Forcing faults diagnosis in K steps in discrete event systems

Forzar el diagnóstico de faltas en K pasos en sistemas de eventos discretos

HERNÁNDEZ-RUEDA, Karen†*, GONZÁLEZ-CASTOLO, Juan Carlos, RAMOS-CABRAL, Silvia and MARTÍNEZ-VARGAS, Martha Patricia

Universidad de Guadalajara

ID 1st Author: *Karen, Hernández-Rueda* / **ORC ID**: 0000-0002-7209-2907, **Researcher ID Thomson**: AAM-4861-2021

ID 1st Co-author: *Juan Carlos, González-Castolo* / **ORC ID**: 0000-0003-2659-0646, **Researcher ID Thomson**: R-5580-2018

ID 2nd Co-author: *Silvia, Ramos-Cabral* / **ORC ID**: 0000-0003-4204-1700, **Researcher ID Thomson**: R-7124-2018

ID 3rd Co-author: *Martha Patricia, Martinez-Vargas* / **ORC ID**: 0000-0002-0085-2567, **Researcher ID Thomson**: ABG-4110-2021

DOI: 10.35429/EJT.2021.10.5.11.21 Received July 12, 2021; Accepted December 30, 2021

Abstract

Discrete Event Systems occur naturally in engineering practice and include industrial processes, production systems, robotics, among others. So, its diagnosis is important. The aim of this work is to present a new approach to enforce faults diagnosis in Discrete Event Systems modeled by Interpreted Petri nets without limited to much its language. This approach is based on a Regulation Circuit that reduces the relative distance between any two pair of transitions that prevent the detection of the firing of transitions whose occurrence indicates that a fault occurred. By modifying the initial marks of the net that make up the Regulation Circuit, language limitation is avoided, and the diagnosis is established in k steps. First, the terminology used in the Interpreted Petri nets and the diagnosis are established, then the relationship between theses nets and the Regulation Circuit is reviewed to determine the characterization of nets where they can be added, they are analysed and then the proposal is made. The proposal is an option to force faults diagnosis in binary Interpreted Petri nets that are not diagnosable without limiting so much its language that represents their behavior.

Interpreted Petri nets, Faults Diagnosis, Discrete Event Systems

Resumen

Los Sistemas de Eventos Discretos ocurren naturalmente en la práctica de ingeniería e incluyen procesos industrials, sistemas de producción, robótica, entre otros. Por lo que es importante su diagnóstico. El objetivo de este trabajo es presentar un nuevo enfoque para fozar el diagnóstico de faltas en k pasos en Sistemas de Eventos Discretos modelados por redes de Petri Interpretadas sin limitar mucho su lenguaje. Este enfoque se basa en un Circuito de Regulación que reduce la distancia relativa entre dos transiciones que impiden la detección del disparo de transiciones que indican la ocurrencia de una falta. A través de la modificación de las marcas iniciales de la red que forman el Circuito de Regulación se evita la limitación del lenguaje y se instituye el diagnóstico en k pasos. Primero se establece la terminología usada en las redes de Petri Interpretadas y el diagnóstico, luego se revisa la relación entre esas redes y el Circuito de Regulación para determinar la caracterización de las redes donde se pueden añadir, se analizan y luego se hace la propuesta. La propuesta es una opción para forzar el diagnóstico de faltas en redes binarias que no son diagnosticables sin que limite tanto el lenguaje que representa su comportamiento.

Redes de Petri Interpretadas, Diagnóstico de faltas, Sistemas de Eventos Discretos

Citation: HERNÁNDEZ-RUEDA, Karen, GONZÁLEZ-CASTOLO, Juan Carlos, RAMOS-CABRAL, Silvia and MARTÍNEZ-VARGAS, Martha Patricia. Forcing faults diagnosis in K steps in discrete event systems. ECORFAN Journal-Taiwan. 2021. 5-10: 11-21

* Correspondence to Author (e-mail: karen.hrueda@academicos.udg.mx)
† Researcher contributing as first author.

Introduction

Currently there exist industrial systems larger and complex, dynamic systems, than previous ones to easy adapt to market demands. They can be called Discrete Event Systems (DES). DES evolves according to the occurrences of events, such as the arrival of a message or customer, the unexpected breakdown or scheduled shutdown of a machine, among many others. They can be suffering deviations from their specific behaviour (faults), compromising the systems and human operator safety. Hence, it is important fault diagnosis (fault detection and localization) task must be included it in modern controllers to avoid damage and increase system reliability. However, not all faults are diagnosable because no abnormal behaviour occurs that can be detected in the evolution of the DES, these DES are considered nondiagnosable and they are the interest of this work. So, it is necessary to study if they fulfil the diagnosability property (if they are diagnosable) and if they not, then how to make that they do.

Fault diagnosis of DES have been widely studied in the literature, some works (Sampath, Sengupta, Lafortune and Sinnamohideen, 1995) (Sampath, Sengupta, Lafortune, Sinnamohideen and Teneketzis, 1996) (Lafortune, Teneketzis and Sampath, 2001) use finite automata (FA) and others (Rivera-Rangel, Ramirez-Treviño, Aguirre-Salas and Ruiz-León, 2005) (De Tommasi, Basile, and Chiacchio, 2008) (De Tommasi, Basile, and Chiacchio, 2009) Petri nets (PN) for modelling DES. In (Lin, Wand, Chen, Han & Shen, 2017) a general framework for active on-line diagnosis using N-step lookahead windows that it is called active N-diagnosability is presented using FA. The advantage of PN is that may capture a lot of information about DES in small-size model and reduce computational complexity to solve diagnosis problems.

For example, in (Lefebvre and Leclerq, 2011) a probabilistic function is used to give a measure to the occurrence of a fault using a timed PN; in (Ramírez-Treviño, Ruiz-Beltrán, Arámburo and López-Mellado, 2012) the property of diagnosability is characterized in Interpreted RP (RPI) with a concept called a relative distance; in (Ruiz-Beltrán, Ramírez-Treviño and Orozco-Mora, 2014) algorithms are presented to build diagnostics and test the diagnosability of the system in IPN.

In (Basile, Tommasi and Sterle 2015) an Integer Linear Programming to find a minimal set of sensors of PN is presented to detect faults in at most k observations after their occurrence (k-diagnosable) ; in (Ran, Su, Giua and Seatzu, 2018) a verifier net is presented to make a codiagnosability analysis of bounded nets in decentralized PN models.

Diagnosability of DES deals with the possibility of detecting, within a finite delay, occurrences of unobservable fault events using the record of observed events. A related problem to the diagnosability is the enforcing diagnosability, this means, find out ways to make DES diagnosable adding elements in the system, such as sensors and/or controllers. In (Cabasino, Lafortune and Seatzu, 2013) a sensor location problem is solved to guarantee diagnosability, but this is impractical because of the number of reachable markings may increase exponentially according to the size of the net. In (Chen, Lin, Wang, Le Wang, and Xu, 2014) diagnosability is forced by selecting the appropriate words to achieve fault detection and isolation for a specific case and cannot be generalized.

In (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015) an approach is presented to force diagnosability in a class of RP adding new places (regulation circuit) to restrict the triggering of transitions in the RPI, but it reduces the number and variety of words that the system can perform.

On other hands, in (Ran, Giua and Seatzu, 2019) new sensors are added to enforce the diagnosability to labelled PN under a new labelling function that implies detect faults in at most k observations after their occurrence, based on works of (Basile, Tommasi and Sterle 2015) and (Ran, Su, Giua and Seatzu, 2018), although it can cope with the state explosion problem of both works and considers a Integer Lineal Problem instead of graph analysis, it implies two algorithms to obtain the k parameter using an automaton.

In (Basile, Tommasi and Sterle, 2020) a supervisory control strategy in bounded PN to enforce non-interference is proposed for a system that presents information leaks in distributed control systems, here is computed offline the minimal set of high-level transitions to be disabled to assure non-interference.

This paper presents a new approach to enforce diagnosability property of the DES modeled by an IPN, based on the Regulation Circuit RC from (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015) and the concept of k-diagnosability, i.e., after k steps it is possible determine if there exist or not a fault. This solution is structural, and it consists in adding k marks in the RC to constrain the firing of the PN transitions, but without restring the evolution of DES. The hypothesis considers that IPN fulfils structural and dynamics properties, and it is non diagnosable. This work is organized as follows. The following section presents basic concepts related with Petri and Interpreted Petri nets flowed by the faults diagnosis background, and Regulation Circuit and IPN subclasses. An IPN characterization that add a Regulation Circuit is shown, and the proposal is presented. Finally, the conclusions are given.

Background on Petri nets and Interpreted Petri nets

Next definitions introduce some basic PN and IPN concepts (Desel and Esparza, 1995) (Murata, 1998).

Definition 1. A PN structure is a bipartite digraph defined by the 4-tuple N = (P, T, I, O), where:

- $P = \{p_1, p_2, ..., p_n\}$, $T = \{t_1, t_2, ..., t_m\}$ are finite sets of places and transitions respectively.
- $P \cup T = \emptyset$ and $P \cap T = \emptyset$. $I: P \times T \rightarrow \{0, 1\}$ and $O: P \times T \rightarrow \{0, 1\}$ are the input and output functions describing the arcs going from places to transitions and from transitions to places respectively.

A marking is a function $M: P \rightarrow \{0, 1, 2, 3, ...\}$ that assigns to each place a non-negative integer number, named the number of tokens (marks) residing inside each place. M_0 is the initial token distribution. A PN is a PN structure together with an initial marking, it is denoted by (N, M_0). The n×m incidence matrix C of N is defined by $C(i, j) = O(t_j, p_i) - I(p_i, t_j)$. $\bullet t = \{p|I(p, t) = 0\}$, $t\bullet = \{p|O(p, t) = 0\}$, $\bullet p = \{t|O(p, t) = 0\}$ and $p\bullet = \{t|I(p, t) = 0\}$ represent the input and output places of t and input and output transitions of p respectively (Hernández-Rueda, Meda-Campaña and Arámburo Lizarraga, 2015).

Figure 1 shown an example of a PN, places are depicted by circles (p_1, p_2, p_3), transitions by boxes (t_1, t_2), arcs by arrows and tokens by black dots (black circle in p_1) or integer numbers residing inside each place.

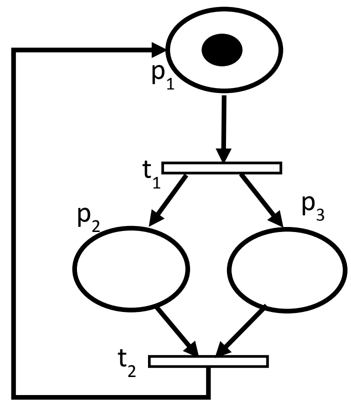

Figure 1 A Petri net example
Source: Own Elaboration

Definition 2: A P−semiflow Y_i (T− semiflow X_i) of a PN is a positive integer solution of the equation $Y_i^T C = 0$ ($CX_i = 0$). The support of the P−semiflow Y_i (T− semiflow X_i) is the set $\|Y_i\| = \{p_j \mid Y_i(p_j) \neq 0\}$ ($\|X_i\| = \{t_j \mid X_i(t_j) \neq 0\}$).

Definition 3: An IPN is the 4-tuple $Q = (G, \Sigma, \lambda, \varphi)$ where:

- $G = (N, M_0)$ is a PN.
- $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_r\}$is the input alphabet of the net, where α_i is an input symbol.
- $\lambda : T \rightarrow \Sigma \cup \{\varepsilon\}$ is a labeling function of transitions with the following constraint: $\forall t_j, t_k \in T$, $j \neq k$, if $\forall p_i$ $I(p_i, t_j) = I(p_i, t_k) \neq 0$ and both $\lambda(t_j) \neq \varepsilon$, $\lambda(t_k) \neq \varepsilon$, then $\lambda(t_j) \neq \lambda(t_k)$. In this case ε represents an uncontrollable (unobservable) system event and the transition is shadowed.
- φ is an output function represented by a q×n matrix $[\varphi_{ij}]$ such that $y_k = \varphi M_k$ is mapping of the marking M_k into the k-th the q−dimensional observation vector (IPN output). Column φ (•, i) is the elementary vector e_h if place p_i has associated the sensor place h; or the null vector if p_i has no associated sensor place. In this case, an elementary vector e_h is the q−dimensional vector with all its entries equal to zero, except entry h, that it is equal to 1. A null vector has all its entries equal to zero. IPN are drawn as PN, where non measurable places are shadowed (Figure 2).

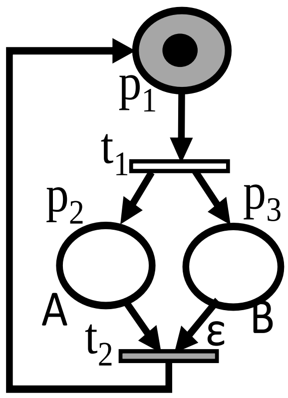

Figure 2 An Interpreted Petri net example
Source: Own Elaboration

Definition 4: A transition $t_j \in T$ of an IPN is enabled at marking M_k if $\forall p_i \in P$, $M_k(p_i) \geq I(p_i, t_j)$. An enabled transition t_j removes $I(p_i, t_j)$ tokens from p_i and adds $O(t_j, p_k)$ tokens to p_k if t_j is fired and then a new marking M_{k+1} is reached.

This fact is represented as $M_k \xrightarrow{t_j} M_{k+1}$; M_{k+1} can be computed using the dynamic part of the state equation represented by (1):

$$\begin{aligned} M_{k+1} &= M_k + C\vec{t_j} \\ y_k &= \varphi M_k \end{aligned} \qquad (1)$$

where *C* is the incidence matrix like in PN and $\vec{t_j}(i) = 1$ iff i=j, otherwise is equal to cero.

Definition 5: A firing transition sequence of an IPN (Q, M_0) is a sequence $\sigma = t_i t_j, \ldots t_k$ such that $M_0 \xrightarrow{\sigma} M_k$ ($M_0 \xrightarrow{t_i} M_1 \xrightarrow{t_j} \ldots M_j \xrightarrow{t_k} M_k$) where M_k is said to be reachable from M_0. The reachability set of Q, R (Q, M_0), is the set of all possible reachable markings from M_0 when is fired only enable transitions.

Remark Through this work (Q, M_0) will be used instead of $Q = (G, \Sigma, \lambda, \varphi)$ to emphasize the fact that there is an initial marking in an IPN.

Definition 6: The set of all firing sequence £ (Q,M_0), is called the firing language of (Q,M_0). £ $(Q, M_0) = \{ \sigma \mid \sigma = t_i t_j \ldots t_k$ where $M_0 \xrightarrow{t_i} M_1 \xrightarrow{t_j} \ldots M_k \}$.

Definition 7: A sequence of observation vectors (output symbols) of (Q, M_0) is a sequence $\omega = (y_0)(y_1) \ldots (y_n)$, where $y_k = \phi M_k$ and $y_i \neq y_{i+1}$.

If ω is a sequence of output symbols, then the set of firing transition sequences $\sigma \in$ £ (Q, M_0) whose firing generates the output sequence ω is represented by $\Omega(\omega)$ (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015).

Definition 8: Let (Q, M_0) be an IPN. The set $\Lambda(Q, M_0)$ denotes all sequences of output symbols of (Q, M_0). The set of all output sequences of length greater than or equal to k will be denoted by $\Lambda^k(Q, M_0)$, i.e., $\Lambda^k(Q, M_0) = \{\omega \in \Lambda(Q, M_0) \mid |\omega| \geq k\}$ (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015).

Definition 9: The set of all output sequences leading to an ending marking in the IPN (Q, M_0) is denoted by $\Lambda_B(Q, M_0)$, i.e., $\Lambda_B(Q, M_0) = \{\omega \in \Lambda(Q, M_0) \mid \exists \sigma \in \Omega(\omega)$ such that $M_0 \xrightarrow{\omega} M_j$ and M_j enables no transition, or when M_j enables t_i ($M_0 \xrightarrow{t_i}$) then $C(\bullet, t_i) = \vec{0}\}$ (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015).

Definition 10: An IPN (Q, M_0) is *k*-safe (*k*-bounded) if $\forall M \in R(Q, M_0)$ and $\forall p \in P$, $M(p) \leq k$. 1 − safe nets are simply called safe or binary.

Definition 11: An IPN (Q, M_0) is live if $\forall M_i \in R(Q, M_0)$ and $\forall t \in T$ it is true that $\exists \sigma$, such that $M_i \xrightarrow{\sigma} M_j \xrightarrow{t}$.

Definition 12: A siphon is a subset of places $S = \{p_1, \ldots, p_s\} \subseteq P$ of a IPN such that the set of input transitions •S is contained in the set of output transitions S•, i.e., •S ⊂ S•.

Definition 13: The PN structures is strongly connected if there exist directed paths form n_a to n_b and form n_b to n_a, where $n_a, n_b \in P \cup T$. (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015).

Definition 14: An IPN (Q, M_0) is event-detectable iff $\forall \sigma \in$ £(Q, M_0), the firing of any pair of transition $t_i, t_j \in \sigma$, can be distinguished from each other using the information in $\omega \in \Lambda(Q, M_0)$ (Ramírez-Treviño, Ruiz-Beltrán, Rivera-Rangel and López-Mellado, 2007).

Lemma 1: A live IPN (Q, M_0) is event-detectable iff $\forall$ $t_i,t_j \in T$ such that $\lambda(t_i)= \lambda(t_j)$ or $\lambda(t_j)= \varepsilon$ it holds that $\varphi C(\bullet, t_i) \neq \varphi C(\bullet, t_j)$, and $\forall$ $t_k \in T$ it holds that $\varphi C(\bullet, t_i) \neq 0$. The proof is in (Rivera-Rangel, Ramírez-Treviño, Aguirre-Salas and Ruiz-León, 2005).

Faults diagnosis Background

A fault is any event that changes the behavior of the DES such that it does not satisfy its purpose and does not behave according to the specifications. Faults that are considered here are permanent ones. A permanent fault occurs when a task stops its execution while other(s) task(s) can be continued to run in the system. A fault f_i is represented by transition t_{fi}, place p_{fi} and arc going from t_{fi} to p_{fi} is a IPN subnet (Figure 3), i.e., it is considered that a fault event modeled occurs when a t_{fi} (unobservable) is fired according to the rules and properties of the IPN.

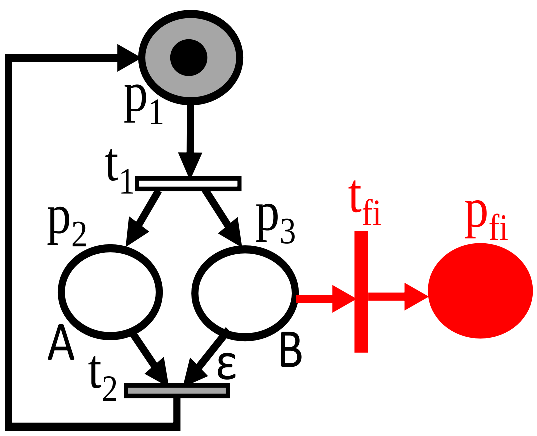

Figure 3 An IPN from a DES with a permanent fault f_i
Source: Own Elaboration

The set of places P of an IPN (Q, M_0), (Q, M_0) represents normal (Q^N, M_0^N) and fault behavior, is partitioned into two subsets $P = P^F \cup P^N$, where P^F represents the set of places modelling permanent faulty states, and P^N is the set of places coding normal states of the IPN. The set of transitions T of (Q, M_0) is partitioned into the following in two subsets too $T=T^N \cup T^{PF}$. They represent the normal and permanent fault transitions sets respectively, where $T^{PF} = {}^\bullet P^{PF}$ are not considered. Figure 3 represents an IPN (Q, M_0) with normal (Q^N, M_0^N) and fault behavior. In (Q^N, M_0^N) the set of places is $P^N = P - P^F$, the set of transitions is $T^N = T - T^{PF}$ and the set of arcs of (Q^N, M_0^N) is $A^N = ((P^N \times T^N) \cup (T^N \times P^N)) \cap (A)$, where $A = \{(p_i, t_j)|p_i \in P, t_j \in T \text{ and } I(p_i, t_j) = 1\} \cup \{(t_i, p_j)|p_i \in P, t_j \in T \text{ and } O(p_i, t_j) = 1\}$. In Figure 3, $P^N = \{p_1, p_2, p_3\}$, $P^F = \{p_{fi}\}$, $T^N = \{t_1, t_2\}$ and $T^{PF} = \{t_{fi}\}$.

Definition 15: Let (Q, M_0) be an IPN and $t_i \in T^{PF}$. The risky places set of t_i is $P^R = \{p_k|p_k \in {}^\bullet t_i\}$. The post-risk places set of t_i is $P^{PR} = \{p_k|p_k \in ({}^\bullet t_i)^{\bullet\bullet} \cap P^N\}$. The pre-risk transition set of t_i is $T^R = \{t_k|t_k \in {}^\bullet P^R \cap T^N\}$. The post-risk transition set of t_i is $T^{PR} = \{t_k \mid t_k \in P^{R\bullet} \cap T^N\}$ (Ramírez-Treviño *et al.*, 2007). In Figure 3, $P^R =\{p_3\}$, $P^{PR} = \{p_1\}$, $T^R = \{t_1\}$ and $T^{PR} =\{t_2\}$.

Diagnosability problem consist in determining if a system is diagnosable, i.e., if the occurrence of a fault can be detected in a finite number of steps, using the input-output system information. According to (Sampath 1996) if an F_i *-indeterminate cycle* (a transitions sequence that can be fired infinity and it contains a fault whose IPN output is the same to another transitions sequence without fault) appears in the reachability graph, then the IPN is not input-output diagnosable. Figure 4 shows an IPN that has a permanent fault f_i non diagnosable because it has a firing transitions sequence $\sigma = t_3t_4t_3t_4t_3t_4...$ that represents an indeterminate cycle with the firing transitions t_3t_4, this is an F_i *-indeterminate cycle*. An equivalent definition is the input-output diagnosability property of DES based on IPN.

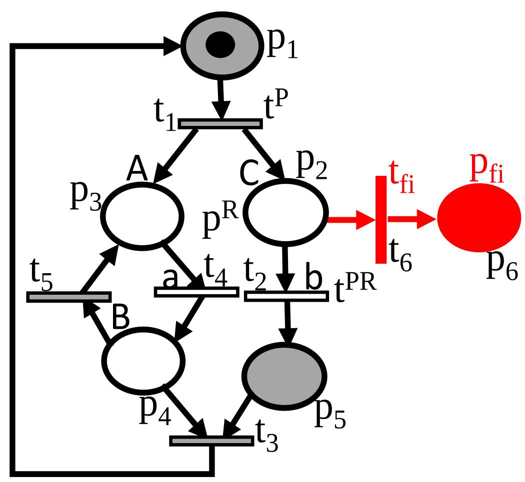

Figure 4 An IPN where a permanent fault f_i is not diagnosable
Source: Own Elaboration

Definition 16: An IPN (Q, M_0) is said to be input-output diagnosable in $k < \infty$ steps iff using any $\omega \in \Lambda^k(Q, M_f) \cup \Lambda_B(Q, M_f)$ and th structure of (Q, M_0) are sufficient for distinguishing the occurrence of faults in the DES (Ramírez-Treviño, Ruiz-Beltrán, Arámburo and López-Mellado, 2012).

As the firing of post-risk transitions can be detected from the IPN output sequence, are event-detectable, then an *F_i -indeterminate cycle* can be avoided if these transitions (post-risk transitions) belong to any finite transition firing sequence and this implies the notion of relative distance (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015) of IPN given in (Ruiz-Beltrán, Ramírez-Treviño, López-Mellado, and Arámburo-Lizárraga, 2007) and the siphons like in (Desel and Esparza, 1995).

Definition 17: Let (Q, M_0) be a binary IPN, the relative distance $D_R(t_i,t_j)$ between any pair of transition $t_i,t_j \in T$ is the maximum number of times that t_j can be fired without firing t_i when a token is held into places $\bullet t_i$, that is, the token cannot be used to fire the transition t_i. The maximum relative distance $D_H(t_i,t_j)$, between any pair of transitions $t_i,t_j \in T$ is $D_H(t_i,t_j) = \max\{ D_H(t_i,t_j), D_H(t_j,t_i)\}$ (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015).

Remark If for all pair of transitions in an IPN the $D_H(t_i,t_j) < \infty$, then the IPN is diagnosable, this implies that the IPN has not any *F_i -indeterminate cycle*.

Proposition 1: Let (Q, M_0) be a safe (Q^N, M_0^N) that is safe, live and strongly connected. Let t_i be a permanent fault, p_k be a risky place and S_{ti} be the siphon that will be unmarked when t_i is fired. Assume that $|p_k\bullet| =1$ and the post-risky transition $t_a \in p_k\bullet$ and the pre-risky transitions are event detectable. (Q, M_0) is diagnosable with respect to t_i if all the T-semiflows of the net contains transitions in $\bullet S_{ti} \cup S_{ti}\bullet$ (Ruiz-Beltrán, Ramírez-Treviño and Orozco-Mora, 2014). It is important to know that all transitions are not live when the siphons become unmarked.

Regulation Circuits and IPN subclasses

The IPN structure that is non diagnosable can be modified through the addition of a Regulation Circuit RC (Desel and Esparza, 1995) to be diagnosable. A RC is formed by new places in the IPN. The way in which the new places must be added to the IPN to it is still being live, binary, and event-detectable is introduced in the following definition, according to (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015).

Definition 18: Let (Q, M_0) be an IPN and $T_r = \{t_i, t_j, \ldots t_x\} \subseteq T$ be a set of transitions such that $\bullet t_i = \bullet t_j = \ldots \bullet t_x$. Then the set of places to be added to the IPN $C_r = \{p'_i, p'_j, \ldots, p'_x\}$ is a Regulation Circuit for T_r if $\bullet p'_i = t_i$, $p'_i\bullet = t_j$, $\bullet p'_j =$ tj, $\ldots\bullet p'_x = t_x$ and $p'_x\bullet = t_i$. Only one place in C_r is marked at the initial marking.

For the purpose to add a RC in a IPN that is non diagnosable, the usual IPN classification is follows.

Definition 19: Let N=(Q, M_0) be an IPN. N is state machine IPN (SM) if it is strongly connected, and every transition has one input and one output arc. N is a marked graph IPN (MG) if it is strongly connected, and every place has one input and one output arc. N is a free choice IPN (FC) if it is strongly connected and if $^\bullet t_i \cap {^\bullet t_j} \neq \emptyset$ then $^\bullet t_i = {^\bullet t_j}$. Other IPN clases are named general IPN for the purpose of this work. According to (Murata, 1989)(Desel and Esparza, 1995) the SM are live and binary if only one place of its places is marked in the initial marking with one token (Figure 5). MG are live and binary if the initial marking puts one token in every P-semiflow of the net (Figure 6). FC are live and binary if all the siphons include a proper trap initially marked and every P-semiflow contains only one token (Figure 7).

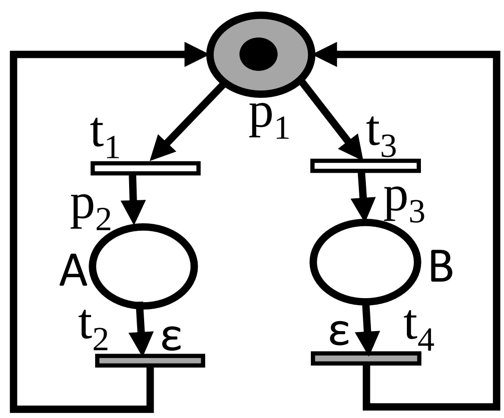

Figure 5 A SM IPN
Source: Own Elaboration

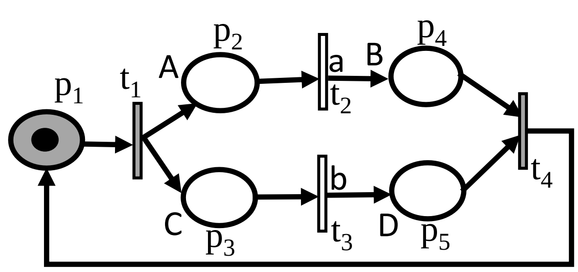

Figure 6 A MG IPN
Source: Own Elaboration

ISSN 2524-2121

Notice that RC cannot be used in MG since when two transitions have the same input place ($^\bullet t_i$ = $^\bullet t_j$ as required by the RC definition) implies that a place has two output arcs (one for t_i and another for $^\bullet t_j$), and places in MG have only one output arc. Then the D_H of every pair of transitions in this net is finite and no RC is required to reduce it. In other class of nets, however, D_H of every pair of transitions can be infinite and a RC can be used to reduce it.

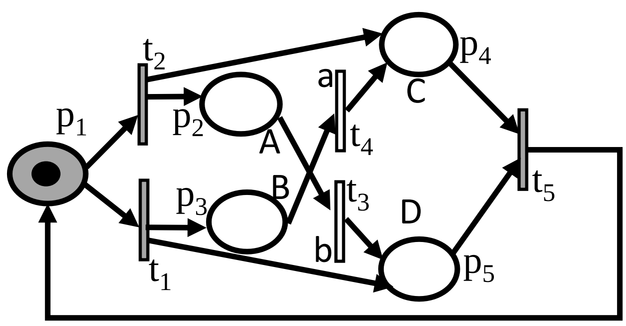

Figure 7 A FC IPN
Source: Own Elaboration

Proposition 2: Let (Q, M_0) be a live, binary, and event-detectable SM. Then adding a RC to this net, it continues being live, binary, and event-detectable SM (Figure 8).

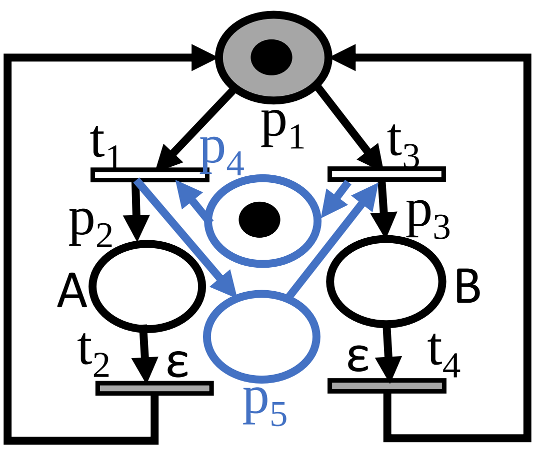

Figure 8 A SM IPN with a C_r
Source: Own Elaboration

Proof. In SM there exist transitions T_r= {t_i, t_j, …t_x} ⊆ T fulfilling that $\bullet t_i = \bullet t_j = \ldots \bullet t_x$. In this case, since transitions has only one input arc (*Definition 19*), then there exists a unique place p such that {p}= $\bullet t_i = \bullet t_j = \ldots \bullet t_x$. Since the SM is live, then it is live by places (Desel and Esparza, 1995), i.e. that if place p is marked and any transition $t_a \in T_r$ is fired, then there exists a sequence σ fired after t_a marking place p again. Then $M_p \xrightarrow{t_a\sigma} M_p$, where M_p marks place p.

Now, introduce the RC to the SM. When p is marked, then the RC will allow the firing of only one transition in T_r. Assume that this transition is $t_j \in T_r$ and it is fired (notice that t_j plays the role of t_a in the original net). Then according to previous reasoning, place p will be marked again ($M_p \xrightarrow{t_j\sigma'} M_p$). From this new marking the RC will allow the firing of only one transition in T_r –{t_j}. Assume that this transition is $t_k \in T_r$ and it is fired. Then according to previous reasoning, place p will be marked again. This process can be repeated until the last place of the RC is marked again and place p is marked again. In this case the process starts by firing t_j again and the SM with the RC is live.

The initial marking has only one token in place p_z and zero tokens to other places. Firing a transition t_x removes one token from p_z and adds it to place p_y. Place p_y has only one token in this new marking, otherwise in previous marking this place has a token, a contradiction. Thus the SM with the RC is binary.

Since, by hypothesis the original SM is evento-detectable, then the conditions of *Lemma 1* are satisfied. Adding the RC, new rows are added to the incidence matrix leading to a new incidence matrix given by (2)

$$C' = \begin{bmatrix} C \\ C_r \end{bmatrix} \quad (2)$$

and new columns are added to the output matrix φ leading to a new output matrix $\varphi' = [\![\varphi \quad 0]\!]$. Since the places of the RC are non measurable, then these columns are equal to the zero vector. Thus φ'C'= φC, then the net is still event-detectable.

Proposition 3: Let (Q, M_0) be a live, binary, and event-detectable FC. Then adding a RC to this net it continues being live, binary, and event-detectable FC.

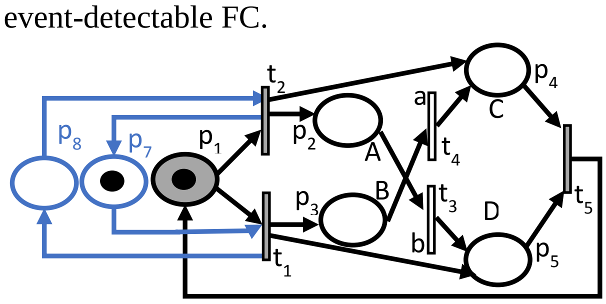

Figure 9 A SM IPN with a C_r
Source: Own Elaboration

Proof. In FC there exist transitions $T_r = \{t_i, t_j, \ldots t_x\} \subseteq T$ fulfilling that $\bullet t_i = \bullet t_j = \ldots \bullet t_x$. In this case there exist a set of places such that $\{p_a, \ldots p_e\} = \bullet t_i = \bullet t_j = \ldots \bullet t_x$. Since FC is live, then it is live by places (*Definition 19*), i.e., that places $\{p_a, \ldots p_e\}$ must be marked simultaneously allowing the firing of any transition in $t_a \in T_r$. When this transition is fired, then there exist a sequence σ fired after t_a marking again the places $\{p_a, \ldots p_e\}$ simultaneously. Then $M_p \xrightarrow{t_a\sigma} M_p$, where M_p marks places $\{p_a, \ldots p_e\}$.

Now, introduce the RC to the FC. When $\{p_a, \ldots p_e\}$ are marked, then the RC Will allow the firing of only one transition in T_r. Assume that this transiton is $t_j \in T_r$ and it is fired (notice that t_j plays the role of t_a in the original net). Then according to previous reasoning, places $\{p_a, \ldots p_e\}$ will be marked again ($M_p \xrightarrow{t_j\sigma'} M_p$). From this new marking the RC will allow the firing of only one transition in $T_r - \{t_j\}$. Assume that this transition is $t_k \in T_r$ and it is fired. Then according to previous reasoning, place p Will be marked again. This process can be repeated until the last place of the RC is marked again and place p is marked again. In this case the process starts by firing t_j again and the RC with the RC is live.

The initial marking has only one token in every P-semiflow. Firing a transtion t_x removes one token from its input places p_z and adds a token to its output places p_y. Place p_y has only one token, otherwise in previous marking these places have a token and there exist P-semiflows with more tan one marking at the initial marking, a contradiction. Thus the FC with the RC is binary.

Since, by hyphotesis the original FC is evento-detectable, then the conditions of *Lemma 1* are satisfied. Adding the RC, new rows are added to the incidence matrix leading to a new matrix given by (2) and new columns are added to the output matrix φ leading to a new output matrix $\varphi' = [\![\varphi \quad 0]\!]$. Since the places of the RC are non measurable, then these columns are equal to the zero vector. Thus φ'C'= φC, then the net is still event-detectable.

Notice that the reasoning used in *Proposition 2* and *Proposition 3* can be applied to any class of IPN. So, it can present the following proposition.

Proposition 4: Let (Q, M_0) be a live, binary and event-detectable IPN where a C_r can be added. If a C_r is added, then new IPN $(Q, M_0)'$ continues being live, binary and event-detectable.

IPN Characterization that add a Regulation Circuit

The maximum relative distance is reduced when a RC is added, but it is necessary to find out sets (T_r) where a RC can be defined and the maximum relative distance from a post-risk transition to other transitions is finite. Next definition indicates how the D_H is reduced.

Definition 20: Let (Q, M_0) be a live, binary and event-detectable IPN, and let $T_r = \{t_i, t_x\} \in T$ such that $\lambda(t_i) \neq \varepsilon$, $\lambda(t_x) \neq \varepsilon$, }, $\bullet t_i = \bullet t_x$ and $D_H(t_i,t_j) = \infty$. If it is possible to add a regulation circuit C_r for T_r such that the new IPN denoted as $(Q, M_0)' = (Q, M_0) + C_r$ fulfills that $(Q, M_0)'$ is binary, live and event-detectable, and $D_H(t_i,t_j) < \infty$, then $(Q, M_0)'$ is called $(t_i,t_j)D_H$ reducible.

To enforce the diagnosability in IPN according to the *Proposition 1*, it is necessary that the T-semiflows be modified and that the new IPN (resulting net) preserves the safeness and liveness properties (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015). Therefore, the following propositions are considered, and their proofs can be consulted in same reference.

Proposition 5: Let (Q, M_0) be a live, binary and event-detectable IPN. Let X_1 and X_2 be two minimum T-semiflows of the IPN. Let $T_r = \{t_i, t_h\}$ where $t_i \in \|X_1\|$, $t_i \notin \|X_2\|$, $t_h \in \|X_2\|$ and $t_h \notin \|X_1\|$. If a C_r is added, then the new IPN an $(Q, M_0)' = (Q, M_0) + C_r$ will have a minimum T-semiflow X_t, where $X_t = X_1 + X_2$.

Proposition 6: Let (Q, M_0) be a live, binary and event-detectable IPN. Let X_1 and X_2 be two minimum T-semiflows of the IPN, where $t_i, t_j \in \|X_1\|$, i.e. $D_H(t_i,t_j) < \infty$, $t_i, t_j \notin \|X_2\|$, $t_h \in \|X_2\|$ and $t_h \notin \|X_1\|$. Let $D_H(t_j,t_h) < \infty$ and $T_r = \{t_j, t_h\}$. If a C_r is added in the IPN, then $D_H(t_i,t_h) < \infty$.

Proposition 7: Let (Q, M_0) be a live, binary and event-detectable IPN. Let $t_{fi} \in T^{PF}$ and $t_x \in T^{PR}$. Let $D_H(t_x,t_j) = \infty$ where $t_j \in T^N$. Let X_1 and X_2 be two minimum T-semiflows of the IPN such that $t_x \in \|X_1\|$, $t_j \in \|X_2\|$. If there exist transititions $t_a \in \|X_1\|$, $t_b \in \|X_2\|$ such that $\bullet t_a = \bullet t_b$, then the IPN is (t_x,t_j) D_H reducible.

Proposition 8: Let (Q, M_0) be a live, binary and event-detectable IPN. Let $t_{fi} \in T^{PF}$ and $t_x \in T^{PR}$. Let $XT = \{X_1, \ldots, X_q, X_x\}$ be the set of minimum T-semiflows such that $t_x \in \|X_x\|$. If for each t_j such that $D_H(t_x,t_j) = \infty$, $t_x \in X_n \cap T^N$ and $X_n \in XT$ there exist transitions $t_a \in \|X_n\|$, $t_b \in \|X_x\|$, $n \neq x$ such that $\bullet t_a = \bullet t_b$ and a C_r is added, then the fault t_{fi} is diagnosable.

Example 1 Consider the IPN depicted on the Figure 4, its language is $£(Q,M_0)=(t_1(t_2V(t_4t_5))^*t_4t_3)^*$ in normal behavior, this net is non diagnosable, but is live, binary and event-detectable and has two T-semiflows $X_1=[111100]^T$ and $X_2=[000110]^T$. It has transitions $t_{fi} = t_6 \in T^{PF}$, $t_1 \in T^R$, $t_x= t_2 \in T^{PR}$ where $t_2 \in \|X_1\|$ and $t_j=t_5$ such that $D_H(t_2,t_5)=\infty$. Furthermore, there exist transitions $t_a = t_5 \in \|X_2\|$ and $t_b = t_3 \in \|X_1\|$ where $\bullet t_a = \bullet t_b$ ($\bullet t_3 = \bullet t_5$). So it is posible to add a $C_r=\{p_7,p_8\}$ between the transitions t_3 and t_5. The new IPN $(Q, M_0)' = (Q, M_0) + C_r$ is depicted on Figure 10. In this IPN $D_H(t_2,t_5) = 1 < \infty$ and the fault t_{fi} is diagnosable according to the *Proposition 1* (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015). If t_{fi} occurs then t_4t_5 is fired only one time. This net has one T-semiflow $X_1=[11121]^T$ as was indicated in *Proposition 5*, and its is language $£(Q,M_0)'=(t_1(t_2V(t_4t_5))^*t_4t_3)$.

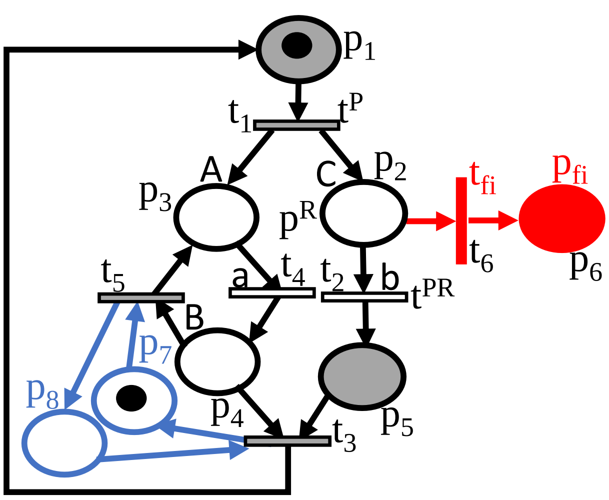

Figure 10 IPN $(Q, M_0)'$ from Figure 4 with a C_r where a permanent fault f_i is diagnosable
Source: Own Elaboration

The language $£(Q,M_0)'=(t_1(t_2V(t_4t_5))^*t_4t_3)$ is limited because the firing sequence $\sigma = t_4t_5$ only can be fired one time before the DES stops if the fault t_{fi} occurred. Also, if the fault does not occur, the firing sequence $\sigma = t_4t_5$ is fired first because the marking in $M(p_8)=0$. This modifies the behavior of the DES.

Regulation Circuit proposal

If the initial marking is 2 tokens, $M(p_7)=2$, instead of one token in the C_r added in the IPN depicted on Figure 10, then if the fault occurs, t_6 is fired and the firing transition sequence $\sigma= t_4t_5$ can be fired two twice, before the IPN stops to localize the fault, its language is $£(Q,M_0)'=(t_1(t_2V(t_4t_5)^2)^*t_4t_3)$ and $D_H(t_2,t_5) = 2 < \infty$. If the initial marking is 3 tokens, $M(p_7)=3$, then the firing transition sequence $\sigma= t_4t_5$ can be fired three times, its language is $£(Q,M_0)'=(t_1(t_2V(t_4t_5)^3)^*t_4t_3)$ and $D_H(t_2,t_5) = 3 < \infty$, and so on. So, it is possible to determine if a fault occurs after k steps with the initial marking k in the C_r ($M(p_7)=k$), i.e., the IPN is k-diagnosable according to (Basile, Tommasi and Sterle 2015). Moreover, if the initial marking is k the language of the IPN is $£(Q,M_0)'=(t_1(t_2V(t_4t_5)^k)^*t_4t_3)$, the language is less limited and $D_H(t_2,t_5) = k < \infty$. Also, $M(p_8) = k$ when the IPN stops. The initial marking k preserves the properties that the IPN already had, the same happens if there exist one token on p_8, $M(p_8) = 1$, but when a fault occurs after $\sigma= t_4t_5$ is fired k times, $M(p_8) = k+1$.

To not restring so much the language in the IPN where a RC can be added to enforce fault diagnosis, a new definition of C_r is proposed as follows.

Definition 21: Let (Q, M_0) be an IPN, k be a number of tokens and $T_r = \{t_i, t_j, \ldots t_x\} \subseteq T$ be a set of transitions such that $\bullet t_i = \bullet t_j = \ldots \bullet t_x$. Then the set of places to be added to the IPN $C_r = \{p'_i, p'_j, \ldots, p'_x\}$ is a Regulation Circuit for T_r if $\bullet p'_i = t_i$, $p'_i \bullet = t_j$, $\bullet p'_j = t_j$, $\ldots \bullet p'_x = t_x$ and $p'_x \bullet = t_i$. The initial marking k of one place of C_r is the number of times that an indeterminate cycle in the IPN can be fired and the other place has one initial marking.

It can use the same algorithm proposed by (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015) to removes indeterminate cycles with the new definition of RC.

ISSN 2524-2121

The Figure 11 shows k tokens as an initial marking of the IPN to fire k times the transition σ= t_4t_5 after the IPN stops, but if the IPN does not stop, it is possible that t_3 can be fired before that σ= t_4t_5 to know if a fault occurred. At this procedure guarantee that the language is less limited.

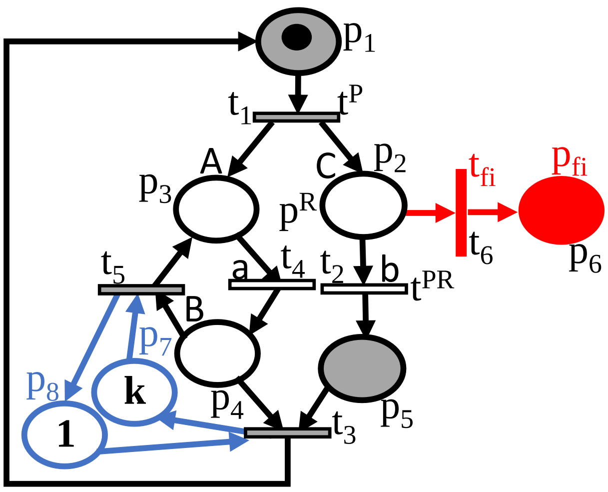

Figure 11 IPN (Q, M_0)' from Figure 10 with a new definition of C_r
Source: Own Elaboration

Conclusions

This paper presented a new approach to enforce the diagnosability in live, binary and event-detectable IPN, but non diagnosable, that represents a DES. The approach is based on the RC proposed by (Hernández-Rueda, Meda-Campaña and Arámburo-Lizarraga, 2015) with the modification of its initial marking to not limited so much the language of the net. The initial marking k is given to the place that can fire the indeterminate cycle and the initial marking one to the another. This approach is k-diagnosable because after k steps is possible detect if a fault is occurred. The maximum relative distance $D_H(t_i,t_j)$ is reduced to k. Also, a description of the IPN subclasses where a Regulation Circuit can be added was given. As future work it is considered a new C_r structure to enforce the property diagnosability without stop the IPN, until it wants to know if a fault occurred after k steps.

References

Basile F., De Tommasi G., and Sterle C. (2015). Sensors selection for K-diagnosability of Petri nets via integer linear programming. in Proc. *23rd Mediterranean Conf. Control Automat.*, Jun. pp. 168–175.

Basile F., De Tommasi G., and Sterle C. (2020). Non-interference enforcement via supervisory control in bounded Petri nets. *IEEE Transactions on Automatic Control*. DOI: 10.1109/TAC.2020.3024274

Cabasino M. P., Lafortune S., and Seatzu C. (2013). Optimal sensor selection for ensuring diagnosability in labeled Petri nets, *Automatica*, 49(8), 2373–2383.

Chen Z., Lin F., Wang C., Le Wang Y. and Xu M. (2014). Active Diagnosability of Discrete Event Systems and its Application to Battery Fault Diagnosis. IEEE *Transactions on Control Systems Technology*, 22(5), 1892-1898. Doi: 10.1109/TCST.2013.2291069.

De Tommasi G., Basile F., and Chiacchio P. (2008). "Sufficient conditions for diagnosability of Petri Nets". *Proceedings of the 9th International Workshop on Discrete Event Systems*. Göteborg, Sweden, May 28-30, 370-375.

De Tommasi G., Basile F., and Chiacchio P. (2009). An efficient approach for on-line diagnosis of discrete event systems. *IEEE Transactions on Automatic Control*, 54(4), 74-759, April.

Desel J. and Esparza J. (1995). Free Choice Petri Nets. University Press. Cambridge.

Hernández-Rueda K., Meda-Campaña M. E., and Arámburo-Lizárraga J. (2015). Enforcing diagnosability in interpreted Petri nets. *IFAC-PapersOnline*, 48 (7), 56–63.

Lafortune S., Teneketzis D. and Sampath M. (2001). Failure Diagnosis of Dynamic Systems: An approach based on Discrete Event Systems, *Proceedings of the American Control Conference*, 2058-2068.

Lefebvre D. and Leclerq E. (2011). Stochastic Petri nets identification for the fault detection and isolation of discrete event systems. *IEEE Transaction on Systems, MAN, Cybernetics, A., Syst. Humans.* 41(2), 213-225.

Liu F., Wang L. Y., Chen W., Han L. and Shen B. (2017). N-Diagnosability for Active On-line Diagnosis in Discrete Event Systems, *Automatica*, 83, 220-225. https://doi.org/10.1016/j.automatica.2007.06.004.

Murata T. (1989). Petri nets: properties, analysis and applications. *Proceedings of IEEE*, 77 (4), 541-580.

Ramírez-Treviño A., Ruiz-Beltrán E., Rivera-Rangel I. and López-Mellado E. (2007). Online Fault Diagnosis of Discrete Event System. A Petri Net Based Approach. *Transaction on Automation Science and Engineering*, 4(1), 31-39.

Ramírez-Treviño A., Ruiz-Beltrán E., Arámburo J. and López-Mellado E. (2012). Structural Diagnosability of DES and Design of Reduced Petri Net Diagnosers. *IEEE Transaction on Systems, MAN and Cybernetics.* 42(2), 416-429.

Ran N., Su H., Giua A., and Seatzu C. (2018). Codiagnosability analysis of bounded Petri nets. *Transactions on Automatic Control*, 63(4), 1192– 1199, Apr.

Ran N., Giua A., and Seatzu C. (2019). Enforcement of diagnosability in labeled Petri nets via optimal sensor selection. *IEEE Transactions on Automatic Control*, 64(7), 997–3004.

Rivera-Rangel I., Ramirez-Treviño A., Aguirre-Salas L. I., and Ruiz-León J. (2005). Geometrical characterization of observability in Interpreted Petri nets. *Kybernetika*, 41(5), 553–574.

Ruiz-Beltrán E., Ramírez-Treviño A., López-Mellado, and J. Arámburo-Lizárraga (2007). A Structural Characterization of Diagnosable Petri Net Models. *Proceedings of the 3rd Annual IEEE Conference on Automation Science and Engineering*. Scottsdale, AZ, USA, Sept22-25, 1137-1142.

Ruiz-Beltrán E., Ramírez-Treviño A., and Orozco-Mora J. L. (2014). Fault diagnosis in Petri nets. In J. Campos, C. Seatzu, and Xiaolan Xie, editors, Formal Methods in Manufacturing, chapter 22, pages 627–651. CRC Press, Boca Raton.

Sampath M., Sengupta R., Lafortune S., and Sinnamohideen K. (1995). Diagnosability of discrete-event system. *IEEE Transactions on Automatic Control*, 40(9), 1555–1575.

Sampath M., Sengupta R., Lafortune S., Sinnamohideen K., and Teneketzis D. (1996). Failure Diagnosis Using Discrete-Event Models. *IEEE Transactions on Control Systems Technology*. 4(2), 105-124.