Non-Concurrent Fault Identification in Discrete Event Systems Using Encoded Petri Net States[1]

Yingquan Wu and Christoforos N. Hadjicostis
Coordinated Science Laboratory and Dept. of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Abstract

In this paper we extend a previously developed coding-based methodology for monitoring faults in discrete event systems that are described by Petri nets. We present a systematic design that enables us to *non-concurrently* detect and identify a maximum of $2k-1$ transition faults *and* a maximum of k place faults that may occur at various instants during the operation of the system. Using an *encoded Petri net model* with $2k$ redundant places (and the connections and tokens associated with them), the worst-case complexity of the detection and identification procedure is $O(k^2(m+n))$, where n and m are respectively the number of places and transitions in the given Petri net model. The proposed fault detection and identification approach does not need to explicitly track or reconstruct the system state evolution and is well-suited for non-concurrent diagnosis.

I Introduction

Large-scale discrete event systems (DES) are subject to a number of diverse faults that tend to degrade their overall performance in unpredictable and possibly devastating ways. For dynamic systems, a commonly used approach to fault detection and identification (FDI) is to introduce analytical redundancy (characterized in terms of a parity space) and to diagnose faults based on parity relations [1], [2]. In [3] a methodology of this nature was developed for monitoring faults in DES that can be modeled by Petri nets. In its most general form, the approach encodes the state of the original Petri net by embedding it into a redundant one in a way that preserves the state, evolution and properties of the original Petri net, while enabling an external FDI mechanism to non-concurrently perform diagnosis. More specifically, faults are detected and identified via linear parity checks on the overall *encoded* state of the (redundant) Petri net embedding. The fault model allows for faults in the Petri net transitions and faults in the Petri net places and is briefly discussed in Section I.A.

[1]This work has been supported in part by NSF Career Award 0092696 and in part by NSF ITR Award 0085917.

In this paper we build on a special case of the approach in [3] that is based on *separate* Petri net embeddings. The approach in [3] and applications of it in the context of power systems in [4] explicitly considered single-FDI. In this paper we extend these ideas to multi-FDI by applying algebraic coding/decoding techniques. Our approach is able to simultaneously detect and identify up to $2k-1$ transition faults and up to k place faults using a separate Petri net embedding with $2k$ additional places (and the connections and tokens associated with them) with worst-case complexity $O(k^2(m+n))$, where m, n are the number of transitions and places respectively. The proposed approach does not need to continuously track the system process (other than the implicit tracking performed by the additional places) and does not need to reconstruct the various possible state evolution paths associated with it. Thus, it is well-suited for non-concurrent FDI (e.g., when FDI is performed periodically) and can potentially reduce the overhead in terms of the number of operations performed by the checking mechanism.

For the purpose of self-containment, in the subsequent two subsections we state the fault model and review the construction of separate redundant Petri net embeddings, both of which were introduced in [3] and are used here for our development.

A Fault model

Our approaches for fault detection and identification are based on three different fault models which allow us to abstract away from the particulars of a system implementation and the faults associated with it. Naturally, given a particular system and the corresponding Petri net model, we need to ensure that our fault model effectively captures the expected faults (i.e., a single fault is mapped into a manageable number of errors).

(i) A *transition fault* models a fault in the implementation of a certain transition. We say that transition T_j has a *post-condition fault* if no tokens are deposited at its output places (even though the tokens from its input places are used). Similarly, we say that transition T_j has a *pre-condition fault* if the tokens that are supposed to be removed from the input places are not removed (even though tokens are deposited at the corresponding

output places).

(*ii*) A *place fault* models a fault that corrupts the number of tokens in a single place of the Petri net.

(*iii*) The *additive fault model* is a generalization of the above fault models and is based on explicitly enumerating all faults that we would like to be able to detect and identify. Each fault f is modeled by its additive effect $\mathbf{e}_f$ on the fault-free state $\mathbf{q}_s[t]$ that the Petri net would be in had there been no faults. If fault occurrences are mutually independent so that the occurrence of a fault at a particular time epoch does not change the additive effect of faults at later time epochs, then we will be able to detect and identify faults by performing checks periodically/non-concurrently as long as we can ensure that enough "book-keeping" is done to guarantee that information about the occurrence of faults is not lost. The way this is achieved becomes clearer in the next section.

B Monitoring using separate redundant embeddings

To monitor faults in a given Petri net $\mathcal{S}$ with n places and m transitions, we construct a separate redundant Petri net embedding $\mathcal{H}$, i.e., a larger Petri net whose state $\mathbf{q}_h[t]$ is η-dimensional ($\eta = n + d, d > 0$) and satisfies

$$\mathbf{q}_h[t] = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{C} \end{bmatrix} \mathbf{q}_s[t] \tag{1}$$

for all time epochs t. Here $\mathbf{B}^+$ ($\mathbf{B}^-$) is the incidence matrix from transitions (places) to places (transitions), and $\mathbf{q}_s[t]$ is the state of the original Petri net $\mathcal{S}$, $\mathbf{I}_n$ is the $n \times n$ identity matrix and $\mathbf{C}$ is a $d \times n$ integer matrix to be designed. In order to guarantee that (1) is valid for all t, the state evolution of $\mathcal{H}$ is chosen to be

$$\begin{aligned} \mathbf{q}_h[t+1] &= \mathbf{q}_h[t] + \begin{bmatrix} \mathbf{B}^+ \\ \mathbf{CB}^+ - \mathbf{D} \end{bmatrix} \mathbf{x}[t] - \begin{bmatrix} \mathbf{B}^- \\ \mathbf{CB}^- - \mathbf{D} \end{bmatrix} \mathbf{x}[t] \\ &= \mathbf{q}_h[t] + \mathcal{B}^+ \mathbf{x}[t] - \mathcal{B}^- \mathbf{x}[t] \ , \end{aligned} \tag{2}$$

where $\mathbf{D}$ is a $d \times m$ integer matrix to be designed [3]. The d additional places in $\mathcal{H}$ form what we refer to as the *monitoring Petri net*.

By using a separate redundant Petri net embedding, we essentially encode the original state $\mathbf{q}_s[t]$ into a separate *codeword* $\mathbf{q}_h[t]$ that consists of the original state and the state of the additional monitoring places. One can check the validity of the codeword by using the parity check matrix $\mathbf{P} \stackrel{\triangle}{=} [-\mathbf{C} \ \ \mathbf{I}_d]$ as follows:

$$\mathbf{P}\mathbf{q}_h[t] = [-\mathbf{C} \ \ \mathbf{I}_d] \left(\begin{bmatrix} \mathbf{I}_n \\ \mathbf{C} \end{bmatrix} \mathbf{q}_s[t] \right) = \mathbf{0} \cdot \mathbf{q}_s[t] = \mathbf{0}. \tag{3}$$

Notice that in order to verify (3), the FDI mechanism needs to know the number of tokens in each place in the original Petri net and the monitoring Petri net.

Our objective in this paper is to develop a monitoring scheme that can efficiently detect and identify multiple transition and/or place faults by appropriately choosing matrices $\mathbf{C}$ and $\mathbf{D}$.

II Mathematical Background and Development

In this section we frequently make references to operations in the Galois Field GF(p), where p is a prime number. In these fields, addition and multiplication can essentially be treated as addition and multiplication modulo p.

For notational simplicity, we define

$$\begin{aligned} &\Lambda_\tau(x_1, x_2, \ldots, x_r) \\ &\stackrel{\triangle}{=} (-1)^\tau \sum_{1 \le i_1 < i_2 < \ldots < i_\tau \le r} x_{i_1} x_{i_2} \ldots x_{i_\tau} \quad \tau \le r \ , \end{aligned} \tag{4}$$

and, for consistency, we set $\Lambda_0(x_1, x_2, \ldots, x_r) = 1$ and $\Lambda_\tau(x_1, x_2, \ldots, x_r) = 0$ for any $\tau > r$. Clearly, we have the following general equality:

$$\begin{aligned} &x^r + \Lambda_1(x_1, x_2, \ldots, x_r) x^{r-1} + \Lambda_2(x_1, x_2, \ldots, x_r) x^{r-2} \\ &+ \ldots + \Lambda_r(x_1, x_2, \ldots, x_r) = \prod_{i=1}^{r} (x - x_i). \end{aligned} \tag{5}$$

We also define

$$\mathcal{S}_\tau(x_1, x_2, \ldots, x_r) \stackrel{\triangle}{=} \sum_{i=1}^{r} x_i^\tau. \tag{6}$$

For the remainder of this paper, when there is no ambiguity in the context, we will use Λ_τ, $\mathcal{S}_\tau$ to represent $\Lambda_\tau(x_1, x_2, \ldots, x_r)$, $\mathcal{S}_\tau(x_1, x_2, \ldots, x_r)$ respectively.

Proposition 1 *Let $x_1, x_2, \ldots, x_r$ be r variables and $p > r$. Then,*
(i) Λ_i and $\mathcal{S}_i$, $i = 1, 2, \ldots, r$, satisfy the following relations in GF(p):

$$\begin{cases} \mathcal{S}_1 + \Lambda_1 = 0, \\ \mathcal{S}_2 + \Lambda_1 \mathcal{S}_1 + 2\Lambda_2 = 0, \\ \quad \vdots \\ \mathcal{S}_r + \Lambda_1 \mathcal{S}_{r-1} + \ldots + \Lambda_{r-1} \mathcal{S}_1 + r\Lambda_r = 0. \end{cases} \tag{7}$$

(ii) If $s_1 = \mathcal{S}_1, s_2 = \mathcal{S}_2, \ldots, s_r = \mathcal{S}_r$, then there is at most one solution (up to reordering of the elements). Specifically, $x_1, x_2, \ldots, x_r$ are the r roots of the equation

$$x^r + \Lambda_1 x^{r-1} + \Lambda_2 x^{r-2} + \ldots + \Lambda_{r-1} x + \Lambda_r = 0, \tag{8}$$

where the Λ_i, $i = 1, 2, \ldots, r$, can be obtained uniquely from (7). □□

The equations in (7) are known as Newton's identities; refer to [5] for the details of the proof. We highlight that the above equality is consistent to setting $\Lambda_\tau(x_1, x_2, \ldots, x_r)$ to zero for any $\tau > r$ in the previous paragraph. Clearly,

$$\Lambda_i \stackrel{\triangle}{=} \mathcal{F}_i(\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_i) = \frac{1}{i!} \begin{vmatrix} S_1 & 1 & 0 & \ldots & 0 & 0 \\ S_2 & S_1 & 2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ S_{i-1} & S_{i-2} & S_{i-3} & \ldots & S_1 & i-1 \\ S_i & S_{i-1} & S_{i-2} & \ldots & S_2 & S_1 \end{vmatrix}, \quad (9)$$

$i = 1, 2, \ldots, r$, are independent of the number of original variables $x_1, x_2, \ldots$. (Note that since Λ_i has a factor $\frac{1}{i!}$, $\mathcal{F}_i$, $i = 1, 2, \ldots, r$, are well defined only if $p > r$.) Now, we deduce this observation to a particular condition, as identified in the following proposition.

Proposition 2 *Let S_i, T_i, $i = 1, 2, \ldots, \tau$, be 2τ arbitrary given parameters in GF(p) with $p > \tau$. Then,*

$$\mathcal{F}_\tau(S_1 + T_1, S_2 + T_2, \ldots, S_\tau + T_\tau) = \sum_{i=0}^{\tau} \mathcal{F}_i(S_1, S_2, \ldots, S_i) \mathcal{F}_{\tau-i}(T_1, T_2, \ldots, T_{\tau-i}). \quad (10)$$

The proof is by induction and is omitted because it is lengthy and tedious. The next proposition follows straightforwardly from Proposition 2.

Proposition 3 *Let $x_1, x_2, \ldots, x_r$ be r variables and $s_1, s_2, \ldots, s_\tau$ be τ given parameters in GF(p) with $p > \tau$. Then,*

$$\mathcal{F}_\tau(s_1 + \mathcal{S}_1,\ s_2 + \mathcal{S}_2,\ \ldots,\ s_\tau + \mathcal{S}_\tau) = \sum_{i=0}^{\min\{r,\,\tau\}} \mathcal{F}_{\tau-i}(s_1, s_2, \ldots, s_{\tau-i}) \cdot \Lambda_i \,. \quad (11)$$

III Non-Concurrent Detection and Identification of Transition Faults

In this section we discuss non-concurrent detection and identification of *up to k transition faults* ($k < p$) within the epoch interval $[1, N]$. Here, the term "non-concurrent" means that checking and diagnosis are performed once every N time epochs, instead of every epoch. We assume that each transition may not suffer both pre-condition and post-condition faults within the epoch interval $[1, N]$. (Actually, if a particular transition suffers the same number of pre-condition and post-condition faults within $[1, N]$, their effects will be cancelled, making their non-concurrent detection impossible, at least under the set up of this paper.)

Let $\mathbf{e}_T^+ \in (\mathbb{Z}^+)^m$ be an indicator vector of post-condition faults and $\mathbf{e}_T^- \in (\mathbb{Z}^+)^m$ denote an indicator vector of pre-condition faults. The erroneous state $\mathbf{q}_f[N]$ at time epoch N is given by

$$\mathbf{q}_f[N] = \mathbf{q}_h[N] - \mathcal{B}^+ \mathbf{e}_T^+ + \mathcal{B}^- \mathbf{e}_T^- \,, \quad (12)$$

where $\mathbf{q}_h[N]$ is the state that would have been reached under fault-free conditions [3]. The error syndrome at time epoch N is then easily calculated to be

$$\begin{aligned} \mathbf{s}[N] &= \mathbf{P}\mathbf{q}_f[N] \\ &= [-\mathbf{C}\ \ \mathbf{I}_d](\mathbf{q}_h[N] - \mathcal{B}^+ \mathbf{e}_T^+ + \mathcal{B}^- \mathbf{e}_T^-) \\ &= \mathbf{D}\mathbf{e}_T, \end{aligned} \quad (13)$$

where $\mathbf{e}_T \stackrel{\triangle}{=} \mathbf{e}_T^+ - \mathbf{e}_T^-$ and $\mathbf{D}$ is a $d \times m$ matrix to be determined.

The expression in Eq. (13) indicates that k or less transition faults are detectable (respectively, identifiable) if and only if $\mathbf{s}[N] \stackrel{\triangle}{=} \mathbf{D}\mathbf{e}_T$ is nonzero (respectively, unique) for any $\mathbf{e}_T$ such that $|\mathbf{e}_T| \stackrel{\triangle}{=} \sum_{i=1}^m |e_T^i| \leq k$ (by assumption no cancellations take place in $\mathbf{e}_T$, i.e., no transition suffers both a pre-condition and a post-condition fault within epoch interval $[1, N]$, i.e., $|\mathbf{e}_T| = |\mathbf{e}_T^+| + |\mathbf{e}_T^-|$). In the following, we aim to design $\mathbf{D}$ to achieve this objective. (Note that $\mathbf{C}$ does not directly enter the development here; we consider it later when we discuss detection and identification of place faults.)

If p is a prime number larger than m, the following choice[1] for matrix $\mathbf{D}$

$$\mathbf{D} \stackrel{\triangle}{=} \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & 2 & 3 & \ldots & m \\ 1 & 2^2 \bmod p & 3^2 \bmod p & \ldots & m^2 \bmod p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2^k \bmod p & 3^k \bmod p & \ldots & m^k \bmod p \end{pmatrix} \quad (14)$$

allows the detection and identification of up to k transition faults. We show this by demonstrating that the error syndrome $\mathbf{s}[N] = \begin{bmatrix} s_0 & s_1 & s_2 & \ldots & s_k \end{bmatrix}^T$ is nonzero and unique for any $\mathbf{e}_T$ that satisfies $|\mathbf{e}_T| \stackrel{\triangle}{=} \sum_{i=1}^m |e_T^i| \leq k$.

Note that $s_0 = |\mathbf{e}_T^+| - |\mathbf{e}_T^-|$ (for notational simplicity let $\tau \stackrel{\triangle}{=} s_0$). Without loss of generality, we assume $\tau \geq 0$ and show that each combination of up to k faults causes a unique (nonzero) output syndrome $\mathbf{s}[N]$, implying that all combinations of up to k transition faults are identifiable. Suppose that a combination of $\tau + i$ post-condition faults and i pre-condition faults $[x_1, x_2, \ldots\ x_{\tau+i}, x_{\tau+i+1}, \ldots, x_{\tau+2i}]$ $(\tau + 2i \leq k)$ results in the same syndrome as a combination of

[1] As will become evident in Section V, $\mathbf{C}$ can always be chosen to allow $\mathbf{D}$ as in (14), as long as each transition has at least one input place and at least one output place.

$\tau + j$ post-condition faults and j pre-condition faults $[y_1, y_2, \ldots, y_{\tau+j}, y_{\tau+j+1}, \ldots, y_{\tau+2j}]$ ($\tau+2j \le k$). Then, It easily seen that the following equation array holds:

$$\begin{cases} \sum_{l=1}^{\tau+i} x_l + \sum_{l=\tau+j+1}^{\tau+2j} y_l \equiv \sum_{l=1}^{\tau+i} y_l + \sum_{l=\tau+i+1}^{\tau+2i} x_l, \\ \sum_{l=1}^{\tau+i} x_l^2 + \sum_{l=\tau+j+1}^{\tau+2j} y_l^2 \equiv \sum_{l=1}^{\tau+j} y_l^2 + \sum_{l=\tau+i+1}^{\tau+2i} x_l^2, \\ \qquad\qquad \vdots \\ \sum_{l=1}^{\tau+i} x_l^k + \sum_{l=\tau+j+1}^{\tau+2j} y_l^k \equiv \sum_{l=1}^{\tau+j} y_l^k + \sum_{l=\tau+i+1}^{\tau+2i} x_l^k, \end{cases} \tag{15}$$

where the equality is now taken modulo p. For notational simplicity, in the sequel we use notation "$\equiv$" to stand for equality modulo p. Since $\tau + i + j \le k$, we can use Proposition 1 to argue that $i = j$ and that, ignoring order, $\{x_1, x_2, \ldots, x_{\tau+2i}\} = \{y_1, y_2, \ldots, y_{\tau+2j}\}$. This establishes the uniqueness of syndrome $\mathbf{s}[N]$ under this combination of transition faults. Therefore, the matrix $\mathbf{D}$ defined in (14) allows the detection and identification of k or less transition faults.

Next, we aim to establish an efficient identification algorithm. Without loss of generality, we assume that $\tau + r$ post-condition faults and r pre-condition faults have taken place ($\tau + 2r \le k$), and consider the following equation array:

$$\begin{cases} \sum_{l=1}^{\tau+r} (x_l \bmod p) - \sum_{l=\tau+r+1}^{\tau+2r} (x_l \bmod p) & = s_1, \\ \sum_{l=1}^{\tau+r} (x_l^2 \bmod p) - \sum_{l=\tau+r+1}^{\tau+2r} (x_l^2 \bmod p) & = s_2, \\ & \vdots \\ \sum_{l=1}^{\tau+r} (x_l^{\tau+2r} \bmod p) - \sum_{l=\tau+r+1}^{\tau+2r} (x_l^{\tau+2r} \bmod p) & = s_{\tau+2r}. \end{cases}$$

We can weaken and rewrite the above equation array in the following form:

$$\begin{cases} \sum_{l=1}^{\tau+r} x_l & \equiv s_1 + \sum_{l=\tau+r+1}^{\tau+2r} x_l, \\ \sum_{l=1}^{\tau+r} x_l^2 & \equiv s_2 + \sum_{l=\tau+r+1}^{\tau+2r} x_l^2, \\ & \vdots \\ \sum_{l=1}^{\tau+r} x_l^{\tau+2r} & \equiv s_{\tau+2r} + \sum_{l=\tau+r+1}^{\tau+2r} x_l^{\tau+2r}. \end{cases} \tag{16}$$

We recall that

$$\Lambda_l(x_1, x_2, \ldots, x_{\tau+r}) = 0$$

for $l > \tau + r$. Using this observation in conjunction with Proposition 3, we obtain, for $l > \tau + r$,

$$\begin{aligned} 0 &= \Lambda_l(x_1, \ldots, x_{\tau+r}) \\ &\equiv \mathcal{F}_l(s_1 + \sum_{j=\tau+r+1}^{\tau+2r} x_j, \ldots, s_l + \sum_{j=\tau+r+1}^{\tau+2r} x_j^l) \\ &= \sum_{j=0}^{r} \mathcal{F}_{l-j}(s_1, \ldots, s_{l-j}) \cdot \Lambda_j(x_{\tau+r+1}, \ldots, x_{\tau+2r}) \end{aligned}$$

Note that the above is true for $\ell = \tau + r + 1$, $\tau + r + 2$, ..., $\tau + 2r$, so that we obtain the linear array (17). We are now ready to discuss the specific decoding procedure. The first stage computes sequentially $\mathcal{F}_1(s_1)$, $\mathcal{F}_2(s_1, s_2)$, $\ldots$, $\mathcal{F}_k(s_1, s_2, \ldots, s_k)$, by utilizing (7) (or (9)). This stage requires $O(k^2)$ operations. The second stage tries the following procedure for $r = 0, 1, \ldots, \lfloor (k - |\tau|)/2 \rfloor$ one by one, until the valid solution is obtained (here k is the maximum number of tolerable faults and τ is given by s_0): (i) Solve for $\Lambda_l(x_{\tau+r+1}, \ldots, x_{\tau+2r})$, $l = 1, 2, \ldots, r$, in equation array (17); this can be solved with complexity of $O(r^2)$ operations because it is a Toeplitz problem [7]. (ii) Substitute the obtained $\Lambda_l(x_{\tau+r+1}, \ldots, x_{\tau+2r})$, $l = 1, 2, \ldots, r$, into Eq. (8) and, using Proposition 1, obtain the solution of $x_{\tau+r+1}, \ldots, x_{\tau+2r}$ by testing for transitions $1, 2, \ldots, m$, one by one (this is successful only if the solution exists); this takes $O(mr)$ steps. (iii) With known $x_{\tau+r+1}, \ldots, x_{\tau+2r}$, we immediately obtain $\mathcal{S}_i(x_1, x_2, \ldots, x_{\tau+r}) = s_i - \sum_{l=\tau+r+1}^{\tau+2r} x_l^i$; we then need $O((\tau + r)^2)$ steps to get $\Lambda_1(x_1, \ldots, x_{\tau+r}), \ldots, \Lambda_{\tau+r}(x_1, \ldots, x_{\tau+r})$, by following (7). Substituting these values into (8) and following Proposition 1, we get the solution of $x_1, \ldots, x_{\tau+r}$, again by testing $1, 2, \ldots, m$ one by one (again, this is successful only if the solution exists). In total, the second stage requires $O(m(\tau+r))$ steps. Thus, the overall decoding/identification complexity is $O(k^2 m)$.

Note that for $k = 1$, the first row of matrix $\mathbf{D}$ in (14) is obviously redundant; thus we only need

$$\mathbf{D} \stackrel{\triangle}{=} (1, 2, \ldots, m), \quad k = 1. \tag{18}$$

For $k = 2$, the first row is again redundant. This is justified by the fact that the following equation array

$$\begin{cases} x_1 \equiv x_2 + x_3, \\ x_1^2 \equiv x_2^2 + x_3^2, \end{cases}$$

does not have a nonzero (non-trivial) solution in $\mathrm{GF}(p)$[2]; thus, there is no confusion on the number of faults. Therefore, for $k = 2$, we can use the following matrix $\mathbf{D}$:

$$\mathbf{D} \stackrel{\triangle}{=} \begin{pmatrix} 1 & 2 & \ldots & m \\ 1 & 2^2 \bmod p & \ldots & m^2 \bmod p \end{pmatrix}, \quad k = 2. \tag{19}$$

In summary, the discussion in this section justifies the following theorem.

Theorem 1 *Let the monitoring matrix* $\mathbf{D}$ *be defined as in Eq.* (14) *for* $k \ge 3$ *(or Eq.* (19) *for* $k = 2$ *or Eq.* (18) *for* $k = 1$*). If* k *or less transition faults occur among* m *transitions, these faults can be detected and identified based on the syndrome* $\mathbf{s}[N] = \begin{bmatrix} s_0 & s_1 & s_2 & \ldots & s_k \end{bmatrix}^T$*. Furthermore, the faults can be identified with (worst-case) complexity* $O(k^2 m)$. □□

[2] We observe that $x_2^2 + x_3^2 \equiv (x_2 + x_3)^2$ yields $2x_2x_3 \equiv 0$ which implies that either $x_2 \equiv 0$ or $x_3 \equiv 0$.

$$\begin{cases} \sum_{j=1}^{r} \mathcal{F}_{\tau+r+1-j}(s_1,\ldots,s_{\tau+r+1-j}) \cdot \Lambda_j(x_{\tau+r+1},\ldots,x_{\tau+2r}) \equiv -\mathcal{F}_{\tau+r+1}(s_1,\ldots,s_{\tau+r+1}) \\ \sum_{j=1}^{r} \mathcal{F}_{\tau+r+2-j}(s_1,\ldots,s_{\tau+r+2-j}) \cdot \Lambda_j(x_{\tau+r+1},\ldots,x_{\tau+2r}) \equiv -\mathcal{F}_{\tau+r+2}(s_1,\ldots,s_{\tau+r+2}) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ \sum_{j=1}^{r} \mathcal{F}_{\tau+2r-j}(s_1,\ldots,s_{\tau+2r-j}) \cdot \Lambda_j(x_{\tau+r+1},\ldots,x_{\tau+2r}) \equiv -\mathcal{F}_{\tau+2r}(s_1,\ldots,s_{\tau+2r}) \end{cases} \tag{17}$$

IV Non-Concurrent Detection and Identification of Place Faults

Place faults within epoch interval $[1, N]$ are modeled as follows

$$\mathbf{q}_f[N] = \mathbf{q}_h[N] + \mathbf{e}_P, \tag{20}$$

where $\mathbf{e}_P \in \mathbb{Z}^\eta$ denotes the error vector. If $e_P^i < 0$ then the number of tokens in the ith place has decreased, whereas if $e_P^i > 0$ then the number of tokens in the ith place has increased (by $|e_P^i|$ tokens in either case). We assume that the number of tokens in the redundant Petri net does not get affected by place faults (i.e., $e_P^i = 0$ for $i = n+1, n+2, \ldots, n+d = \eta$). This is justified by the fact that the places in the Petri net embedding are internal to the monitor, which is assumed to be fault-free. We consider the error syndrome

$$\begin{aligned} \mathbf{s}[N] &= \mathbf{P}\mathbf{q}_f[N] \\ &= [-\mathbf{C} \;\; \mathbf{I}_d](\mathbf{q}_h[N] + \mathbf{e}_P) \\ &= -\mathbf{C}\mathbf{e}_P, \end{aligned} \tag{21}$$

where for notational simplicity the error vector in the last equation is still denoted by $\mathbf{e}_P$ (note that $\mathbf{e}_P \in \mathbb{Z}^n$). As in Section III, we are interested in designing matrix $\mathbf{C}$ such that (the negative of) the error syndrome $\mathbf{s} \triangleq \mathbf{C}\mathbf{e}_P$ is nonzero and unique for any $\mathbf{e}_P$ with at most k non-zero entries ($k \le n/2$). Notice that the entries of $\mathbf{e}_P$ can be any integer now (not necessary positive) and that detection and identification of place faults is independent of the choice of matrix $\mathbf{D}$ (recall that detection and identification of transition faults were essentially independent of matrix $\mathbf{C}$). Consider the following form for matrix $\mathbf{C}$:

$$\mathbf{C} \triangleq \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2^2 \bmod p & 3^2 \bmod p & \ldots & n^2 \bmod p \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{2k} \bmod p & 3^{2k} \bmod p & \ldots & n^{2k} \bmod p \end{pmatrix}, \tag{22}$$

where p is a prime number greater than n.

Lemma 1 *Let* $\mathbf{C}$ *be defined in* (22) *and assume* $k \le n/2$. *Then*
(*i*) *any* $2k$ *column vectors are linearly independent,*
(*ii*) *any linear combination of* k *or less column vectors is unique.*

Proof: (*i*) The determinant of a matrix consisting of any $2k$ column vectors, say the r_1-th, r_2-th, ..., r_{2k}-th columns of $\mathbf{C}$, is equal to $\prod_{i<j}(r_j - r_i)$ [6]. Thus, these $2k$ column vectors are independent since $\prod_{i<j}(r_j - r_i) \neq 0$.
(*ii*) Suppose the conclusion does not hold, that is, there exist two different linear combinations of k or less columns such that

$$\sum_{i=1}^{a} \alpha_i \mathbf{g}_{r_i} = \sum_{i=1}^{b} \alpha_i' \mathbf{g}_{r_i'}, \quad a, b \le k,$$

where α_i, α_i' are constants and $\mathbf{g}_{r_i}$ and $\mathbf{g}_{r_i'}$ denote the r_i-th and r_i'-th columns of $\mathbf{C}$. Then, we have

$$\sum_{i=1}^{a} \alpha_i \mathbf{g}_{r_i} - \sum_{i=1}^{b} \alpha_i' \mathbf{g}_{r_i'} = 0.$$

Since $a + b \le 2k$, this conflicts with the former conclusion that any $2k$ or less column vectors are independent; thus, we conclude the lemma. □□

We have shown that, with $\mathbf{C}$ defined as in (22), any k or less place faults lead to a syndrome that is nonzero and unique. We proceed to establish a specific identification procedure. We assume τ ($1 \le \tau \le k$) places are in fault and corrupted by amount α_i, $i = 1, 2, \ldots, \tau$, respectively (note that here each $|\alpha_i|$ can be an arbitrary integer, in particular, it may be larger than p). The syndrome $\mathbf{s} = \mathbf{C}\mathbf{e}_P$ can then be written as

$$\begin{cases} \sum_{i=1}^{\tau} \alpha_i x_i & = s_1, \\ \sum_{i=1}^{\tau} \alpha_i (x_i^2 \bmod p) & = s_2, \\ & \vdots \\ \sum_{i=1}^{\tau} \alpha_i (x_i^{2k} \bmod p) & = s_{2k}. \end{cases} \tag{23}$$

Since $\tau \le k$, the Berlekamp-Massey algorithm can be employed to solve equation array (23) to obtain $x_1, x_2, \ldots, x_\tau$, with computational complexity of $O(kn)$ [6]. The obtained values, if valid, are then substituted into (23) to solve for the coefficients α_i, $i = 1, 2, \ldots, \tau$ (the problem is now linear in the α_i's). This stage requires $O(\tau^3)$ operations.

Theorem 2 *The monitoring matrix* $\mathbf{C}_{2k \times n}$ *defined in* (22) *reaches the minimum row dimension required to be able to detect and identify* k *or less place faults out of* n *places (based on the syndrome* $\mathbf{s}[N] =$

$\left[\ s_0 \quad s_1 \quad s_2 \quad \ldots \quad s_k\ \right]^T$). *Furthermore, there exists an algorithm that detects and identifies faults with (worst-case) complexity* $O(kn + k^3)$. □□

V Detection and Identification of Simultaneous Transition and Place Faults

In this section we discuss the synthesis of a detection and identification scheme for simultaneous transition and place faults. We will show that by using a redundant Petri net embedding with $2k$ additional places ($k \leq n/2$), it is possible to detect and identify all combinations of faults such that the number of place faults is less than or equal to k and the number of transition faults is less than or equal to $2k-1$. Again, we assume that the number of tokens in the $2k$ additional places in the redundant part of the Petri net embedding is error-free and that each transition does not simultaneously suffer pre-condition and post-condition faults during the epoch interval $[1, N]$.

By combining Eqs. (13) and (21), we have the following error syndrome at time epoch N:

$$\begin{aligned}\mathbf{s}[N] &= \mathbf{P}\mathbf{q}_f[N] = [-\mathbf{C}\ \ \mathbf{I}_{2k}](\mathbf{q}_h[N] - \mathcal{B}^+\mathbf{e}_T^+ + \mathcal{B}^-\mathbf{e}_T^- + \mathbf{e}_P) \\ &= \mathbf{D}\mathbf{e}_T - \mathbf{C}\mathbf{e}_P, \end{aligned} \tag{24}$$

where, again for notational simplicity, the place error vector is still denoted by $\mathbf{e}_P$. Let p be a prime integer larger than both m and n. Define $\mathbf{D}^*$ and $\mathbf{C}^*$ by

$$\mathbf{D}^* = \mathbf{D}, \tag{25}$$

$$\mathbf{C}^* = p\mathbf{C}. \tag{26}$$

Note that

$$\mathbf{s} \stackrel{\triangle}{=} \mathbf{P}\mathbf{q}_f[N] \equiv \mathbf{D}^*\mathbf{e}_T \pmod{p}. \tag{27}$$

When $2k-1$ or less transition faults occur, they can be detected and identified by the method developed in Section III. After the transition faults have been identified, the place faults can be identified by

$$\mathbf{s}' \stackrel{\triangle}{=} (\mathbf{D}^*\mathbf{e}_T - \mathbf{s})/p = (\mathbf{C}^*/p)\mathbf{e}_P = \mathbf{C}\mathbf{e}_P, \tag{28}$$

where $\mathbf{C} \stackrel{\triangle}{=} \mathbf{C}^*/p$. Thus, the method proposed in Section IV can be applied to detect and identify any k or less place faults. If we make the reasonable assumption that the number of places n and the number of transitions m are of the same order, the entire algorithmic complexity is $O(k^2m) + O(kn + k^3) \leq O(k^2(m+n))$. The following theorem summarizes this discussion.

Theorem 3 *Let a Petri net* $\mathcal{S}$ *be such that each transition has at least one input place and at least one output place; let* $\mathcal{H}$ *be a separate redundant embedding for* $\mathcal{S}$*, with* $\mathbf{D}^*$ *and* $\mathbf{C}^*$ *defined as in Eqs.* (25) *and* (26) *respectively. Then, all possible faults such that the number place faults is less than or equal to* k *and the number of transition faults is less than or equal to* $2k-1$ *(or* 2 *for* $k = 1$*) are detectable and identifiable. Furthermore, the (worst-case) computational complexity is* $O(k^2(m+n))$. □□

Note that, no matter how many place faults occur, transition faults are always detectable and identifiable (as long as no more than $2k-1$ transition faults happen).

VI Conclusions

In this paper we presented a monitoring scheme that, based on a non-concurrent parity check at time epoch N, is able to simultaneously detect and identify up to $2k-1$ transition faults and up to k place faults that may have taken place in the epoch interval $[1, N]$. The scheme is based on a separate redundant Petri embedding of $2k$ additional places (and the connections and tokens associated with them). These additional places essentially perform the necessary book-keeping that allows the FDI mechanism to non-concurrently detect and identify faults in a straightforward manner. The worst-case operational complexity of the FDI mechanism is $O(k^2m)$ operations, where m is the number of transitions in the given Petri net model. In comparison with existing developments, the proposed diagnosis scheme avoids tracking the state evolution of the system and is, thus, well-suited for non-concurrent FDI of multiple and mixed faults.

References

[1] J. Gertler, *Fault Detection and Diagnosis in Engineering Systems*. New York: Marcel Dekker, 1998.

[2] E. Y. Chow and A. S. Willsky, "Analytical redundancy and the design of robust failure detection systems," *IEEE Trans. Automatic Control*, vol. 29, pp. 603–614, July 1984.

[3] C. N. Hadjicostis and G. C. Verghese, "Monitoring discrete event systems using Petri net embeddings," *Application and Theory of Petri Nets 1999 (Series Lecture Notes in Computer Science, vol. 1639)*, pp. 188-207, 1999.

[4] C. N. Hadjicostis and G. C. Verghese, "Power system monitoring using Petri net embeddings," *IEE Proc. C. Generation, Transmission and Distribution*, vol. 147, pp. 299–303, Sept. 2000.

[5] J. Riordan, *An Introduction to Combinatorial Analysis*, New York: Jorn Wiley & Sons, 1958.

[6] S. B. Wicker, *Error Control Systems*, Prentice Hall, Upper Saddle River, NJ, 1995.

[7] W. H. Press, S. A. Teukolsky, W. T. Vellerling and B. P. Flannery, *Numerical Recipes in C – The Art of Scientific Computing*, Second Edition, Cambridge University Press, UK, 1992.