DETECCIÓN ACTIVA DE FALTAS EN SISTEMAS DE EVENTOS DISCRETOS

Karen Hernández Rueda

Universidad de Guadalajara-CUCSUR

karenhr@cucsur.udg.mx

María E. Meda Campaña

Universidad de Guadalajara-CUCEA

emeda@cucea.udg.mx

Bernardo Haro Martínez

Universidad Autónoma de Guadalajara

bernardo.haro@gmail.com

Resumen

El objetivo de este trabajo es presentar una propuesta de solución de Diagnóstico Activo en Sistemas de Eventos Discretos modelado por redes de Petri. La propuesta se basa en un controlador llamado Circuito de Regulación Inteligente que reduce la distancia relativa entre las transiciones que modelan faltas y las del resto de la red de Petri, permitiendo la detección y diagnóstico de faltas mientras se mantiene la vivacidad del sistema y se reduce la flexibilidad del sistema sólo en los estados requeridos. Finalmente, los resultados presentados se ilustran en un ejemplo.

Palabras Claves: Detección activa, diagnosticabilidad, redes de Petri, sistemas de eventos discretos.

Abstract

The aim of this work is to present a proposal of Active Diagnosis in Discrete Event Systems modeled by Petri nets. This approach is based on a controller named Intelligent Regulation Circuit which reduces the relative distance among the system transition allow in the detection and diagnosis of faults while maintaining

the liveness of the system. Finally, the results presented are illustrated by an example.

Keywords**:** *Active detection, diagnosability, discrete event system, Petri nets.*

1. Introducción

En la actualidad los sistemas industriales cada vez más se vuelven grandes y complejos por lo que no están exentos de sufrir cualquier tipo de desviación de su comportamiento especificado (normal), comprometiendo la seguridad tanto de los sistemas como de los operadores humanos. Por lo tanto, las tareas de detección y localización de faltas deben incluirse en los controladores modernos para incrementar la confiabilidad de los sistemas.

La detección y localización de faltas han sido estudiadas extensamente en la literatura desde el punto de vista de los autómatas finitos (FA) y de las redes de Petri (RP). Existen varios enfoques que usan FA; en [Sampath et al., 1995] y [Sampath et al., 1998] se caracteriza la propiedad de diagnosticabilidad y se resuelven problemas de detección y localización de faltas en línea. Después de estos trabajos seminales, estos conceptos han sido extendidos y aplicados a diferentes áreas y herramientas formales. Por ejemplo, en [Lafortune, 2007] se aborda la diagnosticabilidad en sistemas distribuidos. En [Seatzu, 2005] y [Wu, 2005] se trata el problema de diagnóstico usando redes de Petri. Posteriormente, en [Dotoli et al., 2009] se usa un problema de programación entera para determinar cuál secuencia de transiciones fue disparada y así determinar la ocurrencia de una falta. En [Lefebvre, 2011] se usa una función probabilista para dar una medida a la ocurrencia de una falta; en [Ramírez et al., 2012] la propiedad de diagnosticabilidad se caracteriza usando RP Interpretadas (RPI); en [Ruiz et al., 2014] se presentan algoritmos para construir diagnosticadores y probar la diagnosticabilidad del sistema.

Un problema relacionado con la diagnosticabilidad es forzar la diagnosticabilidad en Sistemas de Eventos Discretos (SED). Esto significa, encontrar formas de hacer que un SED sea diagnosticable agregándole elementos al sistema, tales como sensores y/o controladores. Este problema ha sido abordado desde

diferentes puntos de vista. En [Ziqiand et al., 2014] la diagnosticabilidad es forzada seleccionando las palabras apropiadas para conseguir la detección de faltas y su aislamiento (diagnosticabilidad activa) para un caso específico y no se puede generalizar. En [Cabasino et al., 2013] se resuelve un problema de localización de sensor para garantizar la diagnosticabilidad. Por otro lado, en [Hernández et al., 2015] se presenta un enfoque para forzar la diagnosticabilidad en una clase de RP utilizando un controlador nombrado como un Circuito de Regulación [Densel, 1995], la solución es estructural y consiste en añadir nuevos lugares para restringir el disparo de las transiciones en la RPI. Sin embargo, la inclusión de estos lugares reduce el número y variedad de palabras que el sistema puede realizar y, si no se realiza adecuadamente, la inclusión de estos lugares puede bloquear a la red.

Este trabajo presenta una propuesta de diagnosticabilidad activa a través de un Circuito de Regulación Inteligente (CRI) en una clase de redes de RP que no es diagnosticable pero sí acotada y viva. La solución es estructural, considera un marcado de k marcas en el CRI para asegurar que la ocurrencia de cualquier falta pueda ser detectada y aislada.

En la siguiente sección se presentan la propuesta y los sustentos teóricos necesarios para su comprensión, así como la caracterización de una clase de RP donde se puede realizar un diagnóstico activo.

2. Métodos

Esta sección introduce los conceptos básicos de RP y diagnóstico que serán necesarios para la explicación del material presentado en el trabajo. Un lector interesado puede consultar las referencias [Densel, 1995] y [Murata, 1989] para más información.

Redes de Petri

- Una estructura de una red de Petri es un dígrafo bipartito definido por la 4-tupla $Q=(P,T,I,O)$, donde $P = \{p_1,p_2,...,p_n\}$, $T = \{t_1,t_2,...,t_m\}$ son conjuntos finitos de lugares y transiciones respectivamente. $P \cup T \neq \emptyset$ y $P \cap T = \emptyset$. $I: P \times T \rightarrow \{0,1\}$ y $O: P \times T \rightarrow \{0,1\}$ son las funciones de entrada y salida que

describen los arcos que van de los lugares a las transiciones y de las transiciones a los lugares respectivamente.

- Un marcado es una función M: P→{ 0,1,2,3,...} que asigna a cada lugar un numero entero no negativo, nombrado como el número de marcas que residen dentro de cada lugar. M_0 es la distribución inicial de marcado.
- Una red de Petri N es una estructura Q junto con un marcado inicial, esto se denota como N=(Q, M_0).
- La matriz de incidencia C de n×m de N está definida por C{i,j}= $O(t_j,p_i)-I(p_i,t_j)$. La notación •t={p|I(p,t)≠0}, t•={p|O(p,t)≠0},•p={t|O(p,t)≠0} y p•={t|I(p,t)≠0} representa los lugares de entrada y de salida de t, y las transiciones de entrada y de salida de p respectivamente.
- Sea (Q, M_0) una RP. Los vectores X_i tal que CX_i =0, X_i ≥ 0 son conocidos como T-semiflujos. El soporte de un T-semiflujo X_i, denotado por $\langle X_i \rangle$, es el conjunto de transiciones T_i = {t_j|$X_i(j) > 0$}. La subred T_i = {(P_i,T_i,I,O),M_{0i}} de N generada por el T-semiflujo X_i es una T-componente si P_i=(•$\langle X_i \rangle \cap \langle Xi \rangle$•), T_i=$\langle X_i \rangle$; I_i, O_i y M_{0i} son las funciones de entrada y salida, y el marcado inicial restringido a P_i y T_i respectivamente.

Una transición t_j se dice que está habilitada en el marcado M_k si este tiene $M_K(p_i)$ ≥ $I(p_i,t_j)$ marcas en cada lugar p_i de entrada a t_j. Una transición habilitada t_j se puede disparar, remueve $I(p_i,t_j)$ marcas de p_i y añade $O(t_j,p_k)$ marcas a p_k produciendo un nuevo marcado M_{k+1} (representado por $M_k \xrightarrow{t_j} M_{k+1}$) que puede ser calculado usando la ecuación de estado $M_{k+1} = M_k + C\vec{t_j}$ donde C es la matriz de incidencia y $\vec{t_j}(i)$ =1 si i=j y $\vec{t_j}(i)$=0 en cualquier otro caso.

Observe que $M_0 \xrightarrow{t_j} M_1$ puede ser extendido a una secuencia de transiciones $M_0 \xrightarrow{\sigma} M_q$ donde σ = $t_a t_b ... t_r$. En este caso M_q se dice que es alcanzable desde M_0. El conjunto de alcanzabilidad de N, denotado por R(Q, M_0), es el conjunto de todos los posibles marcados alcanzables desde M_0, disparando solamente las transiciones habilitadas:

Definición 1. Una RP (Q, M_0) es viva (o equivalentemente M_0 es un marcado de N vivo) si, no importa cual marcado ha sido alcanzado desde M_0, es posible disparar de última instancia cualquier transición de N al progresar a través de alguna secuencia de disparo adicional.

Definición 2. Una RP (Q, M_0) es k-segura si $\forall M \in R(Q, M_0)$ y $\forall p \in P$, $M(p) \leq k$. Si se cumple que $\forall M \in R(Q, M_0)$ y $\forall p \in P$, $M(p) \leq 1$, la red es llamada 1-segura (segura o binaria).

Definición 3. Una RP (Q, M_0) es fuertemente-conexa para cualesquiera dos nodos de la red X, Y (lugares o transiciones) hay un camino de X a Y y de Y a X.

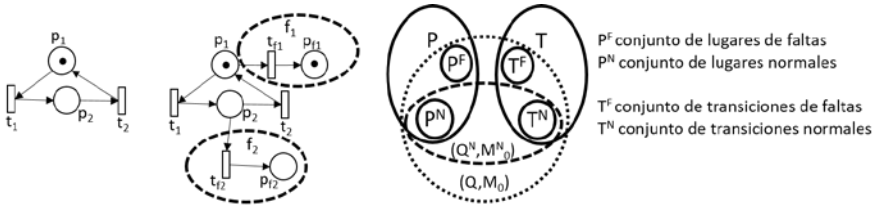
Definición 4. Un sifón (o cerrojo) es un subconjunto de lugares $S=\{p_1, \ldots, p_s\} \subseteq P$ de una RP tal que $\bullet S \subset S\bullet$. Las siguientes definiciones están relacionadas con la secuencia de transiciones de disparo con los vectores de observación de salida.

Definición 5. Una secuencia de transiciones de disparo en una RP (Q, M_0) es una secuencia $\sigma = t_i t_j \ldots, t_k, \ldots$ tal que $M_0 \xrightarrow{t_i} M_1 \xrightarrow{t_j} M_2 \ldots M_w \xrightarrow{t_k} \ldots$

En este trabajo se asume que la RP es evento-detectable, es decir, que el disparo de cualquier transición siempre es detectado. En [Ramírez et al., 2012] y [Rivera et al., 2005] se presenta esta propiedad. Gráficamente una RP se puede ver como en la figura 1a.

Diagnosticabilidad

En este trabajo sólo se consideran las faltas permanentes f_i. En la figura 1b se representan dos faltas permanentes f_1 y f_2 en una RP, estas son subredes. En la figura 1c se muestra los subconjuntos de lugares P y transiciones T considerados en la RP en estado normal y de falta.



a) Normal. b) Faltas c) Subconjuntos.

Figura 1 Conjuntos de P y T.

En este trabajo se supone que el disparo de las transiciones de falta no es evento-detectable. En el caso de que lo sea el problema de detección de faltas estaría resuelto.

La siguiente definición es tomada de [Ramírez et al., 2012].

Definición 6. Sea (Q, M_0) una RP y $t_{fi} \in T^F$. El conjunto de lugares de pre-riesgo de t_{fi} es $P_i^R = \{p_k | p_k \in \bullet t_i\}$. El conjunto de lugares de post-riesgo de t_{fi} es $P_i^{PR} = \{p_k | p_k \in (\bullet t_i)^{\bullet\bullet} \cap P^N\}$. El conjunto de transiciones de pre-riesgo de t_{fi} es $T_i^R = \{t_k | t_k \in \bullet P_i^R \cap T^N\}$ y el conjunto de transiciones de post-riesgo de t_{fi} es $T_i^{PR} = \{t_k | t_k \in \bullet P_i^{PR} \cap T^N\}$.

La propiedad de diagnosticabilidad entrada-salida de un SED basada en los modelos RP se define a continuación.

Definición 7. Una RP viva dada por (Q, M_0) es diagnosticable en $k < \infty$ pasos si usando cualquier secuencia de disparo de transiciones de longitud igual o mayor a k y la estructura de (Q, M_0) son suficientes para distinguir la ocurrencia de una falta en el SED. Esta definición es equivalente a la presentada en [Sampath et al., 1996] desde el punto de vista de las RP. Como se muestra en la figura 2, si un ciclo a) que contiene una falta f_i cuya salida RP es igual a otro ciclo b) que no contiene la falta f_i entonces la RP es no diagnosticable entrada-salida.

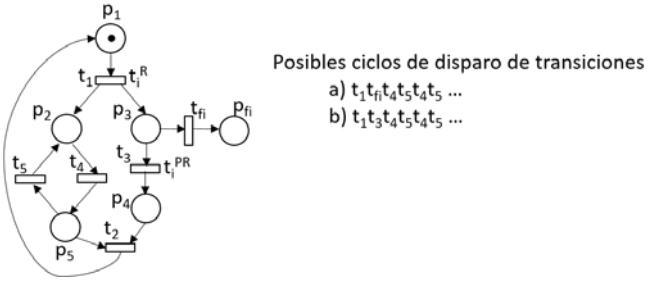


Figura 2 RP con ciclos de disparo indistinguibles.

Si $t_3 \in T^{PR}$ es evento-detectable (es decir, el disparo de esta transición se detecta), entonces los ciclos pueden distinguirse si t_3 pertenece a cualquier secuencia de disparo de transiciones finita. El intentar disparar t_3 y no poder hacerlo indica que su lugar de entrada no tiene marcas, y esto ocurre porque la marca está retenida en el lugar de falta, es decir ocurrió la falta. Por lo tanto, si la transición de post-riesgo está en cualquier secuencia finita en el comportamiento normal de la red,

entonces en un número finito de pasos se intentará disparar dicha transición, y su disparo o no disparo permite determinar si la falta existió. Este hecho se estudia a través de la distancia relativa [Ruiz et al., 2007] entre dos transiciones y los sifones [Densel, 1995] de la red.

Definición 8. Sea (Q, M_0) una RP limitada, la distancia relativa $D_R(t_i,t_j)$ entre cualquier par de transiciones $t_i,t_j \in T$, es el número máximo de veces que t_j puede ser disparado sin que se dispare t_i cuando una marca se retiene en el lugar $\bullet t_i$, esto es, el marcado que habilita a t_i no puede usarse para disparar la transición t_j. La distancia máxima relativa $D_H(t_i,t_j)$, entre cualquier par de transiciones $t_i,t_j \in T$ es $D_H(t_i,t_j)=\max\{D_R(t_i,t_j),D_R(t_j,t_i)\}$.

El problema de caracterizar la diagnosticabilidad de las faltas permanentes necesita el cálculo de las distancias máximas relativas. Este cálculo parece ser un problema complejo. Sin embargo, existen condiciones estructurales de la RP que pueden ser explotadas para determinar polinómicamente la distancia máxima relativa entre las transiciones en una clase de RP.

La siguiente proposición presentada en [Ruiz et al., 2014] caracteriza la diagnosticabilidad en términos de la distancia relativa máxima (si los sifones se desmarcan todas las transiciones no son vivas).

Proposición 1. Sea (Q, M_0) una RP limitada, donde (Q^N, M_0^N) es viva, acotada y fuertemente-conexa. Sea t_{fi} una falta permanente, p_k un lugar de riesgo y S_{ti} el sifón que se desmarcará cuando t_{fi} se dispare. Se asume que $|p_k\bullet|=1$ y la transición post-riesgo $t_a \in p_k\bullet$ y las transiciones pre-riesgo son evento-detectable. (Q, M_0) es diagnosticable respecto a t_{fi} si todos los T - semiflujos de la red contienen transiciones en $\bullet S_{ti} \cap S_{ti}\bullet$.

En la proposición anterior, la notación $\bullet S_{ti} \cap S_{ti}\bullet$ indica las transiciones de entrada y de salida a los lugares que forman el sifón S_{ti}.

Diagnosticabilidad Activa

Las RP que tienen ciclos indeterminados no son diagnosticables. Sin embargo, como se indica en [Hernández et al., 2015], es posible remover estos ciclos modificando la estructura de la RP. La modificación de la RP se realiza a través de

la adición de un Circuito de Regulación (CR) [Densel y Esparza, 1995]. Esto es, si ∃ un conjunto $T_r=\{t_i,t_j, \ldots t_q\}\subseteq T$ tales que $\bullet t_i=\bullet t_j=\ldots \bullet t_q$ entonces se añade un conjunto $C_r= \{p_i',p_j',\ldots,p_q'\}$ conocido como un CR para T_r y arcos tales que $\bullet p_i'=t_i, p_i'\bullet=t_j$, $\bullet p_j'=t_j,\ldots\bullet p_q'=t_q$ con una marca inicial en uno de los lugares de C_r.

Considere, por ejemplo, un estacionamiento automatizado que tiene tres entradas (Entrada1, Entrada2, Entrada3), una salida y cuatro cajones (Lugar1, Lugar2, Lugar3, Lugar4) para estacionarse. La figura 3 muestra de lado izquierdo un esquema del estacionamiento y de lado derecho su modelo en RP.

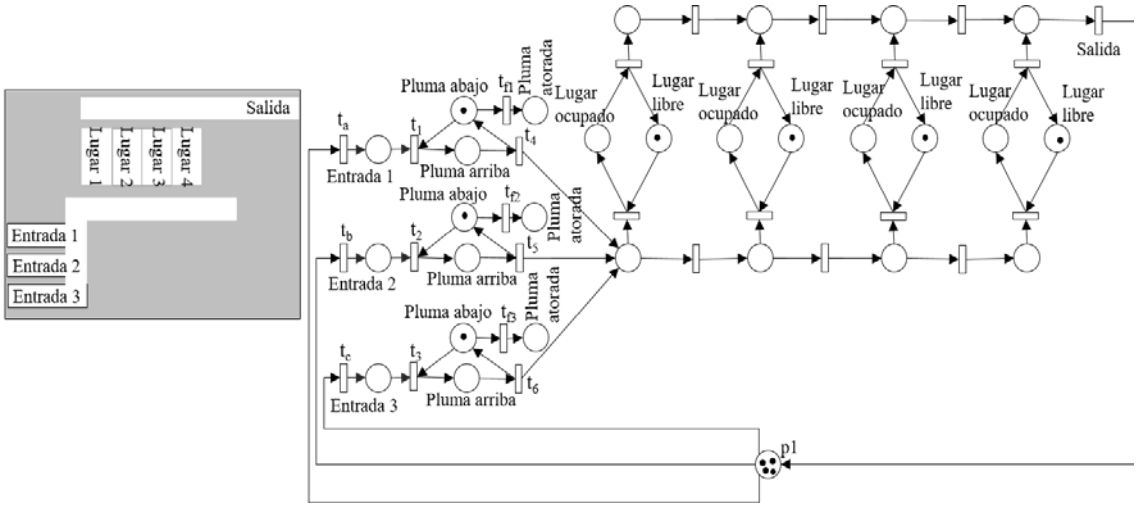


Figura 3 Estacionamiento de capacidad cuatro y su modelo en RP.

Imagine como faltas que las plumas fallen al levantarse ante la llegada de un coche. Hay muchas otras faltas, sin embargo, con la explicación de éstas bastará para ejemplificar al CRI y las demás faltas se pueden tratar exactamente igual. Las partes que destacar en el modelo son las secciones de entrada, las secciones de cada pluma de entrada y las posibles faltas donde las plumas se puede quedar atoradas. En este caso $t_4,t_5,t_6\in T^R$ son transiciones de pre-riesgo a las fallas de la pluma de la Entrada1 atorada, pluma de la Entrada2 atorada y pluma de la Entrada3 atorada respectivamente, y $t_1,t_2,t_3\in T^{PR}$ son transiciones de post-riesgo de las faltas de la Entrada 1, 2 y 3 respectivamente. Las transiciones $t_{f1},t_{f2},t_{f3}\in T^F$ son las faltas Pluma1 atorada, Pluma2 atorada y Pluma3 atorada, respectivamente. Haciendo el análisis de diagnosticabilidad se obtiene que $D_H(t_b,$

$t_1)=\infty$, $D_H(t_c, t_1)=\infty$, $D_H(t_a, t_2)=\infty$, $D_H(t_c, t_2)=\infty$, $D_H(t_a, t_3)=\infty$, $D_H(t_b, t_3)=\infty$, por lo que ninguna de las faltas es diagnosticable.

Según [Hernández et al., 2015] se debe poner un C_r en $\{t_a,t_b,t_c\}$ como se muestra en la figura 4 para que los T-semiflujos que pasan por $t_i,t_j, \ldots t_q$ se sumen creando un nuevo T-semiflujo que contenga transiciones en $\bullet S_{ti} \cap S_{ti} \bullet$ y el sistema se vuelva diagnosticable, es decir forzar la diagnosticabilidad. La parte resaltada en negro es el CR, si se dispara primero t_b luego se dispara t_a y por último t_c. Esto provoca que sólo una entrada esté habilitada a la vez, teniendo los coches que buscar dicha entrada y si están distantes entre sí, es inconveniente.

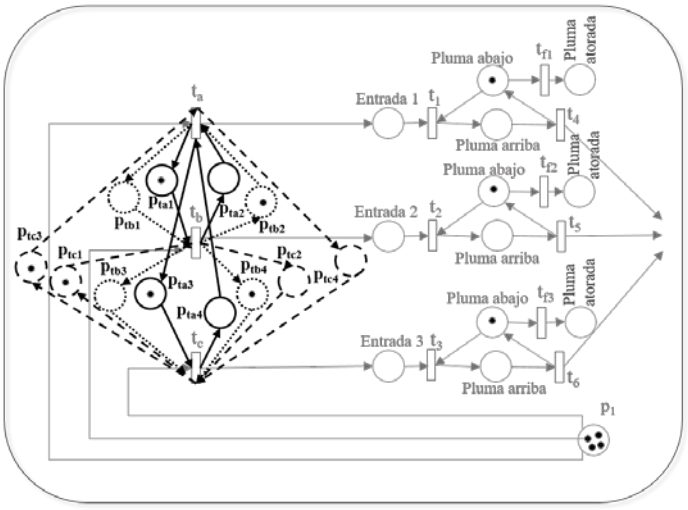


Figura 3 Modelo del estacionamiento con el C_r.

Circuito de Regulación Inteligente

Como se indicó anteriormente, forzar la diagnosticabilidad significa la eliminación de ciertas secuencias infinitas que incluyen las transiciones de pre-riesgo, pero que no incluyen las transiciones de post-riesgo. Durante este proceso pueden ocurrir dos cosas, la primera es que se eliminen secuencias de más y que pueden ser importantes para el sistema, y la segunda, que se generan secuencias que bloquean al sistema.

El CR presentado en trabajos anteriores introduce una solución que garantiza la vivacidad, pero establece una $D_H(t_i,t_j)=1$, eliminando la flexibilidad en el sistema. Además, introduce un orden estricto en el disparo de $t_i,t_j, \ldots t_q$, lo cual es limitante

en aplicaciones prácticas como el caso del estacionamiento. Ahora se propone un Circuito de Regulación Inteligente (CRI), que no impone ningún orden en las transiciones del sistema. El circuito sólo actúa cuando se requiere detectar si hay alguna falta. Esto ocurre cuando el circuito detecta el disparo de alguna transición de pre-riesgo y no se ha detectado el disparo de su transición de post-riesgo después de la ocurrencia de un número prestablecido de eventos.

Antes de la definición formal de CRI, se necesita la definición del conjunto de transiciones de regulación de falta, que es el conjunto de transiciones cuyo disparo se puede manipular para asegurar la detección de una falta.

Definición 9. Sea (Q, M_0) una RP y t_{fi} una transición de falta del sistema. Sea $T_{tfi}= \{t_i, t_j, ... t_q\} \subseteq T$ un conjunto de transiciones tales que $\bullet t_i = \bullet t_j = ... \bullet t_q$. El conjunto es un conjunto de transiciones de regulación de la falta t_{fi} si existe al menos una $t_a \in T_{tfi}$ tal que $D_H(t_a, t_x) = \infty$, donde t_x es la transición de post-riesgo de t_{fi}.

El disparo de las transiciones de este conjunto es el que se puede controlar para reducir la distancia relativa entre transiciones y detectar la falta. La siguiente proposición muestra que si existe una falta no diagnosticable t_{fi} entonces también existe el conjunto T_{tfi}.

Proposición 2*.* Sea (Q^N, M_0^N) una RP viva y acotada y fuertemente conexa. Sea $t_{fi} \in T^F$ y t_x su transición post-riesgo tal que existe t_j con $D_H(t_x, t_j)=\infty$ y $t_j \in T^N$. Entonces existe T_{tfi} que es el conjunto de transiciones de regulación de la falta t_{fi}.

Demostración. Tomar t_x la transición de post-riesgo de la falta t_{fi} para construir una trayectoria de nodos ascendente de la siguiente forma. Tomar los caminos desde t_x recorriendo la RP en sentido inverso a sus arcos hasta encontrar una transición t_a a la que se le puede encontrar un conjunto de transiciones $T=\{t_a, t_b, ... t_q\}$ tales que $\bullet t_a = \bullet t_b = ... \bullet t_q$. Tal transición existe, de lo contrario cada transición en el camino tiene exactamente un lugar de entrada y estos lugares sólo pueden habilitar las transiciones del camino. Como la red es fuertemente conexa, eventualmente se regresará a t_x formando un ciclo, aunque no necesariamente mínimo. Como la red es viva, se puede proponer un marcado inicial M_0 acotado que hace viva a la red. De este marcado inicial se puede hacer evolucionar a la red. Como los lugares sólo habilitan transiciones del camino y el camino es finito (los conjuntos de

transiciones y lugares en una red son finitos), eventualmente se deberá disparar t_x, es decir $D_H(t_x, t_j) < \infty$, una contradicción. Por lo tanto, existe el conjunto T y éste es el conjunto de transiciones de regulación de la falta t_{fi}. i.e. existe el conjunto $T_{tfi}=T$.

La demostración de la proposición anterior nos sugiere un algoritmo para construir los conjuntos de transiciones de regulación para la falta t_{fi}. Note que si se construye un conjunto T_{tf1} y se agrega un circuito de regulación como en [Hernández et al., 2015] a este conjunto, podría resultar en que todavía existen transiciones con distancia relativa infinita hacia la falta t_{fi}, entonces, por la proposición anterior, debe existir otro conjunto T_{tf2} con otras transiciones de regulación de falta. Este procedimiento se debe repetir tantas veces como sea necesario, hasta que la falta t_{fi} sea diagnosticable.

Ahora ya se puede definir el Circuito de Regulación Inteligente.

Definición 10. Sea $(Q^N, M_0{}^N)$ una RP viva, acotada y fuertemente conexa. Sea t_{fi} una transición de falta del sistema. Sea $T_{tk}= \{t_a, t_b, ... t_x\} \subseteq T$ un conjunto de transiciones de regulación de la falta t_{fi}. Un CRI para el conjunto T_{tk} está formado para cada $t \in T_{tk}$ por un lugar de auto-lazo p_{ai} para una transición $t \in T_{tk}$, un lugar de salida p_{ci} llamado contador para una transición $t \in T_{tk}$; para cada $t_j \in T^R$ un $p_j{}^R$ lugar de salida para la transición de pre-riesgo de t_j, para cada $t_z \in T^{PR}$ un $p_z{}^{PR}$ lugar de post-riesgo de salida a t_z y un algoritmo de toma de decisiones (STD) que calcula el marcado de los lugares agregados. En el marcado inicial todos los lugares de auto-lazo tienen una marca y los lugares contadores y de post-riesgo están desmarcados.

Los lugares de pre-riesgo están inicialmente marcados sólo si los lugares de entrada a la falta están inicialmente marcados. En la figura 5 se muestra el esquema del CRI. Los lugares mostrados son los añadidos. Hay un circuito por cada conjunto de transiciones de regulación de la falta f_i.

Funcionamiento del Circuito de Regulación Inteligente para la Falta X

Sea $T_{tx}= \{t_1, t_2, ... t_{nc}\}$, p_{ci}=lugar del contador i-ésimo, p_{+i}= lugar pre-riesgo i-ésimo, p_{-i}= lugar post-riesgo i-ésimo, p_{ai}= lugar de auto-lazo i-ésimo, k= el número máximo de veces que se pueden disparar algunas de las transiciones en el

conjunto de transiciones de regulación de la falta sin disparar alguna otra del mismo conjunto.

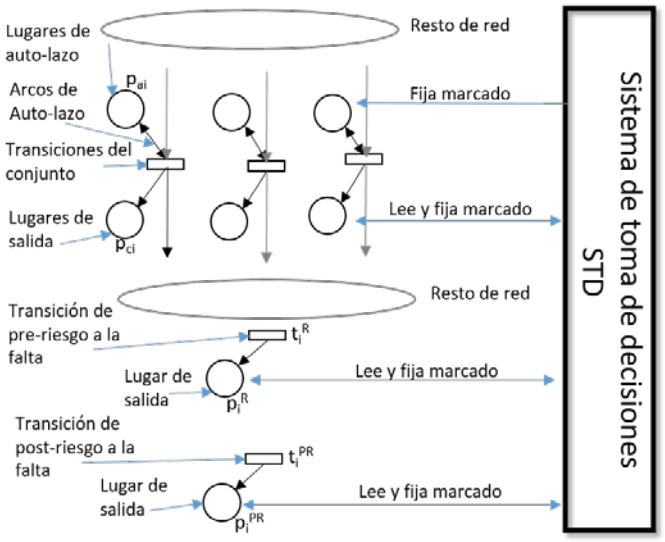


Figura 5 Circuito de regulación inteligente.

Etapa de Diagnostico activo

- Si $\forall p_{ci}\ M(p_{ci}) > 0$ entonces $\forall p_{ci}\ M(p_{ci}) = 0, \forall p_{ci}\ M(p_{ai}) = 1.$
- Si $\sum_{i=1}^{nc} M(p_{ci}) \geq k$ entonces $M(p_{ai}) = 0$ para $M(p_{ci}) > 0$.

Etapa de Diagnostico

- Si $M(p_{+i}) = 1$ entonces activar el disparo de t_i^{PR} (transición de post-riesgo de la falta i).
  a. Si se intentó disparar t_i^{PR} y $M(p_{-i}) = 0$ entonces error. Dejar $M(p_{ai}) = 0$ falta permanente.
  b. Si se intentó disparar t_i^{PR} y $M(p_{-i}) = 1$ entonces todas bien. $M(p_{-i}) = 0$.

Proposición 3. Sea (Q^N, M_0^N) una RP viva, acotada y fuertemente conexa. Sea $t_{fi} \in T^F$ no diagnosticable y $T_{tfi} = \{t_a, t_b, \ldots t_q\}$ uno de sus conjuntos de transiciones de regulación. Si se le añade un CRI a T_{tfi}, entonces la RP con CRI también es viva.

Demostración. Como la RP original es viva, entonces existen secuencias de disparo de transiciones desde el marcado inicial que marcan el lugar p, que es de

entrada a todas las transiciones de T_i (por definición todas las transiciones de T_i tienen el mismo lugar de entrada).

Aseveramos que como $\bullet t_a = \bullet t_b = \ldots \bullet t_q$, entonces el disparo de dos transiciones es independiente, es decir, se puede disparar una de ellas, por ejemplo, t_a, un número infinito de veces, sin necesidad de disparar alguna otra en el conjunto, por ejemplo, t_b. Suponer lo contrario, es decir que después de dispararse t_a un número máximo $k_a < \infty$ de veces se necesita el disparo de alguna otra transición, por ejemplo, t_b. Si t_a se dispara k_a veces y se marca de nuevo p, entonces se puede disparar cualquier transición en T_{ti}. En especial se puede disparar t_a nuevamente. Dos casos ocurren, que k_a no era el número máximo de veces que se dispara t_a o que se bloquee la red después del disparo de t_a. Como la red es viva y k_a ya era el máximo, ambos casos son una contradicción. Entonces el número de veces que se puede disparar cada transición sin disparar otra en T_{ti} es infinito.

Si las secuencias $t_a\sigma_1, t_b\sigma_2, \ldots, t_q\sigma_q$, son disparadas en la RP, entonces un subconjunto de ellas se dispara cuando se activa el CRI porque algunos lugares de auto-lazo tienen cero marcas. Como los disparos de $t_a, t_b, \ldots, t_q$ son independientes y vienen de secuencias vivas, entonces dichas secuencias permiten que el lugar p se siga marcando frecuentemente. Cada vez que se marca p una transición $t_q \in T_{ti}$ con $M(p_{aq})=1$ se dispara. Después del disparo $M(p_{aq})=0$, por lo que en la siguiente vez que se marque p se disparará una nueva transición y así hasta que todas las transiciones en T_{ti} se hayan disparado al menos una vez y en este momento el CRI para todas las $M(p_{ai})=1$. Cuando todos los lugares de auto-lazo están marcados, entonces se vuelve a tener todo el lenguaje de la RP y la red es viva.

Proposición 4. Sea $(Q^N, M_0{}^N)$ una RP viva, acotada y fuertemente conexa. Sea $t_{fi} \in T^F$ no diagnosticable con $t_x \in T^{PR}$ y $T_{tfi} = \{t_a, t_b, \ldots t_q\}$ uno de sus conjuntos de transiciones de regulación. Si se le añade un CRI a T_{tfi}, entonces t_{fi} se vuelve diagnosticable.

Demostración. Se sabe que $D_H(t_a, t_x) = \infty$ para una alguna transición en $t_a \in T_{tfi}$. Cuando el CRI detecta el disparo de la transición de pre-riesgo de t_{fi}, éste quita las marcas de los lugares auto-lazos de entrada a $t_q \in T_{ffi}$, siempre y cuando $D_H(t_q, t_x) =$

∞. Es decir, $t_q \in T_{tfi}$ ya no se puede disparar mientras que no se intente disparar t_x. Como la red es viva por la proposición anterior, la red no se bloqueará. Por lo tanto, la red se vuelve diagnosticable.

Proposición 5. Sea $(Q^N, M_0{}^N)$ una RP viva, acotada y fuertemente conexa. Sea $t_{fi} \in T^F$ no diagnosticable con $t_x \in T^{PR}$ y $T_{tfi} = \{t_a, t_b, ... t_q\}$ uno de sus conjuntos de transiciones de regulación. Si se le añade un CRI a T_{tfi}, entonces la ocurrencia de t_{fi} se detecta y diagnostica.

Demostración. El circuito de regulación inteligente detecta cuando se dispara la transición de pre-riesgo de t_{fi}. En este estado, el CRI reduce la distancia relativa de t_{fi} a todas las transiciones en uno por modificar los marcados en los lugares de auto-lazo. También detecta si se intenta disparar t_x. Si ésta se dispara entonces no hay falta, si ésta no puede dispararse, entonces no tiene marcas en sus lugares de entrada, esto sólo se debe a que ocurrió la falta t_{fi}. Por lo tanto, la falta se detecta y diagnostica.

3. Resultados

Ahora si se observa el modelo del estacionamiento de la figura 1 se puede notar que $T_{tf1}=T_{tf2}=T_{tf3}= \{t_a, t_b, t_c\}$ por lo que solo se requiere un CRI. La figura 6 muestra el CRI para el estacionamiento. Los lugares remarcados en obscuro son los agregados por el circuito, el resto, lugares claros, ya pertenecían al modelo en RP. En este caso los lugares p_{a1}, p_{a2} y p_{a3} son los lugares de auto-lazo, note que están inicialmente marcados permitiendo que las transiciones del sistema se disparen conforme lo requiera el sistema. Los lugares p_{c1}, p_{c2} y p_{c3} son contadores de ejecución de las transiciones a las que se conectan. Las transiciones $t_a, t_b, t_c \in T_{tk}$ son las transiciones que conforman los conjuntos de transiciones de regulación. Los lugares $\{p_{+1}, p_{+2}, p_{+3}\}$ y $\{p_{-1}, p_{-2}, p_{-3}\}$ son los lugares de pre-riesgo y post-riesgo a las faltas. Los lugares de pre-riesgo están marcados inicialmente porque las condiciones iniciales del sistema marcan los lugares pluma abajo que son de riesgo, aquí es donde puede ocurrir que la pluma se quede atascada provocando una falta.

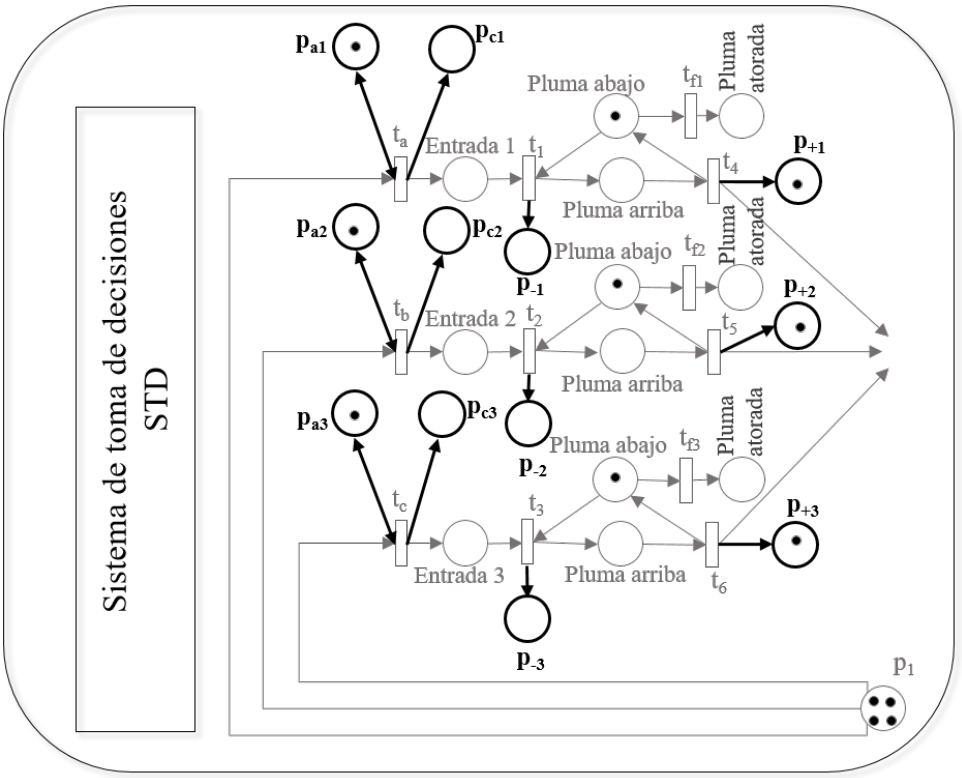


Figura 6 Modelo del estacionamiento don un CRI.

Se agrega un CRI, de acuerdo con la definición del CRI se tiene la siguiente forma de operar el conjunto con el CRI. Suponer que para cada falta se tiene la misma constante k=3, es decir a lo más tres coches pueden entrar al estacionamiento sin permitir el no uso de alguna de las entradas. Después de este número el STD debe trabajar para garantizar la diagnosticabilidad de las faltas. Suponer que entran dos carros por la entrada 1 y dos por la entrada 2, entonces el marcado de p_{c1} es igual a dos, lo mismo para p_{c2}. Entonces la suma de estos marcados es cuatro, indicando que cuatro coches entraron al estacionamiento sin usar la entrada 3, i.e. más de lo permitido. Entonces el STD desmarca los lugares p_{a1} y p_{a2} inhabilitando la entrada 1 y 2. Por lo que el siguiente coche que quiera entrar al estacionamiento deberá hacerlo por la entrada 3. Como el lugar p_{+3} tiene marca, el STD está consciente de la posible falta. Como las distancias relativas de todas las transiciones son finitas en la condición de los lugares p_{a1} y p_{a2} desmarcado, entonces eventualmente se intentará el disparo de t_c. Si se marca p_{-3} entonces el disparo de t_c se realizó y la pluma fue levantada indicando que no hay falta. En

este caso el STD pone los marcados a condiciones iniciales en los lugares de auto-lazo y contadores. También remueve la marca del lugar p_{-3}. Permitiendo nuevamente la máxima flexibilidad en el sistema y detectando que no hubo falta alguna. Si por el contrario el lugar p_{-3} no se marca entonces el STD marca que la falta t_{f3} está presente, por lo tanto, hay un error en la pluma de la tercera entrada. En este caso el STD pone el marcado de los lugares añadidos a condiciones iniciales, excepto p_{a3}, que lo pone en cero con el objetivo de no permitir acceso por esta entrada, ya que está dañada la pluma.

4. Discusión

Con base en los resultados se verifica que con el CRI no se requiere un orden estricto en el disparo de las transiciones a diferencia de tener un CR. Con el CR sólo se puede usar una entrada a la vez y dependiendo de la entrada que se seleccione primero se establece un orden para usar las otras entradas, pero con el CRI las tres entradas se pueden usar indistintamente, es decir, están disponibles en todo momento a excepción del instante en que se desee verificar si hay alguna falta en el sistema, especialmente si se detecta que una de las entradas no se utiliza. El CRI sólo actúa cuando se requiere detectar si hay alguna falta. Por otro lado, en la figura 4 se nota que un CR implica colocar más lugares a diferencia del uso del CRI de la figura 6 y otra cosa que se puede notar es que el CR modifica la estructura de la RP, pasando de 12 T-semiflujos a uno solo y con el CRI se mantiene la misma cantidad. Además, si se observara el lenguaje de la RP con el CRI se notaría que realmente no se restringe, sigue siendo el mismo y sólo se limita cuando se requiere verificar si existe o no una falta. Sin embargo, el lenguaje se limita drásticamente cuando se usa el CR porque sólo se puede usar una entrada a la vez. Algo importante que señalar es que el CR se propuso para RP binarias y aunque se ve en el ejemplo que se puede usar para RP no binarias no está analizado el caso, pero el CRI si se analiza para RP no binarias.

El sistema continúa conservando las propiedades de vivacidad y puede ser diagnosticable con la propuesta de la diagnosticabilidad activa. El diagnostico activo se aplica cuando no hay seguridad de que haya ocurrido una falta, pero es

probable que haya sucedido, esto ocurre cuando los usuarios eligen una sola entrada o dejan de usar una de las entradas y se puede verificar si todo está en orden o si puede haber ocurrido una falta.

El STD sirve para realizar el diagnóstico activo y considera las condiciones de funcionamiento del CRI, es el que controla cuándo revisar si ocurrió una falta después de que se usen las entradas k veces.

Es posible que los mismos usuarios ayuden a verificar el sistema cuando alguien elija otra entrada diferente a la que usan muchos usuarios y eso evitaría parar el sistema por un momento.

5. Conclusiones

Este trabajo reporta un diagnóstico activo para los SEDs y aplica los resultados al problema de diagnóstico de faltas de los sistemas de estacionamiento con tres entradas y una salida. Las principales contribuciones en el área son: 1) el diagnostico se realiza usando un Circuito de Regulación Inteligente, 2) se introduce una definición de diagnóstico activo para detección de faltas para SED controlables, y 3) los resultados son usados para diagnosticar un estacionamiento. Como trabajo futuro se considera extender el diagnóstico de otros tipos de faltas y a otras clases de RP, y contar con un algoritmo.

6. Bibliografía y Referencias

[1] Cabasino M.P., Lafortune S. and Seatzu C. Optimal sensor selection for ensuring diagnosability in labeled Petri nets. Automatica, vol. 49. Pp.2372-2383, 2013.

[2] Densel J. and Esparza J. Free Choice Petri Nets. University Press. Cambridge, 1995.

[3] Murata T. Petri nets: properties, analysis and applications. Proceedings of IEEE, vol.77. No.4. Pp.541-580, 1989.

[4] Dotoli M., Fanti M.P., Mangini A.M. and Ukovich W. On-line Fault Detection in Discrete Event Systems by Petri nets and Integer Linear Programming. Automatica, vol. 45. no. 11. Pp. 2665-2672, October 2009.

[5] Hernández-Rueda K., Meda-Campaña M.E. and Arámburo-Lizárraga J. Enforcing Diagnosability in Interpreted Petri Nets. IFAC-Papers On Line, vol. 48. No. 7. Pp. 58-63. DOI: 10.1016/j.ifacol.2015.06.473, 2015

[6] Lafortune S. and Genc S. Distributed diagnosis of place-bordered petri nets. IEEE Transactions on Automation Science and Engineering, vol.4. No. 2. April. Pp.206-219, 2007.

[7] Lefebvre D. and Leclerq E. Stochastic Petri nets identification for the fault detection and isolation of discrete event systems. IEEE Transactions on Systems, Man, Cybernetics, A., Syst. Humans, vol. 41. No. 2. Pp. 213-225, 2011.

[8] Ramírez-Treviño A., Ruiz-Beltrán E., Arámburo J. and López-Mellado E. Structural Diagnosability of DES and Design of Reduced Petri Net Diagnosers. IEEE Transactions on Systems, Man and Cybernetics, vol. 42. No.2. Pp. 416-429, 2012.

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

[10] Ruiz-Beltrán E., Ramírez-Treviño A. and Orozco-Mora J.L. Formal Methods in Manufacturing: Fault Diagnosis in Petri Nets. Edited by Javier Campos, Carla Seatzu and Xiaolan Xie. CRC Press Taylor-Francis Group. Boca Raton, FL. Pages 728, 2014.

[11] Ruiz-Beltrán E., Ramirez-Treviño A., López-Mellado E. and Arámburo-Lizárraga J. A Structural Characterization of Diagnosable Petri Net Models. Proceedings of the 3rdAnnual IEEE Conference on Automation Science and Engineering. Scottsdale, AZ, USA. Pp.1137-1142. Sept 22-25, 2007.

[12] Sampath M., Sengupta R., Lafortune S., Sinnamohideen and K., Teneketzis D.C. Diagnosability of discrete event systems. IEEE Transactions on Automatic and Control, vol.4. No.9. Pp.1555-1575, 1995.

[13] Sampath M., Sengupta R., Lafortune S., Sinnamohideen and K., Teneketzis D.C. Diagnosis of Discrete-Event Systems. IEEE Transactions on Automatic and Control, vol. 43. No.7. Pp. 908-929, 1998.

[14] Sampath M., Sengupta R., Lafortune S., Sinnamohideen K. and Teneketzis D.C. Failure Diagnosis Using Discrete-Event Models. IEEE Transactions on Control Systems Technology, vol.4. No. 2. Pp.105-124, 1996.

[15] Seatzu C. and Giua A. Fault Detection for Discrete Event Systems using Petri nets with unobservable transition. IEEE CDCD. Pp.6323-6328, December 2005.

[16] Wu Y. and Hadjicostis C. N. Algebraic approaches for fault identification in discrete-event systems. IEEE Trans. Robotics and Automation, vol. 50. No.12. Pp. 2048–2053, 2005.

[17] Ziqiang C., Feng L., Caisheng W. G., Wang L. Y. and Min X. Active Diagnosability of Discrete Event Systems and its Application to Battery Fault Diagnosis. IEEE Transactions on Control Systems Technology, vol.22. No.5. Pp.1892-1898, 2014.