara t_{18}. Por lo que el marcado del sistema es el siguiente

$$M_{6'} = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ ]$$

Y el vector de observación es $\varphi(M_{6'}) = [\ 0\ \ 0\ \ 0\ \ 1\ ] = \varphi(M_6) = \varphi(M_6^D)$
Cuando la entrada a_{16} se da, (Q, M_0) y (Q^D, M_0^D) alcanzan los marcados

$$M_{6'} = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ ]$$

$$M_7^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ ]$$

El vector de observación $\varphi(M_6^D)$ es $[\ 0\ \ 0\ \ 0\ \ 1\ ]$ y $\varphi(M_7^D)$ es $[\ 0\ \ 0\ \ 0\ \ 0\ ]$ y $p = p_{13}$ por lo que el paso 2 se cumple.

- En 2.a se calcula el error. $E_k = \varphi(M_{6'}) - \varphi(M_7^D) = [\ 0\ \ 0\ \ 0\ \ 1\ ] - [\ 0\ \ 0\ \ 0\ \ 0\ ] = [\ 0\ \ 0\ \ 0\ \ 1\ ] \neq 0$.

- En el paso 2.c. $p_{13} \bullet \cap T^F = t_{18}$ se disparó. El marcado del sistema es

$$M_f = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ ]$$

4.3. Diagnosticabilidad en GM

Es esta sección se trata la diagnosticabilidad de faltas permanentes en redes de Petri cuyo funcionamiento normal (Q^N, M_0^N) es un grafo marcado vivo y seguro en el que no existen transiciones no manipulables. La ausencia de transiciones no manipulables no se considera restrictiva, ya que en un grafo marcado no existen lugares en *conflicto estructural*, por lo que la ausencia de transiciones no manipulables sólo afecta el tiempo en que se dispara una transición.

El tiempo en que se puede disparar una transición no manipulable está en el intervalo de $[0, \infty]$ ya que ésta se considera un evento interno; sin embargo, si una transición puede tardar un tiempo infinito en ejecutase, esto implica que el GM se bloquee de manera indefinida, por lo que es realista suponer que toda transición se dispara en un tiempo finito. Además se supone que cada lugar medible tiene asociado un sensor diferente.

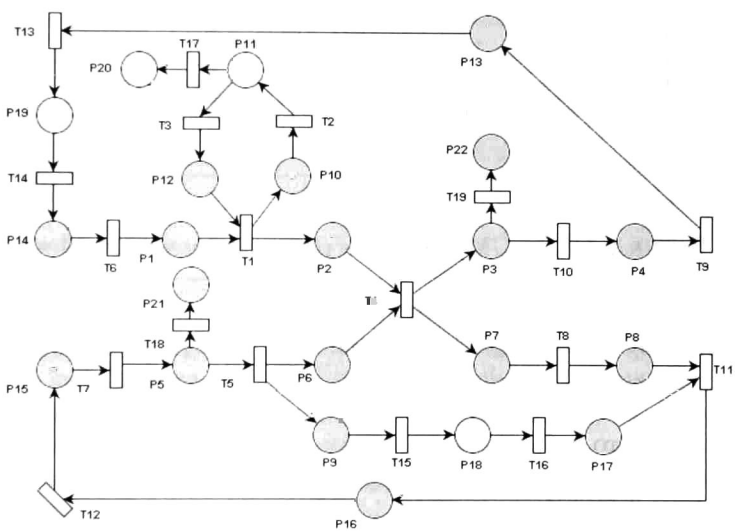


FIGURA 4.3.1. GM no evento-detectable diagnosticable entrada-salida.

A grandes rasgos, una falta permanente se puede diagnosticar si, en un número finito de pasos después de que ocurre es posible determinar su ocurrencia. Esto implica saber cuándo un lugar de riesgo es marcado y asegurar que en un número finito de pasos es posible detectar y aislar la falta. Por ejemplo, en el GM de la figura 4.3.1 donde $\lambda(t_i) = a_i$, los lugares p_{11}, p_{18}, p_{19} son medibles y los lugares p_3, p_5, p_{11} son lugares de riesgo; si se dió la secuencia de entrada "$a_7 a_5 a_4 a_{10} a_9 a_{13}$' a partir de M_0 sucede que, si al dar la entrada a_{13} no se obtiene la observación correspondiente al disparo de t_{13} se detecta la presencia de faltas en el sistema, pero aún no es posible saber cual de ellas ocurrió. Las posibles faltas son t_{18} y t_{19}. Al dar la entrada a_{15} se puede determinar con seguridad la falta ocurrida. Si se obtiene la observación esperada para el lugar p_{18} se sabe que ocurrió t_{19}, si no se obtiene la observación esperada se sabe que ocurrió t_{18}. Sabemos que en un

número finito de pasos se deberá disparar t_{15} debido a que en un grafo marcado vivo y seguro solo existe un T-semiflujo, por lo que en un número finito de pasos es posible saber cuales lugares de riesgo fueron alcanzados y cuales faltas ocurrieron, es decir, detectar y aislar la falta. Con esto en mente en las secciones siguientes se propone una caracterización y un esquema de diagnóstico.

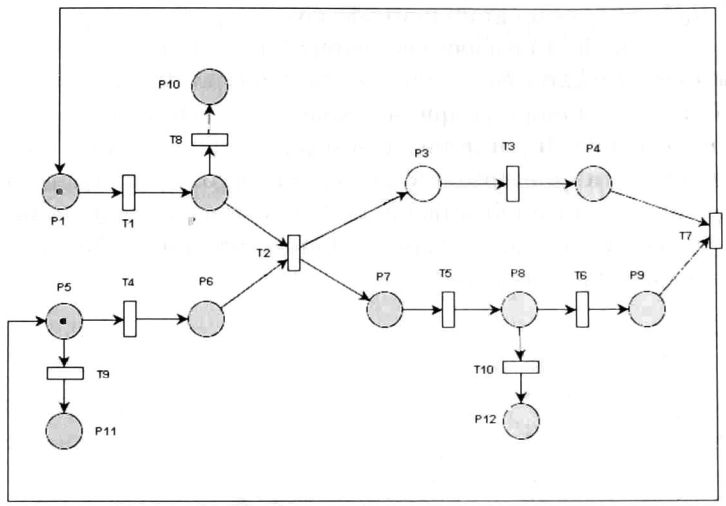


FIGURA 4.3.2. GM con faltas permanentes detectables.

4.3.1. Caracterización de diagnosticabilidad.

En esta sección se propone una caracterización para grafos marcado vivos y seguros en base al concepto de *área de influencia única* definido más adelante en esta sección.

El hecho de que un GM vivo y seguro sólo tiene un T-semiflujo nos indica que si se pierde una marca, entonces en un número finito de pasos el grafo marcado no tendrá transiciones habilitadas. Para propósitos de diagnóstico esto nos indica que en un número finito de pasos no se tendrán más observaciones. Considere el GM de la figura 4.3.2 donde el único lugar medible es p_3; es posible detectar la presencia de faltas en el GM si al intentar disparar la transición t_2 no se obtiene la observación esperada.

La proposición siguiente establece que, en un GM donde existe al menos una observación, es posible detectar la presencia de faltas.

PROPOSICIÓN 1. *Sea (Q, M_0) un grafo marcado vivo y seguro, con faltas permanentes y sin transiciones no manipulables. Si existe al menos un lugar medible, entonces es posible detectar la presencia de faltas en (Q, M_0).*

DEMOSTRACIÓN. Debido a que no existen transiciones no manipulables en (Q^N, M_0^N) y se conoce el marcado inicial entonces es posible conocer el marcado de (Q^N, M_0^N) en todo momento a menos que ocurra una falta. Puesto que un GM vivo y seguro está cubierto por un T-semiflujo, entonces si una o varias faltas ocurren, esto provocará que las transiciones post-riesgo relacionadas con las faltas ocurridas no se puedan ejecutar, y por lo tanto las transiciones que pertenecen al T-semiflujo no se podrán ejecutar de manera infinita, en particular las transiciones $\bullet p_i$ para todo p_i

medible. Cuando $\lambda(\bullet p_i)$ se da al sistema y no se obtiene la observación esperada, según el marcado actual de (Q^N, M_0^N) entonces se sabe que una o varias faltas ocurrieron. □

Note que, aunque esto basta para detectar la presencia de faltas, no es suficiente para aislar las faltas ocurridas, para esto es necesario asociar cada ausencia de observación con alguna falta especifica. El concepto de área de influencia única definido a continuación permite verificar ésta situación.

DEFINICIÓN 42. *El* Área de influencia única *de un lugar de riesgo* p_i, $Aiu(p_i)$ *está compuesto por las transiciones que se pueden disparar a partir de un marcado* M *tal que* $M(p_i) = 1$ *independientemente del disparo del resto de las transiciones post-riesgo* $p_j\bullet$ *para todo lugar de riesgo* p_j.

Puesto que, el área de influncia única de un lugar de riesgo p_i está compuesta por las transiciones que se pueden disparar a partir de que un lugar de riesgo independientemente del disparo de las demás transiciones post-riesgo, esto nos permite asociar de manera única cada observación en una área de influencia con la no ocurrencia de la falta asociada. A continuación se detalla esto.

Algoritmo 6 Cálculo de $Aiu(p_i)$ en un GM.

Entrada:
p_i - Lugar de riesgo al que se le calcula el área de influencia única.
Constantes:
(Q^N, M_0^N) Grafo marcado.
Salida:
$Aiu(p_i)$ Área de influencia de p_i.

1. $Aiu(p_i) = T$
2. Para toda transición t_i tal que $t_i \in p_j\bullet$, donde p_j es un lugar de riesgo diferente de p_i.
   a) Mientras existan transiciones habilitadas diferentes de t_i en M_0^N
      1) Disparar transiciones habilitadas diferentes de t_i.
   b) Si $M(p_i) = 1$ entonces $Aiu(p_i) = \emptyset$. Terminar.
   c) $A(p_i) = \{t \in \rho | \rho$ es un camino que inicia en $p_i\bullet$ y termina en la primera transición t_j tal que $\forall p_k \in t_j\bullet$, p_k está marcado y $\nexists p_l \in \rho$ tal que p_l está marcado.$\}$
   a) $Aiu(p_i) = Aiu(p_i) \cap A(p_i)$.

Vea por ejemplo la RPI de la figura 4.3.2, siguiendo los pasos del algoritmo 6 tenemos que:
El área de influencia única para p_2 se calcula de la siguiente manera. Inicialmente $Aiu(p_2) = \{t | t \in (Q^N, M_0^N)$ donde t es una transición$\}$. Aplicando el paso 2.a para la transición t_4 el marcado resultante es $M[\ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ ]$ Y puesto que p_2 es un lugar marcado entonces $Aiu(p_2) = \emptyset$.
El área de influencia única para p_5 se calcula de la siguiente manera. $Aiu(p_5) = \{t | t \in (Q^N, M_0^N)$ donde t es una transición$\}$ inicialmente. Reteniendo el disparo de t_2 en el paso 2.a se obtiene el marcado $M[\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ ]$. Aplicando paso 2.c, $A(p_5) = \{t_4\}$ por lo que $Aiu(p_5) = Aiu(p_5) \cap \{t_4\}$ hasta el momento. Reteniendo el disparo de t_6 se alcanza el marcado $M[\ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$, $A(p_5) = \{t_4, t_2, t_3, t_5\}$ y $Aiu(p_5) = \{t_4\} \cap \{t_4, t_2, t_3, t_5\} = \{t_4\}$.

El área de influencia única para p_8 se calcula de la siguiente manera. $Aiu(p_8) = \{t | t \in (Q^N, M_0^N)$ donde t es una transición$\}$ inicialmente. Reteniendo el disparo de t_2 en el paso 2.a se obtiene el marcado $M[\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ ]$. Aplicando paso 2.c, $A(p_8) = \{t_6, t_7, t_4, t_1\}$ por lo que $Aiu(p_8) = \{t_6, t_7, t_4, t_1\}$ hasta el momento. El marcado $M[\ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ ]$ se alcanza reteniendo el disparo de t_4, $A(p_8) = \{t_6, t_7, t_1\}$ y $Aiu(p_8) = \{t_6, t_7, t_4, t_1\} \cap \{t_6, t_7, t_1\} = \{t_6, t_7, t_1\}$.

Como resultado tenemos que $Aiu(p_2) = \emptyset$, $Aiu(p_5) = \{t_4\}$, $Aiu(p_8) = \{t_6, t_7, t_1\}$. Lo que nos indica que, para p_2 no existen transiciones cuyo disparo no depende del disparo de alguna otra transición post-riesgo en un marcado tal que $M(p_2) = 1$. En el caso de p_5 en un marcado donde $M(p_5) = 1$, el disparo de t_4 está asegurado independientemente del disparo de otras transiciones post-riesgo; lo mismo sucede con p_8 y las transiciones t_6, t_7, t_1.

El área de influencia única de un lugar de riesgo p_i indica las transiciones que se pueden disparar aún cuando otras faltas ocurran en un marcado $M(p_i) = 1$. Si existen transiciones evento-detectables en el área de influencia única de p_i, éstas se tendrán que disparar en un tiempo finito en (Q^N, M_0^N); en caso de no tener la observación esperada al disparar una transición evento-detectable $t_i \in Aiu(p_i)$ esto se puede asociar de forma única a la ocurrencia de la falta asociada a p_i.

PROPOSICIÓN 2. *El algoritmo 6 calcula el área de influencia única de un lugar de riesgo* p_i.

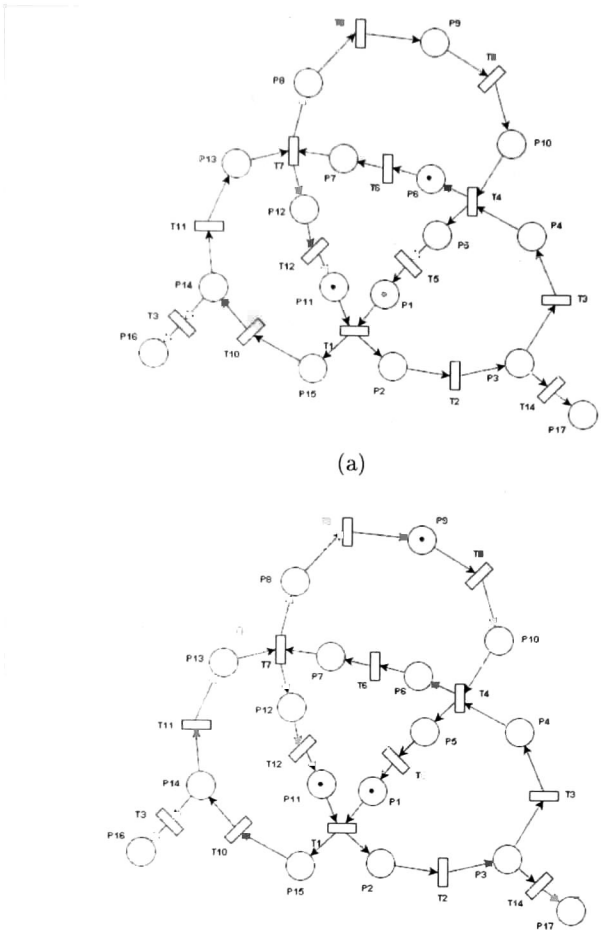
DEMOSTRACIÓN. Existen dos posibilidades.

a) Si p_i se marca en paralelo con p_j, entonces existe un marcado tal que $M_k(p_i) = 1$ y $M_k(p_j) = 1$ y al menos una transición t_i que sincroniza a p_i y p_j. Si $p_j\bullet$ no se dispara debido a una falta entonces no se podrá disparar cualquier t_i que sincroniza a p_i y p_j. Debido a esto las transiciones $t_i \bullet\bullet$ y las transiciones posteriores no se podrán disparar. Por lo que las únicas transiciones que se pueden disparar en un marcado tal que $M_k(p_i) = 1$ son las transiciones $p_i\bullet$ y posteriores sin llegar a t_i. Puesto que el algoritmo 6 retienen el disparo de $p_j\bullet$ y dispara el resto de las transiciones posibles entonces las transiciones que se dispararon a partir de un marcado $M_k(p_i) = 1$ conducen a lugares marcados a partir de los cuales no se pueden disparar más transiciones.

b) Si p_i no se marca en paralelo con p_j, entonces no existe marcado tal que $M_k(p_i) = 1$ y $M_k(p_j) = 1$. Si $M_k(p_i) = 1$ y $M_k(p_j) = 0$, existe un camino dirigido que lleva la marca de p_i a p_j. Sino se dispara $p_j\bullet$ entonces $p_j \bullet\bullet$ y posteriores no se podrán disparar, por lo que las únicas transiciones que se pueden disparar en un marcado tal que $M_k(p_i) = 1$ son $p_i\bullet$ y posteriores que no pertenecen a $p_j \bullet\bullet$ y posteriores. Puesto que el algoritmo 6 retiene el disparo de $p_j\bullet$ cuando se alcanza un marcado $M_k(p_j) = 1$ entonces las únicas transiciones que se pueden disparar a partir de un marcado $M_k(p_i) = 1$ son las transiciones $p_i\bullet$ y posteriores sin llegar a $p_j\bullet$ ya que p_j está marcado y las transiciones tales que existe un camino dirigido de $p_i\bullet$ a algún lugar marcado. □

Una característica interesante del área de influencia única de un lugar de riesgo es que cambia según el marcado inicial del sistema. En la figura 4.3.3 se muestran dos grafos marcados que tienen la misma estructura pero marcados iniciales diferentes; se puede ver que el área de influencia única cambia según el marcado inicial. En el grafo marcado de la figura 4.3.3.a $Aiu(p_{14}) = \{t_{11}, t_7, t_{12}, t_8, t_9\}$, $Aiu(p_3) = \{t_3\}$, sin embargo en el grafo marcado de la figura 4.3.3.b $Aiu(p_{14}) = \{t_{11}\}$, $Aiu(p_3) = \{t_3, t_4, t_5, t_6\}$. Esto nos indica que el área de influencia única de un lugar de riesgo cambia según el marcado inicial.

A continuación vemos un ejemplo en el que es posible que no se tengan las observaciones esperadas en $Aiu(p_i)$ debido a que no se alcanzó un marcado de riesgo $M(p_i) = 1$, sin embargo



(a)

(b)

FIGURA 4.3.3. Área de influencia única según marcado inicial.

en un tiempo finito se puede determinar si realmente se alcanzó un marcado tal que $M(p_i) = 1$, y una vez que esto se sabe, es posible determinar si ocurrió realmente la falta asociada a p_i.

EJEMPLO 12. *Considere el GM de la figura 4.3.4 con* $\lambda(t_1) = a_1$, $\lambda(t_2) = a_2$, $\lambda(t_3) = a_3$, $\lambda(t_4) = a_4$, $\lambda(t_5) = a_5$, $\lambda(t_6) = a_6$, $Aiu(p_2) = \{t_2, t_3, t_5, t_6\}$, $Aiu(p_4) = \{t_4, t_1\}$. *Si se da la secuencia de entrada* $a_1a_2a_3a_4a_1a_2$ *y no se obtiene la observación esperada para la entrada* a_4 *no se puede concluir que* t_8 *se disparó ya que es probable que* t_7 *se haya disparado. Si embargo en una cantidad de pasos finita esto se sabrá, porque se tendrán que disparar las transiciones evento-detectables que pertenecen a* $Aiu(p_2)$ *para que el sistema continue su funcionamiento. Si se obtiene la observación esperada para la entrada* a_5 *se concluye que* t_7 *no ocurrió, por tanto se sabe que* t_9 *se disparó y que no se alcanzó un marcado tal que* $M(p_2) = 1$ *después de un marcado tal que* $M(p_4) = 1$.

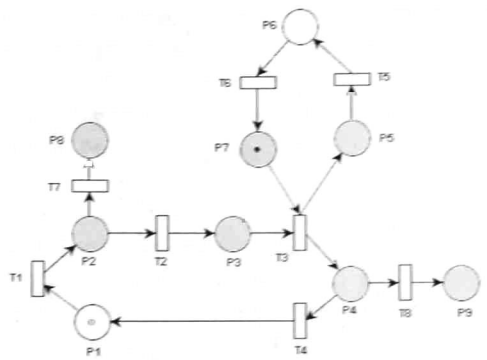


FIGURA 4.3.4. Detección y aislamiento de faltas.

En el teorema siguiente se establece que si para todo lugar de riesgo se cumple que existe al menos una transición evento-detectable que pertenece a su área de influencia única entonces es posible aislar la ocurrencia de cada falta.

TEOREMA 5. *Sea* (Q, M_0) *un grafo marcado vivo y seguro, con faltas permanentes. Si para todo lugar de riesgo* p_i *se cumple que existe al menos una transición evento-detectable en* $Aiu(p_i)$*, entonces es posible detectar y aislar la ocurrencia de cualquier falta.*

DEMOSTRACIÓN. Por la proposición 1 la ocurrencia de cualquier falta en (Q, M_0) se pude detectar. Puesto que $Aiu(p_i)$ de un lugar de riesgo p_i contiene las transiciones que se pueden disparar independientemente del disparo de alguna otra transición post-riesgo, entonces una vez que se alcanza un marcado donde $M(p_i) = 1$ las transiciones de $Aiu(p_i)$ se podrán disparar con seguridad, a menos que la falta asociada a p_i ocurra, en este caso se podrá asociar la ausencia de observaciones a la ocurrencia de la falta asociada a p_i. Para el caso cuando no se sabe si realmente se alcanzó el marcado $M(p_i) = 1$ y al disparar una transición evento-detectable de $Aiu(p_i)$ no se obtiene la observación esperada, esto se podrá saber en un número finito de pasos ya que para todo lugar de riesgo p_j existe al menos una transición evento-detectable $t_i \in Aiu(p_i)$ y se asegura que todas las transiciones evento-detectables que pertenecen al área de influencia única de algún lugar de riesgo se disparan en un tiempo finito debido a que un GM vivo y seguro esta cubierto por un T-semiflujo solamente por lo que se podrá saber si realmente se alcanzó el marcado $M(p_i) = 1$. □

4.3.2. Esquema de diagnóstico.

En esta sección se propone un esquema diagnosticador para GM.

El esquema diagnosticador presentado aquí se muestra en la figura 4.3.5 y está compuesto por:

- El *modelo diagnosticador* (Q^N, M_0^N)
- El modulo de *detección y localización* de faltas.

El modelo diagnosticador representa el funcionamiento normal del sistema: el módulo de detección y localización está compuesto por el algoritmo 7. Una n en la 3-tupla (p_i, n, σ_i) indica que aún no se da la entrada correspondiente a una transición evento-detectable en $Aiu(p_i)$, una s indica que se dió $\lambda(t)$ donde t es una transición evento-detectable en $Aiu(p_i)$.

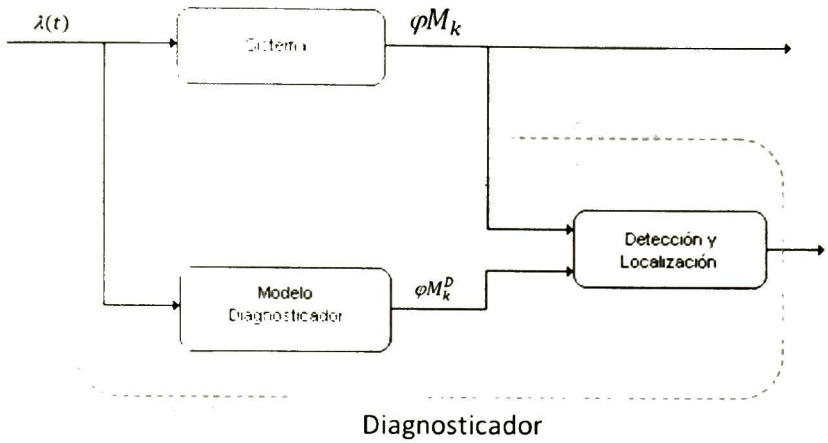


FIGURA 4.3.5. Esquema diagnosticador en GM.

Algoritmo 7 Detección y localización de faltas en GM.

Entrada:
M_k^D Marcado del modelo diagnosticador.
$\varphi(M_k)$ Observación del sistema.
Variables:
F Contiene las posibles faltas. Inicialmente es vacía.
Salida:
Transición de falta ocurrida.

1. Si M_k^D marca lugar de riesgo p_i y no existe (p_j, s, σ_j) en F tal que $\bullet p_i \in \sigma_j$ y no existe (p_i, n, ε).
   a) Agregar la 3-tupla (p_i, n, ε) a la fila F
2. Si t_l se dispara en (Q^N, M_0^N).
   a) $\forall$ 3-tupla $(p_i, -, \sigma_i)$ en F si $\bullet\bullet t_l \in \sigma_i$ o $\bullet t_l = p_i$ entonces
      1) $\sigma_i = \sigma_i t_l$
   b) Si $\varphi C(\bullet, t_l) \neq 0$ y $t_l \in \sigma_i$, para algún $(p_i, -. \sigma_i)$ de F
      1) Si $\varphi(M_{k+1}) - \varphi(M_k) = \varphi(M_{k+1}^D) - \varphi(M_k^D)$
         a' $\forall$ 3-tupla $(p_i, n. \sigma_i)$ en F tal que $t_l \in \sigma_i$ eliminar $(p_i. n, \sigma_i)$ de F.
      2) Si $\varphi(M_{k+1}) - \varphi(M_k) \neq \varphi(M_{k+1}^D) - \varphi(M_k^D)$
         a' Si existe $(p_i, n. \sigma_i)$ en F tal que $t_l \in \sigma_i \cap Aiu(p_i)$ hacer
            $\forall(p_j, -, \sigma_j)$ tal que $p_j\bullet \in \sigma_i$ y $(p_j, -. \sigma_j)$ se agregó después que (p_i, n, σ_i), eliminar $(p_j, -, \sigma_j)$.
            $(p_i. n, \sigma_i) = (p_i, s, \sigma_i)$.
            "Presencia de faltas"
      3) $\forall(p_j, s, \sigma_j)$ en F. Sino existe (p_k, n, σ_k), tal que $p_j\bullet \in \sigma_k$, donde $(t_k, n. \sigma_k)$ se agregó antes que (p_j, s, σ_j) a F. entonces
         a' $p_j \bullet \cap T^F$ ocurrió.
         b' Disparar de forma invertida las transiciones habilitadas en σ_j hasta que no exista transición habilitada.
         c' Hacer $M^D(p_j) = 0$.
         d' Eliminar (p_j, s, σ_j) de F.

En seguida se muestra un ejemplo del funcionamiento del módulo de detección y localización.

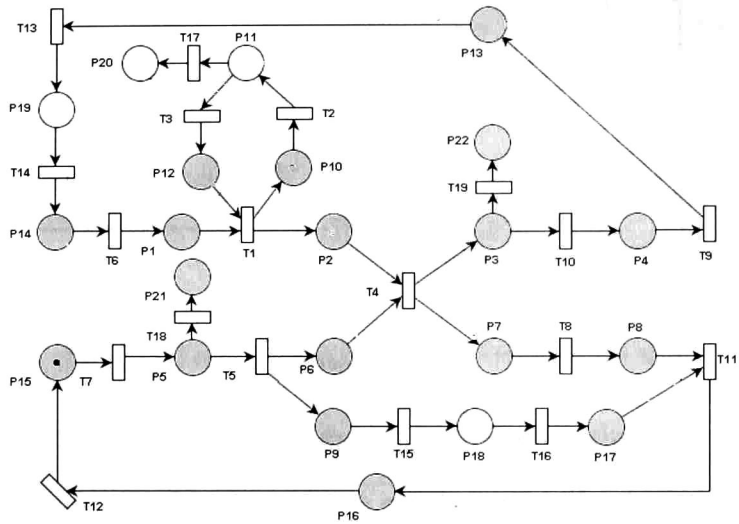


FIGURA 4.3.6. GM

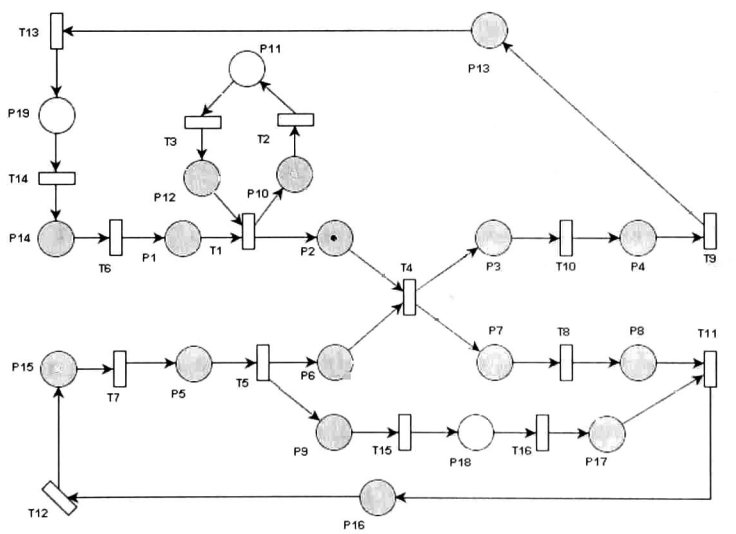


FIGURA 4.3.7. Modelo diagnosticador

$$\varphi C = \begin{bmatrix} 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \end{bmatrix} \tag{4.3.1}$$

EJEMPLO 13. *Considere el GM de la figura 4.3.6 donde* $\lambda(t_i) = a_i$, *los lugares* p_{11}, p_{18}, p_{19} *son lugares medibles. Los lugares* p_3, p_5, p_{11} *son lugares de riesgo.* $Aiu(p_3) = \{t_{10}, t_9, t_{13}, t_{14}, t_6\}$, $Aiu(p_5) = \{t_5, t_{15}, t_{16}\}$, $Aiu(p_{11}) = \{t_3\}$. *En el figura 4.3.7 se muestra el modelo diagnosticador correspondiente a este GM y la ecuación (4.3.1) muestra la matriz* φC *correspondiente al modelo diagnosticador. Si se da como entrada la secuencia "*$a_7, a_5, a_4, a_{10}, a_9, a_8, a_{13}, a_{14}, a_6, a_2, a_3, a_{15}$*" y ocurre* t_{19} *entonces:*

Inicialmente F está vacío y

$$M_0 = [\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_0^D = [\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

Paso 1. M_0^D *no marca lugares de riesgo.*

Con la entrada a_7 *se dispara* t_7 *y se alcanzan los marcados*

$$M_k = [\ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_k^D = [\ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- *Paso 1.* M_k^D *marca el lugar de riesgo* p_5, *y F esta vació por lo que se agrega* $(p_5, n, \sigma_5 = \varepsilon)$ *a F*

1	$(p_5, n, \sigma_5 = \varepsilon)$

- *Paso 2.* t_7 *se dispara en* (Q^N, M_0^N).
  Paso 2.a y 2.b no se cumplen.
  Con la entrada a_5 *se dispara* t_5 *y se alcanzan los marcados*

$$M_k = [\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_k^D = [\ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- *Paso 1. No se cumple.*
- *Paso 2.* t_5 *se dispara en* (Q^N, M_0^N).
- *Paso 2.a* $\bullet t_5 = p_5$, *entonces* $\sigma_5 = t_5$

1	$(p_5, n, \sigma_5 = t_5)$

  Paso 2.b. No se cumple.
  Con la entrada a_4 *se dispara* t_4 *y se alcanzan los marcados*

$$M_k = [\ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

$$M_k^D = [\ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- *Paso 1.* M_k^D *marca el lugar de riesgo* p_3 *y no existe* (p_i, s, σ_i) *donde* $\bullet p_3 = t_4 \in \sigma_i$. *Por lo que* $(p_3, n, \sigma_3 = \varepsilon)$ *se agrega a F*

1	$(p_5, n, \sigma_5 = t_5)$
2	$(p_3, n, \sigma_3 = \varepsilon)$

Debido a que se está considerando el caso cuando t_{19} *ocurre, el marcado del sistema es*

$$M_k = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ ]$$

Paso 2. t_4 *se dispara en* (Q^N, M_0^N).

- *Paso 2.a* $\lambda(a_4)^{-1}$, $\sigma_5 = t_5 t_4$

1	$(p_5, n, \sigma_5 = t_5 t_4)$
2	$(p_3, n, \sigma_3 = \varepsilon)$

Paso 2.b. No se cumple.

Con la entrada a_{10} *se dispara* t_{10} *y se alcanzan los marcados*

$$M_k = [\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ ]$$

$$M_k^D = [\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ ]$$

Paso 1. M_k^D *no marca lugares de riesgo.*

Paso 2. t_{10} *se dispara en* (Q^N, M_0^N).

Paso 2.a $\bullet\bullet t_{10} \in \sigma_5$ *y* $\bullet t_{10} = p_3$ *por lo que* F *se actualiza así*

1	$(p_5, n, \sigma_5 = t_5 t_4 t_{10})$
2	$(p_3, n, \sigma_3 = t_{10})$

Paso 2.b. No se cumple.

Con la entrada a_9 *se dispara* t_9 *y se alcanzan los marcados*

$$M_k = [\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ ]$$

$$M_k^D = [\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ ]$$

Paso 1. M_k^D *no marca lugares de riesgo.*

Paso 2. t_9 *se dispara en* (Q^N, M_0^N).

Por el paso 2.a $\bullet\bullet t_9 \in \sigma_5$ *y* $\bullet\bullet t_9 = p_3$ *por lo que* F *se actualiza así*

1	$(p_5, n, \sigma_5 = t_5 t_4 t_{10} t_9)$
2	$(p_3, n, \sigma_3 = t_{10} t_9)$

Paso 2.b. No se cumple.

Con la entrada a_8 *se dispara* t_8 *y se alcanzan los marcados*

$$M_k = [\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ ]$$

$$M_k^D = [\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ ]$$

Paso 1. M_k^D *no marca lugares de riesgo.*

Paso 2. t_8 *se dispara en* (Q^N, M_0^N).

Por el paso 2.a $\bullet\bullet t_8 \in \sigma_5$ *por lo que* F *se actualiza así*

1	$(p_5, n, \sigma_5 = t_5 t_4 t_{10} t_9 t_8)$
2	$(p_3, n, \sigma_3 = t_{10} t_9)$

Paso 2.b. No se cumple.

Con la entrada a_{13} *se dispara* t_{13} *y se alcanzan los marcados*

$$M_k = [\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ ]$$

$$M_k^D = [\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ ]$$

Paso 1. M_k^D *no marca lugares de riesgo.*

Paso 2. t_{13} *se dispara en* (Q^N, M_0^N).

- *Paso 2.a* $\bullet\bullet t_{13} \in \sigma_5$ *y* $\bullet\bullet t_{13} \in \sigma_3$ *por lo que* F *se actualiza así*

1	$(p_5, n, \sigma_5 = t_5 t_4 t_{10} t_9 t_8 t_{13})$
2	$(p_3, n, \sigma_3 = t_{10} t_9 t_{13})$

- *Paso 2.b* $\varphi C(\bullet, t_{13}) = [\ 0\ \ 0\ \ 1\ ]^T \neq \mathbf{0}$ *y* $t_{13} \in \sigma_5$, $t_{13} \in \sigma_3$ *por lo que se cumple la condición.*

Puesto que $\varphi(M_k) = [\ 0\ \ 0\ \ 0\ ]^T$ $\varphi(M_{k+1}) = [\ 0\ \ 0\ \ 0\ ]^T$ $\varphi(M_k^D) = [\ 0\ \ 0\ \ 0\ ]^T$ *y* $\varphi(M_{k+1}) = [\ 0\ \ 0\ \ 1\ ]^T$

$$\varphi(M_{k+1}) - \varphi(M_k) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\varphi(M_{k+1}^D) - \varphi(M_k^D) = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\varphi(M_{k+1}) - \varphi(M_k) \neq \varphi(M_{k+1}^D) - \varphi(M_k^D)$$

- *Paso 2.b.1. No se cumple.*
- *Paso 2.b.2. Se cumple.*
- *Paso 2.b.2.a' Se cumple para* $(p_3, n, \sigma_3 = t_{10} t_9 t_{13})$ *ya que* $t_{13} \in \sigma_3 \cap Aiu(p_3)$
  - *No existen* $(p_i, -, \sigma_i)$ *tales que* $p_i\bullet \in \sigma_3$ *que se agregaron después que* $(p_3, n, \sigma_3 = t_{10} t_9 t_{13})$.
  - $(p_3, n, \sigma_3 = t_{10} t_9 t_{13}) = (p_3, s, \sigma_3 = t_{10} t_9 t_{13})$.
  - *"Presencia de faltas"*
- *Paso 2.b.3. Para* $(p_3, s, \sigma_3 = t_{10} t_9 t_{13})$ *existe* $(p_5, n, \sigma_5 = t_5 t_4 t_{10} t_9 t_8 t_{13})$ *que se agregó antes y* $p_3\bullet \in \sigma_5$ *por lo que no se cumple.*
- *Con la entrada* a_{14} *se dispara* t_{14} *y se alcanzan los marcados*

$$M_k = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ ]$$

$$M_k^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- *Paso 1.* M_k^D *no marca lugares de riesgo.*
- *Paso 2.* t_{14} *se dispara en* (Q^N, M_0^N).
- *Paso 2.a* $\bullet\bullet t_{14} \in \sigma_5$ *y* $\bullet\bullet t_{14} \in \sigma_3$ *por lo que* F *se actualiza así*

1	$(p_5, n, \sigma_5 = t_5 t_4 t_{10} t_9 t_8 t_{13} t_{14})$
2	$(p_3, s, \sigma_3 = t_{10} t_9 t_{13} t_{14})$

- *Paso 2.b* $\varphi C(\bullet, t_{14}) = [\ 0\ \ 0\ \ -1\ ]^T \neq \mathbf{0}$ *y* $t_{14} \in \sigma_5$, $t_{14} \in \sigma_3$ *por lo que se cumple la condición.*

Puesto que $\varphi(M_k) = [\ 0\ \ 0\ \ 0\ ]^T$ $\varphi(M_{k+1}) = [\ 0\ \ 0\ \ 0\ ]^T$ $\varphi(M_k^D) = [\ 0\ \ 0\ \ 1\ ]^T$ *y* $\varphi(M_{k+1}) = [\ 0\ \ 0\ \ 0\ ]^T$

$$\varphi(M_{k+1}) - \varphi(M_k) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\varphi(M^D_{k+1}) - \varphi(M^D_k) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$$

$$\varphi(M_{k+1}) - \varphi(M_k) \neq \varphi(M^D_{k+1}) - \varphi(M^D_k)$$

Paso 2.b.1. No se cumple.

Paso 2.b.2. Se cumple.

- *Paso 2.b.2.a. No se cumple.*

Paso 2.b.3. Para $(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14})$ *existe* $(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}, t_{14})$ *que se agregó antes y* $p_3\bullet \in \sigma_5$ *por lo que no se cumple.*

- *Con la entrada* a_6 *se dispara* t_6 *y se alcanzan los marcados*

$$M_k = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ ]$$

$$M^D_k = [\ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- *Paso 1.* M^D_k *no marca lugares de riesgo.*
- *Paso 2.* t_6 *se dispara en* (Q^N, M^N_0).

Paso 2.a $\bullet\bullet t_6 \in \sigma_5$ *y* $\bullet\bullet t_6 \in \sigma_3$ *por lo que F se actualiza así*

1	$(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}t_{14}t_6)$
2	$(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$

Paso 2.b. No se cumple.

Con la entrada a_2 *se dispara* t_2 *y se alcanzan los marcados*

$$M_k = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ ]$$

$$M^D_k = [\ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

Paso 1. M^D_k *marca el lugar de riesgo* p_{11} *y no existe* (p_i, s, σ_i) *tal que* $\bullet p_{11} = t_2 \in \sigma_i$ *por lo que* $(p_{11}, n, \sigma_{11} = \varepsilon)$ *se agrega a F*

1	$(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}t_{14}t_6)$
2	$(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$
3	$(p_{11}, n, \sigma_{11} = \varepsilon)$

Paso 2. t_2 *se dispara en* (Q^N, M^N_0).

Por el paso 2.a $\bullet\bullet t_2 \notin \sigma_5$, $\bullet\bullet t_2 \notin \sigma_3$ *por lo que F no se actualiza.*

1	$(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}t_{14}t_6)$
2	$(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$
3	$(p_{11}, n, \sigma_{11} = \varepsilon)$

Paso 2.b. No se cumple.

Con la entrada a_3 *se dispara* t_3 *y se alcanzan los marcados*

$$M_k = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ ]$$

$$M_k^D = [\ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- *Paso 1.* M_k^D *no marca lugares de riesgo.*
- *Paso 2.* t_3 *se dispara en* (Q^N, M_0^N).
- *Paso 2.a* $\bullet t_3 = p_{11}$ *por lo que* F *se actualiza así.*

1	$(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}t_{14}t_6)$
2	$(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$
3	$(p_{11}, n, \sigma_{11} = t_3)$

Paso 2.b. $\varphi C(\bullet, t_3) = [\ -1\ \ 0\ \ 0\ ]^T \neq \mathbf{0}$ *y* $t_3 \in \sigma_{11}$, *por lo que se cumple la condición.*

Puesto que $\varphi(M_k) = [\ 1\ \ 0\ \ 0\ ]^T\ \ \varphi(M_{k+1}) = [\ 0\ \ 0\ \ 0\ ]^T\ \ \varphi(M_k^D) = [\ 1\ \ 0\ \ 0\ ]^T$ *y* $\varphi(M_{k+1}) = [\ 0\ \ 0\ \ 0\ ]^T$

$$\varphi(M_{k+1}) - \varphi(M_k) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \\ 0 \end{bmatrix}$$

$$\varphi(M_{k+1}^D) - \varphi(M_k^D) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \\ 0 \end{bmatrix}$$

$$\varphi(M_{k+1}) - \varphi(M_k) = \varphi(M_{k+1}^D) - \varphi(M_k^D)$$

- *Paso 2.b.1. Se cumple.*
- *2.b.1.a'. Se cumple para* $(p_{11}, n, \sigma_{11} = t_3)$ *ya que* $t_3 \in \sigma_{11} \cap Aiu(p_{11})$, *por lo que* $(p_{11}, n, \sigma_{11} = t_3)$ *se elimina de* F

1	$(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}t_{14}t_6)$
2	$(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$

- *Paso 2.b.2. No se cumple.*

Paso 2.b.3. No se cumple para algún elemento de F
Con la entrada a_{15} *se dispara* t_{15} *y se alcanzan los marcados*

$$M_k = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ ]$$

$$M_k^D = [\ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$$

Paso 1. M_k^D *no marca lugares de riesgo.*
Paso 2. t_{15} *se dispara en* (Q^N, M_0^N).
Paso 2.a. $\bullet \bullet t_{15} \in \sigma_5$, *por lo que* F *se actualiza.*

1	$(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}t_{14}t_6, t_{15})$
2	$(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$

Paso 2.b. Se cumpla para $(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}t_{14}t_6, t_{15})$ *ya que* $\varphi C(\bullet, t_{15}) = [\ 0\ \ 1\ \ 0\ ]^T \neq \vec{0}$ *y* $t_{15} \in \sigma_5$.

Puesto que $\varphi(M_k) = [\ 0\ \ 0\ \ 0\ ]^T$ $\varphi(M_{k+1}) = [\ 0\ \ 1\ \ 0\ ]^T$ $\varphi(M_k^D) = [\ 0\ \ 0\ \ 0\ ]^T$ *y* $\varphi(M_{k+1}) = [\ 0\ \ 1\ \ 0\ ]^T$

$$\varphi(M_{k+1}) - \varphi(M_k) = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\varphi(M_{k+1}^D) - \varphi(M_k^D) = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\varphi(M_{k+1}) - \varphi(M_k) = \varphi(M_{k+1}^D) - \varphi(M_k^D)$$

- *Paso 2.b.1. Se cumple.*
- *Paso 2.b.1.a´ Para* $(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}t_{14}t_6, t_{15})$, $t_{15} \in \sigma_5$, *por lo que se elimina* $(p_5, n, \sigma_5 = t_5t_4t_{10}t_9t_8t_{13}t_{14}t_6, t_{15})$ *de* F

1	$(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$

Paso 2.b.2. No se cumple.

Paso 2.b.3. Se cumple para $(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$ *ya que no existe* (p_k, n, σ_k) *tal que* $p_3\bullet = t_{10} \in \sigma_k$ *y* (p_k, n, σ_k) *se agregó antes que* $(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$.

Paso 2.b.3.a. Se concluye que $p_3 \bullet \cap T^F = t_{19}$ *se disparó.*

Paso 2.b.3.b. Para recuperar el marcado real del GM se disparan de forma invertida $\sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$, *es decir haciendo* $\forall t_i \in \sigma_3$ *si* $I(p_i, t_i) = 1$ *hacer* $O(p_i, t_i) = 1$, $I(p_i, t_i) = 0$ *y si* $O(p_i, t_i) = 1$ *hacer* $I(p_i, t_i) = 1$, $O(p_i, t_i) = 0$.

$M_k^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$

$M_k^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ ]$

$M_k^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$

$M_k^D = [\ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$

$M_k^D = [\ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$

Paso 2.b.3.c.

$M_k^D = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$

Paso 2.b.3.d. $(p_3, s, \sigma_3 = t_{10}t_9t_{13}t_{14}t_6)$ *se elimina de* F

Conclusiones

En esta tesis se abordó el problema de diagnóstico en línea de Sistemas de Eventos Discretos Temporizados (SEDT) modelados con redes de Petri interpretadas temporizadas (RPIT).

Como resultado de esta investigación se definió la propiedad de T-diagnosticabilidad para RPIT y se propuso una caracterización para clases de RPIT que tienen esta propiedad. Además se extendió el concepto de diagnosticabilidad entrada-salida para ser aplicado en RPIT y se analizó la relación que existe entre estos conceptos de diagnosticabilidad.

Entre las aportaciones relevantes de este trabajo, se encuentra la relajación de la restricción de la condición de evento-detectabilidad para las propiedades de diagnosticabilidad (T y entrada-salida). Con ello fue posible extender el análisis estructural a otras clases de RPI que no son evento-detectables, el cual puede ser realizado con algoritmos polinomiales. Los esquemas diagnosticadores propuestos son igualmente eficientes.

Los resultados aquí presentados constituyen una base inicial sobre el diagnóstico de los SEDT. Algunas de estas propuestas parecen tener extensiones en un futuro cercano; tal es el caso de una caracterización de diagnosticabilidad entrada-salida para RPI vivas y seguras no evento-detectables, la cual permita una verificación en tiempo polinomial; consecuentemente se podría proponer una caracterización de RPIT T-diagnosticables.

Referencias

[Alcaraz04] Mildreth Isadora Alcaraz Mejía, "Diagnóstico de fallas en sistemas de manufactura discretos", Cinvestav GDL, 2004.

[Bouyer05] Patricia Bouyer, Fabrice Chevalier and Deepak D'Souza. Fault Diagnosis Using Timed Automata. In Proceedings of the 8th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'05), Edinburgh, U.K., April 2005, LNCS 3441, pages 219-233. Springer.

[Chen97] Y. Chen and G. Provan, "Modeling and diagnosis of timed discrete event systems-A factory automation example," in Proc. Amer. Control Conf., Albuquerque, NM, Jun. 1997, pp. 31-36.

[Chen99] Jie Chen, R.J. Patton, "Robust Model-Based Fault Diagnosis For Dynamic Systems", Kluwer Academic Publishers, 1999.

[Christos93] Christos G. Cassandras. Discrete Event Systems Modeling and Performance Analysis. University of Massachusetts at Amherst. Aksen Associates Incorporated Publishers, 1993.

[Correcher05] Correcher, A. Garcia, E., Morant, F., Quiles, E."Diagnostico de fallos intermitentes: un enfoque basado en modelos de eventos discretos", Revista iberoamericana de automatica e informatica industrial (RIAI), ISSN 1697-7912, Vol. 2, Nº. 3, 2005, pags. 61-73.

[Debouk00] R. Debouk, S. Lafortune, and D. Teneketzis, "Coordinated decentralized protocols for failure diagnosis of discrete-event systems," Joumal of Discrete Event Dynamical Systems: Theory and Applications, 10:33-86, 2000.

[Desel95] Desel J. and J. Esparza. Free Choice Petri Nets, Cambridge University Press, 1995

[Genc06] Predictability in discrete-event systems under partial observation

[Genc05] S. Genc and S Lafortune, "Distributed diagnosis of discrete-event systems using petri nets", in Proc. 24th ATPN, 2003, pp. 316-336.

[Giua05] A. Giua and C. Seatzu, "Fault detection for discrete event systems using Petri nets with unobservable transitions", in the 44th Int. Conf. on Decision and Control and European Control Conference, 2005, pp 6323-6328.

[Hashtrudi03] S. Hashtrudi Zad, R. H. Kwong, W. M. Wonham. Fault Diagnosis in Discrete-Event Systems: Framework and Model reduction, IEEE Transactions on Automatic Control , vol. 48, no. 7, 2003, pp. 1199-1212.

[Hashtrudi05] S. Hashtrudi Zad, R.H. Kwong and W.M. Wonham, "Fault diagnosis in discrete-event systems: Incorporating timing information," IEEE Transactions on Automatic Control, vol. 50, no. 7, pp. 1010-1015, July 2005.

[Jalote94] P. Jalote. Fault Tolerance in Distributed Systems. Prentice Hall, Englewood Cliffs, NJ, 1994.

[Jiroveanu06] G. Jiroveanu, R.K. Boel, and B. De Schutter, "Fault diagnosis for time Petri nets," Proceedings of the 8th International Workshop on Discrete Event Sys- tems (WODES'06), Ann Arbor, Michigan, pp. 313–318, July 2006.

[Lefevbre07] Dimitri Lefebvre, Catherine Delherm. Diagnosis of DES with Petri Net Models. IEEE Transactions on automation science and engineering, vol. 4. No. 1, january 2007.

[Meda98] M. E. Meda, A. Ramírez-Treviño and A. Malo. Identification in discrete event systems. Proceedings of the IEEE Conference on Systems, Man & Cybernetics, pp. 740- 745, 1998.

[Olivier04] Olivier Contant, Stéphane Lafortune, Demosthenis Teneketzis, Diagnosis of Intermittent Faults. Discrete Event Systems: Theory and Applications, 14, 171-202, 2004.

[Pan06] J. Pan and S. Hashtrudi-Zad, "Diagnosability Test for Timed Discrete Event Systems," Proc. 18th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 06), Washington, DC, USA, pp. 63-72, November 2006.

[Provan02] Provan, G. "On the diagnosability of decentralized, timed discrete event systems", Proceedings of the 41st IEEE Conference on Decision and Control, Las Vegas, Nevada USA, December 2002.

[RamTrev07] Ramirez-Trevino, A. Ruiz-Beltran, E. Rivera-Rangel, I. Lopez-Mellado, E. "Online Fault Diagnosis of Discrete Event Systems. A Petri Net-Based Approach," IEEE Transactions on Automation Science end Engineering, vol. 4, no. 1, 2007, pp. 31-39.

[Rivera05] I. Rivera-Rangel, A. Ramirez-Treviño, L.I. Aguirre-Salas and J. Ruiz-León. Geometrical characterization of observability in Interpreted Petri Nets. Kybernetika, vol. 41, 553-574, 2005.

[Ruiz-Beltran07] Elvia Ruiz-Beltran, "Esquemas de diagnóstico de faltas en sistemas de eventos discretos", Cinvestav GDL, 2007.

[Sampath95] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. "Diagnosability of discrete-event systems," IEEE Trans. Autom. Control, vol. 40, no 9, pp. 1555-1575, Sep. 1995.

[Tripakis02] S. Tripakis. Fault diagnosis for timed automata. In Proc. 7th Int. Symp. Formal Techniques in Real-Time and Fault Tolerant Systems (FTRTFT'02), vol. 2469 of LNCS, pp. 205–224. Springer, 2002.

APÉNDICE A

Seguimiento del algoritmo 3 para la RPI de la figura 4.2.5.

Considere la RPI de la figura 4.2.5 con la función φ como se muestra en la ecuación (4.2.3) y $\lambda(t_8) = \varepsilon$, $\lambda(t_{13}) = \varepsilon$, $\lambda(t_{15}) = \varepsilon$ y $\lambda(t_i) = a_i$ para cualquier otra transición.

Usando el algoritmo 3 para determinar si existen $\rho_f(p_1)$ sin transiciones medibles para el lugar de riesgo p_1.

Paso 1. Hacer $Y_P = [\ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$.

El resultado del paso 2 es

$$Y_T = [\ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

El paso 3.a solo se realiza para la transición t_1.

Los pasos 3.a.1, 3.a.2, 3.a.3 no se cumplen ya que t_1 es manipulable, no existe lugar de riesgo en el conjunto $t_1\bullet$ y no es medible respectivamente.

El paso 3.b no se cumple ya que $Y_T(t_1) = 1$.

El resultado del paso 3.c es

$$Y_T = [\ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

El paso 3.a se realiza para t_2 y t_3.

Considerando t_2 primeramente.

El paso 3.a.1 no se cumple ya que t_2 es manipulable. El paso 3.a.2 no se cumple. El paso 3.a.3 no se cumple ya que $\varphi C(\bullet, t_2) = [\ 0\ \ 0\ \ 0\ \ 0\ ]^T$

Considerando t_3.

El paso 3.a.1 no se cumple ya que t_3 es manipulable. El paso 3.a.2 no se cumple. El paso 3.a.3 no se cumple ya que $\varphi C(\bullet, t_3) = [\ 0\ \ 0\ \ 0\ \ 0\ ]^T$

El paso 3.b no se cumple ya que

$$Y_T = [\ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

El resultado del paso 3.c es

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

El paso 3.a se realiza para t_4, t_5.

Considerando t_4 primeramente.

Los pasos 3.a.1, 3.a.2, 3.a.3 no se cumplen ya que t_4 es manipulable, no existe lugar de riesgo en el conjunto $t_4\bullet$ y no es medible respectivamente.

Considerando t_5.

Los pasos 3.a.1, 3.a.2 no se cumplen ya que t_5 es manipulable y no existe lugar de riesgo en el conjunto $t_5\bullet$. 3.a.3 se cumple ya que $\varphi C(\bullet, t_3) = [\ 1\ \ 0\ \ 0\ \ 0\ ]^T$ por lo que

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

El paso 3.b no se cumple ya que $Y_T(t_4) = 1$.
El resultado del paso 3.c es

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- El paso 3.a solo se realiza para la transición t_7.
- Los pasos 3.a.1, 3.a.2, 3.a.3 no se cumplen ya que t_7 es manipulable, no existe lugar de riesgo en el conjunto $t_7\bullet$ y no es medible respectivamente.
  El paso 3.b no se cumple ya que $Y_T(t_7) = 1$.
  El resultado del paso 3.c es

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ ]$$

El paso 3.a se realiza para t_6 y t_{14}.

Considerando t_6 primeramente.

Los pasos 3.a.1, 3.a.2, 3.a.3 no se cumplen ya que t_6 es manipulable, no existe lugar de riesgo en el conjunto $t_6\bullet$ y no es medible respectivamente.

Considerando t_{14}.

- Los pasos 3.a.1, 3.a.2 no se cumplen ya que t_{14} es manipulable y no existe lugar de riesgo en el conjunto $t_{14}\bullet$. 3.a.3 se cumple ya $\varphi C(\bullet, t_{14}) = [\ 0\ \ 0\ \ 1\ \ 0\ ]^T$ por lo que

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- El paso 3.b no se cumple ya que $Y_T(t_6) = 1$.
  El resultado del paso 3.c es

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

El paso 3.a solo se realiza para la transición t_5.
Los pasos 3.a.1 no se cumple ya que t_5 es manipulable. 3.a.2 no se cumple ya que $\varphi C(\bullet, t_5) = [\ 1\ \ 0\ \ 0\ \ 0\ ]^T$ y no existe lugar de riesgo en $t_5\bullet$. 3.a.3 se cumplen ya que $\varphi C(\bullet, t_5) = [\ 1\ \ 0\ \ 0\ \ 0\ ]^T$ por lo que

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

El paso 3.b se cumple.
En el paso 3.b.1 se declara que no existen $\rho_f(p_1)$ sin transiciones medibles.

Para determinar la existencia de $\rho_f(p_9)$ sin transiciones medibles para el lugar de riesgo p_9.

- En el paso 1 se hace $Y_P = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$.
- El resultado del paso 2 es

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- El paso 3.a solo se realiza para la transición t_{11}.
- Los pasos 3.a.1, 3.a.2, 3.a.3 no se cumplen ya que t_{11} es manipulable, no existe lugar de riesgo en el conjunto $t_{11}\bullet$ y no es medible respectivamente.
- El paso 3.b no se cumple ya que $Y_T(t_{11}) = 1$.
  El resultado del paso 3.c es

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

El paso 3.a solo se realiza para la transición t_{12}.

Los pasos 3.a.1, 3.a.2 no se cumplen ya que t_{12} es manipulable, no existe lugar de riesgo en el conjunto $t_{12}\bullet$. El paso 3.a.3 se cumple ya que $\varphi C(\bullet, t_{12}) = [\ 0\ \ 1\ \ 0\ \ 0\ ]^T$ por lo que

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- El paso 3.b se cumple.

  En el paso 3.b.1 se declara que no existen $\rho_f(p_9)$ sin transiciones medibles.

Para determinar la existencia de $\rho_f(p_{13})$ sin transiciones medibles para el lugar de riesgo p_{13}.

- En el paso 1 se hace $Y_P = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$.

  El resultado del paso 2 es

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ ]$$

  El paso 3.a solo se realiza para la transición t_{16}.

  Los pasos 3.a.1, 3.a.2 no se cumplen ya que t_{16} es manipulable, no existe lugar de riesgo en el conjunto $t_{16}\bullet$. El paso 3.a.3 se cumple ya que $\varphi C(\bullet, t_{16}) = [\ 0\ \ 0\ \ 0\ \ -1\ ]^T$ por lo que

$$Y_T = [\ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ ]$$

- El paso 3.b se cumple.
- En el paso 3.b.1 se declara que no existen $\rho_f(p_{13})$ sin transiciones medibles.

CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.
UNIDAD GUADALAJARA

El Jurado designado por la Unidad Guadalajara del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional aprobó la tesis

Diagnóstico de faltas en sistemas de eventos discretos temporizados

del (la) C.

Elías HERNÁNDEZ FLORES

el día 17 de Octubre de 2008.

Dr. Félix Francisco Ramos Corchado
Investigador CINVESTAV 3A
CINVESTAV Unidad Guadalajara

Dr. Antonio Ramírez Treviño
Investigador CINVESTAV 3A
CINVESTAV Unidad Guadalajara

Dr. Mario Angel Siller González
Pico
Investigador CINVESTAV 2A
CINVESTAV Unidad Guadalajara