On Diagnosis of Violations of Constraints in Petri Net Models of Discrete Event Systems Using Fourier-Motzkin Method [*]

Ahmed Khelfa Obeid Al-Ajeli and **Behzad Bordbar**
University of Birmingham, Birmingham, UK
e-mail: {A.K.O.Al-Ajeli, B.Bordbar}@cs.bham.ac.uk

Abstract

Failure diagnosis in partially observable model-based Discrete Event Systems requires modelling failures as unobservable events within the system. Representing failures as events is not always realistic. For example, some classes of failure are in form of violations of constraints such as Service Level Agreement (SLA) and Quality of Service (QoS). To model such failures, we need to modify the plant model which is not always acceptable. Firstly, this may make the models large. Secondly, adding extra transitions is not always preferable from engineers' prospective as every modification of the constraint will modify the model of the plant. This paper applies Integer Fourier-Motzkin Elimination (IFME) approach to address this issue. Since the constraints and their violations can be written as inequalities, we show that starting from a Petri net two sets of inequalities (diagnoser) are obtained. These sets are used to judge whether an observed sequence may satisfy (violate) these inequalities.

1 Introduction

Automata and Petri nets are two common modelling languages used in model-based diagnosis of failure in Discrete Event Systems (DESs) [Sampath *et al.*1995, Genc and Lafortune2007, Jiroveanu *et al.*2008, Basile *et al.*2008, Dotoli *et al.*2009, Cabasino *et al.*2010]. A common practice is to represent failures as a part of the plant's model. For example, in Automata and Petri nets models of the plants, we create unobservable transitions for representing failures. However, this style of the modelling of failures is not always realistic. Sometimes failure is created as a result of violation of Service Level Agreement (SLA) or Quality of Service (QoS). For example, consider the so-called Right-First Time (RFT) failure [Alodib and Bordbar2009] which is of interest to telecommunication services. Right-First Time (RFT) failure occurs when a process fails to complete a task First-Time and it is forced to repeat a part of the task again. This happens when one or more tasks are repeated, indicating incorrect execution of the task in the first place. Such occurrences of failure may result in violations of Service Level Agreement (SLA), causing financial penalties or customer dissatisfaction.

If the failure is expressed as a constraint, there is no event in the system that represents failure. One can argue that if a failure is caused by a violation of a constraint, we can always modify the model of the plant to include extra transitions (or/and states) to model the occurrences of the failure. This would require alterations of the models which is, in our experience, not always acceptable by the engineers. Since the SLA and QoS requirements change over time, if violations of such constraints are modelled by adding transitions, the model of the plant must change whenever such constraints are modified. In addition, in some cases, adding extra events or transitions may result in cumbersome models. To model RFT failure, potentially duplicates of many transitions must be created to mark undesirable repetition of the multiple events. This can result in a serious distortion of an originally elegant design, resulting in a large and complex model.

In [Al-Ajeli and Bordbar2016], we introduced a new approach to address the problem of failures diagnosis. Considering failures as events in the plant model, this approach uses Integer Fourier-Motzkin Elimination (IFME) method. Also, the occurrence of failures is formulated as an inequality. On the other hand, the normal state can be expressed as an inequality too. We showed that the question of creating the diagnoser to detect failures in Petri nets can be converted to the same question of projecting sets of inequalities on variables representing the observable transitions. The introduced approach proceeds as follows. We start with an *acyclic* Petri net $\mathcal{N}$. Then, two inequalities are individually added to E. These inequalities express two cases; failure occurs case and normal case. Applying IFME method to the resulting sets creates two new sets of inequalities by eliminating the variables corresponding to unobservable transitions. These sets are then used as a diagnoser.

The contributions of this paper consist in extending the previous work introduced in [Al-Ajeli and Bordbar2016] beyond *acyclic* Petri nets. Then, applying the extended approach using IFME method to diagnose violations of constraints. Motivated by the use of SLA and QoS, we shall model failure (violation of constraints) as an inequality. Namely, for a Petri net $\mathcal{N}$ and a constraint ϕ which, if violated, a failure has happened, we apply the same procedure described above in case of failures as events. In which case, the model of plant will not be modified neither to model these failures as events nor when constraints change.

This paper is organized as follows. Section 2 presents

[*] The first author acknowledges the partial support by University of Babylon, Iraq.

preliminaries including Petri nets' theory, diagnosis of failures in partially observable DES, Fourier-Motzkin Elimination method and using this method for failures diagnosis. Failures as violations of constraints in addition to a running example are introduced in section 3. Following that, using IFME method to diagnose occurrences of violations of constraints is shown. We end this paper by related works and conclusions.

2 Preliminaries

2.1 Petri nets

A *Petri net* [Murata1989] is defined as a four tuple $\mathcal{N} = (P, T, pre, post)$, where P and T are two nonempty finite sets of places and transitions, respectively. We denote $m = |P|$ and $n = |T|$ as the number of places and transitions. $pre : P \times T \to \mathbb{N}$ and $post : P \times T \to \mathbb{N}$. For a given transition t, an *input* (*output*) place of t is a place p such that $pre(p,t)$ $(post(p,t))$ is positive, respectively. $A = [a_{ij}]$ is an $m \times n$ matrix of integers called *incidence matrix*, where $a_{ij} = post(p,t) - pre(p,t)$ assuming that the set of places are ordered to correspond the coordinates of the matrix. In this paper $\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of non-negative integers, $\mathbb{Z}$ is the set of all integers and $\mathbb{R}$ is the set of real numbers. We write ${}^\bullet t$ $(t^\bullet)$ for the set of all input (output) places of a transition t, respectively. Also, we write ${}^\bullet p$ $(p^\bullet)$ for the set of all input (output) transitions of a place p, respectively. A pair of a place p and transition t is called a *self-loop* if p is both an input and output place of t.

A *state* of a Petri net, known as a *marking*, is represented as $M : P \to \mathbb{N}$ capturing the number of tokens in each place. We sometimes represent a marking as an $m \times 1$ matrix of non-negative integers. A transition t is *enabled* at a marking M if for each $M \geq pre(.,t)$, where $pre(.,t)$ is an $n \times 1$ matrix with coordinates $pre(p,t)$ for $p \in P$. An enabled transition can *fire* resulting in a new marking M', denoted by $M \xrightarrow{t} M'$, where $M' = M + A(.,t)$. A sequence of transitions $\sigma = t_1 \dots t_k$ of T is called *enabled* at a marking M, if there are marking $M_1, \dots, M_k$ so that $M \xrightarrow{t_1} M_1 \xrightarrow{t_2} M_2 \cdots \xrightarrow{t_k} M_k$. In this case, we write $M \xrightarrow{\sigma} M_k$ and refer to M_k as a state *Reachable* from M and σ is the firing sequence. We write $R(\mathcal{N},\ M)$ for the set of all reachable states from M. The initial state of the system is represented by an *initial marking* M_0. We will write $(\mathcal{N},\ M_0)$ for a Petri net with its initial marking M_0.

The set of all finite-length strings of the transitions in T is denoted by T^* and is called the *Kleene-closure* of T. As a result, members of T^* are created from concatenation of finite number of elements of T. In particular, T^* contains the empty string ε, so that $t\varepsilon = \varepsilon t = t$ for all $t \in T$. Every subset of T^* is called a *language on the alphabet* T. Suppose that we have a sequence σ of $(\mathcal{N},\ M_0)$, then the *Parikh vector* $\# : T^* \to \mathbb{N}^n$ is a map which assigns to every sequence σ a map $\#(\sigma)$ that produces the number of firing each transition in σ. In other words, for $\#(\sigma) : T \to \mathbb{N}$, $\#(\sigma)(t)$ is the number of occurrence of $t \in T$ within the sequence σ. Sometimes, we write $\#(t, \sigma)$ to represent the number of the occurrences of t in σ.

The set of sequences of transitions resulting in a reachable marking is called the *Language* of the Petri net and is denoted by $L(\mathcal{N},\ M_0)$ i.e. $L(\mathcal{N},\ M_0) = \{\sigma \in T^* \mid \exists M\ M_0 \xrightarrow{\sigma} M\}$.

Suppose that a destination marking M is reachable from M_0 in a Petri net $\mathcal{N}$ through a sequence σ, we can then find M using the following *state equation*:

$$M = M_0 + A\mathbf{x} \geq \vec{\mathbf{0}}, \tag{1}$$

where A is the incidence matrix of $\mathcal{N}$, and $\mathbf{x} \in \mathbb{N}^n$ is a n-dimensional column vector with $\mathbf{x} = (x_1, \dots, x_n)$ and $x_i = \#(t_i, \sigma)$ for $t_i \in T$. Then, for any firing sequence σ of $\mathcal{N}$, there exists $\mathbf{x} = \#(\sigma)$ satisfying (1). The converse is not always true. In some cases, as shown in Lemma 1 below, the converse holds too.

In what follows, we describe this lemma and the necessary definitions to establish it as presented in [Tsuji and Murata1993].

Definition 1. *[Tsuji and Murata1993] Let $\alpha = (\alpha_1, \dots, \alpha_n)$ be a solution of the state equation for a Petri net $(\mathcal{N}, M_0)$ with a destination marking M. Then, the subnet $\mathcal{N}_\alpha$ is called the firing count subnet with respect to α where each transition t_i in $\mathcal{N}_\alpha$ is such that $\alpha_i > 0$ together with its input and output places and its connecting arcs. $M_{0\alpha}$ denotes the subvector of M_0 for places in $\mathcal{N}_\alpha$.*

A *directed circuit* in a Petri net is a closed directed path from one node (place or transition) back to itself. A Petri net having no directed circuits is called an *acyclic* Petri net.

Definition 2. *[Tsuji and Murata1993] With respect to a directed circuit $\boldsymbol{d}$ in a Petri net, let P_d denotes the set of places on $\boldsymbol{d}$ and T_d denotes the set of transitions on $\boldsymbol{d}$. Then $T_d^{out} = P_d^\bullet \setminus T_d$ is called the set of outlet transitions and $T_d^{in} = {}^\bullet P_d \setminus T_d$ the set of inlet transitions. Where ${}^\bullet P_d = \bigcup_{p \in P_d} ({}^\bullet p)$ and $P_d^\bullet = \bigcup_{p \in P_d} (p^\bullet)$.*

Definition 3. *[Tsuji and Murata1993] With respect to a directed circuit $\boldsymbol{d}$ in a Petri net, the handles are defined as follows:*

- *A PT-handle is a directed path $\boldsymbol{h}$ from a place to a transition such that both belong to $\boldsymbol{d}$.*
- *A TP-handle is a directed path $\boldsymbol{h}$ from a transition to a place such that both belong to $\boldsymbol{d}$.*

where $\boldsymbol{h}$ and $\boldsymbol{d}$ share exactly two common nodes, the initial and terminal nodes of $\boldsymbol{h}$.

Definition 4. *[Tsuji and Murata1993] A PT-handle (TP-handle) $\boldsymbol{h}$ with respect to directed circuit $\boldsymbol{d}$ is said to be token-free if there are no tokens in those places in $\boldsymbol{h} - (\boldsymbol{h} \cap \boldsymbol{d})$.*

Lemma 1. *[Tsuji and Murata1993] In a Petri net $(\mathcal{N}, M_0)$, a marking M is reachable from M_0 if there exists a nonnegative integer solution α of its state equation satisfying the following two conditions:*

- *For each directed circuit $\boldsymbol{d}$ having k token-free PT-handles, $k = 0, 1, 2, \dots$, in the subnet $(\mathcal{N}_\alpha, M_{0\alpha})$, there is at least one inlet transition, or at least $k+1$ tokens.*
- *For each directed circuit $\boldsymbol{d}$ having k' token-free TP-handles, $k' = 0, 1, 2, \dots$, in the subnet $(\mathcal{N}_\alpha, M_\alpha)$, there is at least one inlet transition, or at least $k'+1$ tokens.*

Proof. See [Tsuji and Murata1993] for the proof. □

The class of *acyclic* Petri nets is a special case and satisfies the conditions in Lemma 1.

2.2 Diagnosis of Failure Events in Partially Observable DES

Consider a Petri net $(\mathcal{N}, M_0)$ with a set of transitions T. Suppose that T is partitioned into two sets: observable transitions T_o and unobservable transitions T_u. We further assume that failures are unobservable transitions, i.e. $T_f \subseteq T_u$, in which T_f is the set of transitions which are modelling occurrences of failure. Consider the *projection* function $\pi : T \rightarrow T_o \cup \{\varepsilon\}$ that maps unobservable transitions to the empty string ε, i.e. $\pi(t) = \varepsilon$ for $t \in T_u$ while, $\pi(t) = t$ for $t \in T_o$. The projection function π can be extended to the Kleene-closure of T by $\pi : T^* \rightarrow (T_o \cup \{\varepsilon\})^*$ where for each sequence of transitions σ and each transition t, $\pi(\sigma t) = \pi(\sigma)\pi(t)$. We assume $\pi(\varepsilon) = \varepsilon$ and that $\pi(t\varepsilon) = \pi(\varepsilon t) = \varepsilon$ for each $t \in T_u$. Denote by $\mathbf{s} = \pi(\sigma)$ the observed sequence corresponding to a given sequence $\sigma \in T^*$.

Assuming that t_f is a failure transition, then the failure occurrence can be written as $\neg\mathbf{c} := x_f > 0$. Also, no occurrence of failure can be expressed as $\mathbf{c} := x_f \leq 0$. The set T_o represents all the events that are observable in the systems, such as events which can be recognised via a sensor. Hence, in every execution of events σ, a sequence of events $\mathbf{s} = \pi(\sigma)$ from T_o can be observed. A diagnoser uses such information to identify a diagnosis state to be one of the following [Al-Ajeli and Bordbar2016]: 1) *Normal* state - when all sequences in $L(\mathcal{N}, M_0)$ having the same $\mathbf{s}$ satisfy $\mathbf{c}$, 2) *Faulty* state is obtained when all sequences in $L(\mathcal{N}, M_0)$ with the same $\mathbf{s}$ satisfy $\neg\mathbf{c}$ and 3) *Uncertain* state in which there are two sequences having the same $\mathbf{s}$ but one of them satisfies $\mathbf{c}$ and the other satisfies $\neg\mathbf{c}$.

This definition of the diagnoser states extends their definition in [Cabasino *et al.*2009] which is itself an extension of the definition in [Sampath *et al.*1995].

2.3 Fourier-Motzkin Elimination Method

Fourier-Motzkin elimination (FME) method has originally been suggested for solving a set of linear inequalities and also to establish if the set is solvable [Kuhn1956, Kohler1967, Dantzig1972, Duffin1974]. In other words, given a matrix $A \in \mathbb{R}^{m\times n}$ and vector $b \in \mathbb{R}^m$, FME tests if a set of inequalities $E := A\mathbf{x} \leq \mathbf{b}$, where the vector of variables $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, has a solution. Then if there exist a solution, FME will find it. For the sake of simplicity, all entries in the last column of A are, without loss the generality, assumed to be 0, +1 or -1. Then, the set E can be rewritten as shown in (2). Thus the problem now is to solve this set (the inequalities might need to be reordered first).

$$\begin{aligned} &\mathbf{a_i'}\mathbf{x}' \qquad \leq b_i,\ i = 1,\ldots,m_1 \\ &\mathbf{a_j'}\mathbf{x}' - x_n \leq b_j,\ j = m_1+1,\ldots,m_2 \\ &\mathbf{a_k'}\mathbf{x}' + x_n \leq b_k,\ k = m_2+1,\ldots,m \end{aligned} \tag{2}$$

where $\mathbf{x}' = \{x_1, x_2, \ldots x_{n-1}\}$, i.e., the same set of variables without x_n. Assume that $l = max(\mathbf{a_j'}\mathbf{x}' - b_j, j = m_1 + 1,\ldots,m_2)$ and $u = min(b_k - \mathbf{a_k'}\mathbf{x}', k = m_2+1,\ldots,m)$. Since the last two lines of (2) are equivalent to $l \leq x_n \leq u$, then the variable x_n can be eliminated. This yields the *reduced* set R in (3) as an equivalent to the set E in (2):

$$\begin{aligned} &\mathbf{a_i'}\mathbf{x}' \leq b_i,\ i = 1,\ldots,m_1 \\ &\mathbf{a_j'}\mathbf{x}' - b_j \leq b_k - \mathbf{a_k'}\mathbf{x}',\ j = m_1+1,\ldots,m_2, \\ &k = m_2+1,\ldots,m \end{aligned} \tag{3}$$

By repeating this process, we can successively eliminate the last $n-1$ variables $x_n, x_{n-1}, \ldots, x_2$, and end up with a set of inequalities in one variable x_1 which is trivial. Note that using this method in failure diagnosis, the process of elimination stops when all variables corresponding to unobservable transitions are eliminated as explained later.

Theorem 1. *[Duffin1974] Assume that the variables $x_{k+1}, \ldots, x_n$ have been eliminated in order by using FME method described above from a set of linear inequalities E. This results in the reduced set R. Then $\alpha_1, \ldots, \alpha_k$ is a solution of R iff there exists values $\alpha_{k+1}, \ldots, \alpha_n$ such that $\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n$ is a solution of E.*

Finally, the extension of the FME method described in this section to cope with integer valued variables has been reported in [Williams1976] and [Pugh1991]. For sake of brevity, this extension is not included here.

2.4 Using IFME Approach to Diagnose Failures

In [Al-Ajeli and Bordbar2016], we introduced the notion of using IFME method for failures diagnosis in partially observable DES modelled by Petri nets. Under the assumption that the Petri nets are *acyclic* and have single failure, we showed that the diagnoser can be expressed as two sets of inequalities. These sets are derived from the *state equations* of Petri nets, $\mathbf{c}$ and $\neg\mathbf{c}$.

Based on the definition of the *valuation* described in [Clarke *et al.*1999], we have presented the following definitions [Al-Ajeli and Bordbar2016].

Definition 5. *Let $\mathbf{x} = (x_1, \ldots, x_n)$ be a set of variables. We suppose that the variables range over $\mathbb{N}$. A valuation ν for $\mathbf{x}$ is a function that associates a value in $\mathbb{N}$ to each variable x_i in $\mathbf{x}$.*

Remark: In the light of Definition 5, given a sequence $\sigma \in T^*$, Parikh vector $\#(\sigma)$ represents a valuation of $\mathbf{x}$. In other words, for each x_i of $\mathbf{x}$, $x_i = \#(t_i, \sigma)$, where $i = 1, 2, \ldots, n$.

Definition 6. *Suppose that $\mathbf{e}$ is an inequality of the form $a_1x_1 + \cdots + a_nx_n \leq b$ in the variables set $\mathbf{x} = (x_1, \ldots, x_n), x_i \in \mathbb{N}$ and $a_1, \ldots, a_n, b \in \mathbb{Z}$. Consider a valuation ν as $\alpha_1, \ldots, \alpha_n$ assigned to value $x_1, \ldots, x_n$ respectively. Then we write $\nu \vDash \mathbf{e}$ to say that the valuation ν satisfies the inequality $\mathbf{e}$ if and only if $a_1\alpha_1 + \cdots + a_n\alpha_n \leq b$.*

Definition 7. *Suppose that we have a set of inequalities $E = \{e_i \mid 1 \leq i \leq d\}$ where e_i has the form of $\mathbf{e}$ in Definition 6. Consider a valuation ν for the variables of the inequalities in E. Then $\nu \vDash E$ iff $(\nu \vDash e_1) \wedge (\nu \vDash e_2) \wedge \cdots \wedge (\nu \vDash e_d)$ ("$\wedge$" is the conjunctive operator).*

Now, the IFME approach for failures diagnosis can be outlined as follows. Suppose that $(\mathcal{N}, M_0)$ is an *acyclic* Petri net with the initial marking M_0. Without any loss of generality, suppose that we have renamed the transitions of $\mathcal{N}$ such that the first k transitions are observable, i.e., $T_o = \{t_1, t_2, \ldots, t_k\}$. The remaining transitions are unobservable, i.e. $T_u = \{t_{k+1}, t_{k+2}, \ldots, t_n\}$.

We further assume that the system has a single failure and t_n is the only failure transition of the system. We introduce variables $x_1, x_2, \ldots, x_n$ representing the number of firing of $t_1, t_2, \ldots, t_n$, respectively. Suppose that $E := M_0 + A\mathbf{x} \geq \vec{\mathbf{0}}$ represents the state equations, where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. We further assume that $\mathbf{c}$ is the inequality $x_n \leq 0$ and $\neg\mathbf{c}$ is the negation of $\mathbf{c}$, i.e., the inequality $x_n > 0$. For each firing sequence σ of $(\mathcal{N}, M_0)$, if σ contains t_n, i.e., the failure transition, then $\#(\sigma)$, the Parikh vector of σ, satisfies $\neg\mathbf{c}$. Conversely, for a firing sequence σ, if $\#(\sigma)$ satisfies $\mathbf{c}$, then σ has no the failure transition t_n.

From an *acyclic* Petri net model, we first obtain a set of inequalities $E := M_0 + A\mathbf{x} \geq \vec{\mathbf{0}}$. Then, we create two sets of inequalities $E \cup \{\mathbf{c}\}$ and $E \cup \{\neg\mathbf{c}\}$. Applying IFME method simultaneously to both $E \cup \{\mathbf{c}\}$ and $E \cup \{\neg\mathbf{c}\}$, two reduced sets, R and R', are created by eliminating every variable corresponding to a transition in the set T_u. We use the reduced sets of inequalities to diagnose failure occurrence of t_n as follows.

Theorem 2. *Suppose that $\mathscr{N}$ is an acyclic Petri net with an initial marking M_0. Suppose that E is the set of inequalities $-A\mathbf{x} \leq M_0$ created from the state equation of $\mathscr{N}$. Assume that $T = T_o \cup T_u$, $T_o = \{t_1, \ldots, t_k\}$, $T_u = \{t_{k+1}, \ldots, t_n\}$ and t_n is a failure transition. The vector of variables $x_1, \ldots, x_n$ corresponds to the number of firing the transitions $t_1, \ldots, t_n$. Assume also that $\mathbf{c}$ is the inequality $x_n \leq 0$ and $\neg\mathbf{c}$ is its negation. Suppose that the set of inequalities R and R' are respectively produced from applying of IFME to both $E \cup \{\mathbf{c}\}$ and $E \cup \{\neg\mathbf{c}\}$ to eliminate all variables corresponding to transitions in T_u. Then, for any given sequence of observable events $\mathbf{s} = \pi(\sigma)$, where σ is a firing sequence in $\mathscr{N}$ ($M_0 \overset{\sigma}{\to} M$), if*

1. *$\#(\mathbf{s}) \nvDash R$, then the diagnosis state is Faulty.*
2. *$\#(\mathbf{s}) \nvDash R'$, then the diagnosis state is Normal.*
3. *$\#(\mathbf{s}) \vDash R$ and $\#(\mathbf{s}) \vDash R'$, then the diagnosis state is Uncertain.*
4. *$\#(\mathbf{s}) \nvDash R$ and $\#(\mathbf{s}) \nvDash R'$, it is not possible to have this case.*

Proof. We address [Al-Ajeli and Bordbar2016] for the proof. □

3 Failures in Form of Violations of Constraints

Some failures are not modelling as events in the plant of the system but they represent a form of violations of constraints. Service Level Agreement (SLA) and Quality of Service (QoS) violations are examples of such failures. Many SLA and QoS statements have been defined to restrict SLA and QoS such as error rate, percentage of service availability and the ratio of message loss in communication channel. These statements are termed constraints within these agreements whose violations represent failures. In effect, violation here implies that tasks executed are going below the acceptable level according to the agreement.
Example 1 [Alodib and Bordbar2009]: To describe the problem that has motivated this paper, we shall make use of a simplified business process used within a typical telecommunication company. Suppose the scenario that a domestic customer telephones to report a malfunction such as the broadband connection being slow. We refer to such problems and malfunctions as "tasks" or "jobs". The following example describes a simplified business process from the arrival of the job to its completion.

In Petri net of Fig.1, when the tasks arrive (firing of t_1), depending on the nature of the problem which is reported, every task is allocated to one of the three Departments. Within each Department, there are a few large and complex workflows which we have (seriously) simplified to two cases. Either the problem is resolved (transitions labelled R) or the engineers discover that the allocated job can NOT be resolved (transitions labelled N) within their Department. This would be a case of wrong allocation of jobs and can arise from a multitude of reasons, among them wrong information from the customers or wrong assignment of jobs or the case that one fault triggers another. In the case that the job is resolved, the Department declares that "Job Completed" by firing of t_{12}, t_{13} or t_{14}, which ultimately results in the firing of t_{15} marking the "Completion of the (overall) task." In case that a Department is not able to complete the job (firing of t_6, t_8 or t_{10}), further investigation is required. As a result, a token is placed in p_1 so that the job is reallocated by the Customer Service department. We assume that transitions t_1 and t_{15}, which mark arrival and completion of jobs are observable. In addition, transitions that mark arrival of the jobs in each Department (t_3, t_4 and t_5) are also observable, as they are used by the Department to inform the Customer of the progress of the job. For example if the customer is accessing through a browser to make an online report, he is informed that the relevant department will deal with the problem. Observable transitions in Fig.1 are depicted by solid rectangles, while empty rectangles represent unobservable transitions.

In the above example, firing of t_6, t_8 or t_{10} results in a repetition of a chain of activities that indicates a wrong allocation of jobs to the departments. Since the activities are repeated, the job is not completed Right First Time (RFT). In this case, we say RFT failure has happened. Right First Time failures are becoming increasingly important in Telecom industry [Alodib and Bordbar2009]. Occurrence of a RFT failure may result in unhappy customers, increases cost of resolving the problems and may entail financial penalties. As a result development of methods of discovery of RFT

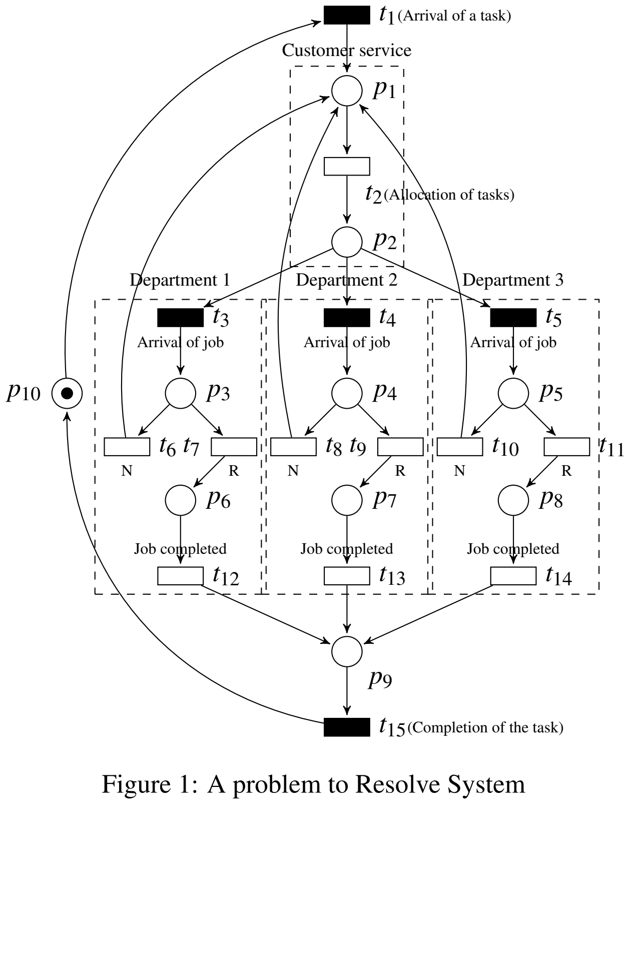

Figure 1: A problem to Resolve System

failures so that remedial actions can be adopted is essential. In addition, in large organisations such methods must be automated to allow dealing with large systems.

In the above example, the transition t_2 marks allocation of jobs and the transition t_{15} marks the completion of a job. Ideally, to ensure no RFT failure, we wish that every allocated job is completed. In other words, for each execution sequence σ of the Petri net.

$$\#(t_2,\sigma) = \#(t_{15},\sigma). \tag{4}$$

If (4) happens, we have no RFT failure. However, it is often not possible to completely eliminate the RFT failure. As a result, the management sets Service Level Agreement (SLA) such as the number of failures should be below a value $\delta \geq 0$ to specify acceptable levels of failure. SLA is satisfied iff for each execution sequence (5) is true.

$$\#(t_2,\sigma) - \#(t_{15},\sigma) \leq \delta. \tag{5}$$

Petri net of Fig.1 represents a model of a plant and (5) represents a constraint (a SLA), which if violated, a failure has happened. *Petri net of Fig.1 has no failure transitions.* As a result, existing failure diagnosis techniques can not be directly applied. One can argue that, one must model failure by modifying the Petri net of Fig.1. This would mean adding extra transitions and places to *simulate* violation of (5). In our experience, this is not an easy task. In addition, modifying Fig.1 may result in cumbersome and large Petri nets which will be hard to understand. Thirdly, advocates of modelling failure must modify his design as soon as the SLA changes. As a result, there is a clear scope for extending existing fault diagnosis techniques in Petri nets for the case that the failure is associated to a violation of constraints such as SLA.

Violation of (5) can be represented as an inequality: Each sequence σ in $\mathcal{N}$ that violates (5) satisfies (6). Hence if (5) is evaluated to false, then (6) will be evaluated to true.

$$\#(t_2,\sigma) - \#(t_{15},\sigma) > \delta. \tag{6}$$

Conversely, if σ satisfies (5), then (6) is evaluated to true. Also, (6) can be rewritten as:

$$\#(t_{15},\sigma) - \#(t_2,\sigma) \leq -(\delta + 1). \tag{7}$$

As (7) is an inequality, violations of constraints can be expressed as inequalities. These inequalities can capture the general form **e** in definition 6. For example, assuming $x_2 = \#(t_2,\sigma), x_{15} = \#(t_{15},\sigma)$, $b = -(\delta+1)$ and the remaining coefficients equal to zero, then (7) corresponds to **e**. Likewise, (5) corresponds to **e**.

A wide range of SLA and QoS statements can be expressed as inequalities. For example, consider the ratio of message loss in communication channel. In this example, let us assume that t_1 represents sending of a message to a channel and t_2 represents arrival of the message at the other end. It is required that the ratio of the loss be $\frac{\#(t_1,\sigma)}{\#(t_2,\sigma)} \leq \frac{p}{q}$ which means $q \times \#(t_1,\sigma) - p \times \#(t_2,\sigma) \leq 0$. This inequality represents the constraint whose violation, written as $q \times \#(t_1,\sigma) - p \times \#(t_2,\sigma) > 0$, is seen as a failure, where $\frac{p}{q} > 1$ and $q \neq 0$. Since these SLA and QoS statements and its violations (seen as failures) can be written as inequalities, IFME approach is suitable to detect such failures.

4 IFME Approach to Diagnose Violations of Constraints

The purpose of this paper has two folds. First, we extend our previous work in [Al-Ajeli and Bordbar2016] beyond acyclic Petri nets supposing that the Petri net $(\mathcal{N}, M_0)$ is such that **the converse of its state equation is true** and with no self-loop. In other words, IFME approach can be applied to the Petri nets such that for any solution $\mathbf{x}$ of the state equation $M_0 + A\mathbf{x} = M$, there is a run $M_0 \overset{\sigma}{\to} M$ and $\mathbf{x} = \#(\sigma)$. For example, any Petri net satisfying the conditions of Lemma 1 will be an example of such nets. Acyclic Petri nets and also the Petri net of Fig. 1 represents examples of these Petri nets. Second, we apply the results obtained to diagnose failures which are NOT captured as events in the model of the system.

Consider a Petri net $\mathcal{N} = (P,T,pre,post)$ with an initial marking M_0. Also, consider that this Petri net has no self-loop and that every solution of its state equations has a sequence in $L(\mathcal{N}, M_0)$. The set of transitions of $\mathcal{N}$ is such that $T = \{t_1, t_2, \ldots, t_n\}$. Suppose that T is partitioned into two sets: observable transitions T_o and unobservable transitions T_u. Notice there is no notion of failure transition. However, we assume that there exists a constraint, denoted ϕ, which if violated, a failure has happened. Thus, a sequence of events σ for which $\#(\sigma) \nvDash \phi$ contains a failure. Conversely, a given sequence σ contains no failure if $\#(\sigma) \vDash \phi$.

In this paper, we assume that the system has single constraint ϕ whose violation, denoted ϕ', is seen as a failure. Further, assume that $\phi := \sum_{i=1}^{n} a_i x_i \leq b$ and $\neg\phi := \sum_{i=1}^{n} a_i x_i > b$, where $x_1, \ldots, x_n$ corresponds to the number of firing the transitions $t_1, \ldots, t_n$ and $a_1, \ldots, a_n, b \in \mathbb{Z}$. In effect, the inequalities **c** and $\neg$**c**, with one variable, are special cases of inequalities ϕ and $\neg\phi$, respectively. Thus the problem of failures diagnosis in partially observable systems in which failures are events can be considered as a special case of the problem of violations of constraints diagnosis. Accordingly, the diagnoser and diagnosis states previously defined (see section 2.2) can be redefined as follows:

Definition 8. *A diagnoser is a mapping that associates to each observed sequence* **s**, *with respect to ϕ and $\neg\phi$, one of the following diagnosis states:*

- *Normal: if $\forall\sigma \in L(\mathcal{N}, M_0)$ and $\pi(\sigma) = \mathbf{s}$, $\#(\sigma) \vDash \phi$. This state shows that there is no sequence having the same observation* **s** *violates ϕ.*
- *Faulty: if $\forall\sigma \in L(\mathcal{N}, M_0)$ and $\pi(\sigma) = \mathbf{s}$, $\#(\sigma) \vDash \neg\phi$. This state implies that all sequences having the same observation* **s** *violate ϕ.*
- *Uncertain: if there exists two sequences σ_1, $\sigma_2 \in L(\mathcal{N}, M_0)$, $\pi(\sigma_1) = \pi(\sigma_2) = \mathbf{s}$, $\#(\sigma_1) \vDash \phi$ and $\#(\sigma_2) \vDash \neg\phi$. In which case, the behaviour of the system is ambiguous because both Normal and Faulty states are possible during the observed sequence. For this reason, this state is called Uncertain state.*

The following theorem describes the extension of our previous work introduced in [Al-Ajeli and Bordbar2016] to the case where the failures are not captured as events but as violations of constraints.

Theorem 3. *Assume that $(\mathcal{N}, M_0)$ is a Petri net such that for any solution* **x** *of the state equation $M_0 + A\mathbf{x} = M$, there is a run $M_0 \overset{\sigma}{\to} M$ and $\mathbf{x} = \#(\sigma)$. Suppose that E is the* *set of inequalities $-A\mathbf{x} \leq M_0$ created from the state equation of $\mathcal{N}$. Assume that $T = T_o \cup T_u$, $T_o = \{t_1, \ldots, t_k\}$, $T_u = \{t_{k+1}, \ldots, t_n\}$ and failures are not captured as events. The vector of variables $x_1, \ldots, x_n$ corresponds to the number of firing the transitions $t_1, \ldots, t_n$. Assume also that ϕ is the constraint and ϕ' is its violation (see above). Suppose that the set of inequalities R and R' are respectively produced from applying of IFME to both $E \cup \{\phi\}$ and $E \cup \{\neg\phi\}$ to eliminate all variables corresponding to transitions in T_u. Then, for any given sequence of observable events $\mathbf{s} = \pi(\sigma)$, where σ is a firing sequence in $\mathcal{N}$, if*

1. *$\#(\mathbf{s}) \nvDash R$, then the diagnosis state is Faulty.*
2. *$\#(\mathbf{s}) \nvDash R'$, then the diagnosis state is Normal.*
3. *$\#(\mathbf{s}) \vDash R$ and $\#(\mathbf{s}) \vDash R'$, then the diagnosis state is Uncertain.*
4. *$\#(\mathbf{s}) \nvDash R$ and $\#(\mathbf{s}) \nvDash R'$, it is not possible to have this case.*

Proof. In what follows assume that $\#(\mathbf{s}) = (\alpha_1, \ldots, \alpha_k)$.

Proof of 1: Assume that $\#(\mathbf{s}) \nvDash R$, but the diagnosis state is not *Faulty*. If $\#(\mathbf{s}) \nvDash R$, then for every valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$, $\nu \nvDash E \wedge \phi$ by Theorem 1. As a result, $\forall \sigma' \in L(\mathcal{N}, M_0)$ such that $\pi(\sigma') = \mathbf{s}$, $\#(\sigma') \vDash \neg\phi$. Hence a violation of constraint has happened during observing $\mathbf{s}$. This contrasts the assumption.

Proof of 2: Using the same argument in **Proof of 1** replacing R with R', we can prove that if $\#(\mathbf{s}) \nvDash R'$, then the diagnosis state is *Normal*.

Proof of 3: Assume that $\#(\mathbf{s}) \vDash R$ and $\#(\mathbf{s}) \vDash R'$, but we are certain about the diagnosis state. If $\#(\mathbf{s}) \vDash R$, then there exists a valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ and $\nu \vDash E \wedge \phi$ by Theorem 1. If $\nu \vDash E \wedge \phi$, then $\nu \vDash E$. Considering that the state equation of $\mathcal{N}$ has a converse, then there exists σ' such that $M_0 \xrightarrow{\sigma'} M'$, $\#(\sigma') = \nu$. Hence, σ' has violated the constraint. Now, we claim that $\pi(\sigma') = \mathbf{s}$. The proof of this claim is accomplished by induction on the length of the observed sequence denoted $|\mathbf{s}|$.

(*Base case*): If $|\mathbf{s}| = 1$, then $\pi(\sigma') = \mathbf{s}$ because $\#(\pi(\sigma')) = \#(\mathbf{s})$. In fact, if $\pi(\sigma') \neq \mathbf{s}$, then there are two entries, representing the observable transitions, in $\#(\mathbf{s})$ and $\#(\pi(\sigma_1))$ having different values and this contrasts $\#(\pi(\sigma')) = \#(\mathbf{s})$.

(*Induction step*): We assume that the claim is true for all $\mathbf{s}$ with $|\mathbf{s}| \leq k_1$ (*Induction hypothesis*). Then, we prove it true for $\mathbf{s}$ with $|\mathbf{s}| = k_1 + 1$. Suppose $\mathbf{s} = \omega t$ where $t \in T_o$ and $\omega \in T_o^*$. Since $\sigma, \sigma' \in L(\mathcal{N}, M_0)$ and $\#(\pi(\sigma)) = \#(\pi(\sigma')) = \#(\mathbf{s})$, then there are sequences $\sigma_1' \in T^*$ and $\sigma_2' \in T_u^*$ such that $\sigma' = \sigma_1' t' \sigma_2'$. In effect, t' is the most recent observable transition in σ'. Then we have

$$M_0 \xrightarrow{\sigma_1'} M_1' \xrightarrow{t'} M_2' \xrightarrow{\sigma_2'} M', t' \in T_o$$

also σ_2' can be empty. For $\sigma = \sigma_1 t \sigma_2$ we have

$$M_0 \xrightarrow{\sigma_1} M_1 \xrightarrow{t} M_2 \xrightarrow{\sigma_2} M, \sigma_1 \in T^*, \sigma_2 \in T_u^*$$

Because $\pi(\sigma) = \mathbf{s} = \omega t$ and t is the last observable transition in σ, then $\pi(\sigma_1) = \omega$. By induction hypothesis, $\pi(\sigma_1') = \omega$. Since $\#(\pi(\sigma')) = \#(\mathbf{s}) = \#(\omega t)$, then $t = t'$ (if $t \neq t'$ then $\#(\pi(\sigma')) \neq \#(\mathbf{s})$ and this is not true). As a result, $\pi(\sigma') = \pi(\sigma_1')t' = \omega t = \mathbf{s}$ and this proves the claim.

Similarly, we can prove that if $\#(\mathbf{s}) \vDash R'$, there exists a sequence σ'' such that $M_0 \xrightarrow{\sigma''} M''$, $\#(\sigma'') \vDash \neg\phi$ (a violation of ϕ has occurred) and $\pi(\sigma'') = \mathbf{s}$.

To conclude, since $\sigma', \sigma'' \in L(\mathcal{N}, M_0)$ with $\pi(\sigma') = \pi(\sigma'') = \mathbf{s}$, $\#(\sigma') \vDash \phi$ and $\#(\sigma'') \vDash \neg\phi$, hence we have *Uncertain* state, see section 2.2. This contrasts the assumption.

Proof of 4: Assume that $\#(\mathbf{s}) \nvDash R$ and $\#(\mathbf{s}) \nvDash R'$, but this case is possible. If $\#(\mathbf{s}) \nvDash R$, then for every valuation $(\alpha_{k+1}, \ldots, \alpha_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$, $\nu \nvDash E \wedge \phi$ by Theorem 1. Also, if $\#(\mathbf{s}) \nvDash R'$, then for every valuation $(\beta_{k+1}, \ldots, \beta_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n)$, $\nu \nvDash E \wedge \neg\phi$ by Theorem 1. Rephrasing this statement, we can say that there exists at least one valuation $(\beta_{k+1}, \ldots, \beta_n)$ of $(x_{k+1}, \ldots, x_n)$ such that $\nu = (\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n)$ and $\nu \vDash E \wedge \phi$ taking into account that $\neg\phi$ is the violation of ϕ and σ is a firing sequence of $\mathcal{N}$, i.e. $\#(\sigma) \vDash E$. Here we have contradictory statements. Hence this case is an impossible case. This contrasts the assumption and completes the proof. □

Remark 1: Note that the proofs of 1 and 2 in theorem 3 are still valid for Petri nets which are not *acyclic*.

Theorem 3 provides a systematic procedure to detect violations of constraints. Note that the case where the observable sequence does not satisfy both R and R' is not possible.

Remark 2: The shape of each individual inequality that expresses the constraint and its violation is important. For example, a less interesting special case is when in the inequality all the non-zero coefficients are for observable transitions. For example, when in $\sum_{i=1}^{n} a_i x_i$ we have $a_i = 0$ if t_i is unobservable. In such a case, the sum can be calculated from the observable events. This is similar to the case that in classic failure diagnosis when some failure transitions are observable. Interesting cases occur when $a_i = 0$ for one or more observable transition.

Example 2: Consider the Petri net $\mathcal{N}$ of Fig.1 of our running example. A special case of RFT failure is described using (7) of section 3. Assuming that $\delta = 2$, the constraint ϕ is written as $\phi := x_2 - x_{15} \leq 2$ and its violation as $\neg\phi := x_{15} - x_2 \leq -3$ (Note that $\neg\phi$ has been rewritten in the standard form of E). Adding these inequalities simultaneously to the set of inequalities E derived from (1), we obtain two sets $E \cup \{\phi\}$ and $E \cup \{\neg\phi\}$. Then using IFME method to eliminate all variables corresponding to unobservable transitions produces the sets of inequalities in (8) and (9) respectively.

$$\begin{array}{rrrrrl}
-x_1 & & & & & \leq 0 \\
 & -x_3 & & & & \leq 0 \\
 & & -x_4 & & & \leq 0 \\
 & & & -x_5 & & \leq 0 \\
-x_1 & -x_3 & -x_4 & -x_5 & & \leq 0 \\
 & & & & -x_{15} & \leq 0 \\
x_1 & & & & -x_{15} & \leq 1 \\
-x_1 & & & & +x_{15} & \leq 0 \\
-x_1 & & -x_4 & & +x_{15} & \leq 0 \\
-x_1 & -x_3 & -x_4 & & +x_{15} & \leq 0 \\
-x_1 & -x_3 & & & +x_{15} & \leq 0 \\
-x_1 & & & -x_5 & +x_{15} & \leq 0 \\
 & +x_3 & +x_4 & +x_5 & -x_{15} & \leq 2 \\
 & -x_3 & -x_4 & -x_5 & +x_{15} & \leq 0 \\
-x_1 & & -x_4 & -x_5 & +x_{15} & \leq 0 \\
-x_1 & -x_3 & & -x_5 & +x_{15} & \leq 0 \\
-x_1 & -x_3 & -x_4 & -x_5 & +x_{15} & \leq 0
\end{array} \tag{8}$$

$$
\begin{array}{rrrrrcl}
-x_1 & & & & & \leq & 0\\
 & -x_3 & & & & \leq & 0\\
 & & -x_4 & & & \leq & 0\\
 & & & -x_5 & & \leq & 0\\
-x_1 & -x_3 & -x_4 & -x_5 & & \leq & 0\\
 & & & & -x_{15} & \leq & 0\\
x_1 & & & & -x_{15} & \leq & 1\\
-x_1 & & & & +x_{15} & \leq & 0\\
-x_1 & & -x_4 & & +x_{15} & \leq & 0\\
-x_1 & -x_3 & & & +x_{15} & \leq & 0\\
-x_1 & & & -x_5 & +x_{15} & \leq & 0\\
 & -x_3 & -x_4 & -x_5 & +x_{15} & \leq & 0\\
2x_1 & -x_3 & -x_4 & & +2x_{15} & \leq & 0\\
-x_1 & & -x_4 & -x_5 & +x_{15} & \leq & 0\\
-x_1 & -x_3 & & -x_5 & +x_{15} & \leq & 0\\
-x_1 & -x_3 & -x_4 & -x_5 & +x_{15} & \leq & 0\\
-x_1 & -x_3 & -x_4 & -x_5 & +2x_{15} & \leq & -3\\
-2x_1 & -2x_3 & -2x_4 & -2x_5 & +3x_{15} & \leq & -6
\end{array}
\qquad (9)
$$

The resulting sets of inequalities shown in (8) and (9) have only variables corresponding to observable transitions $\{t_1, t_3, t_4, t_5, t_{15}\}$. These two sets are used for estimating the current state of the system for a given observed sequence of events.

Table 1: Diagnosis state estimations.

No.	$\mathbf{s} = \pi(\sigma)$	$\#(\mathbf{s}) \vDash R$?	$\#(\mathbf{s}) \vDash R'$?	Diag. state
1	ε	Yes	No	*Normal*
2	t_1	Yes	No	*Normal*
3	t_1t_3	Yes	No	*Normal*
4	$t_1t_3t_3$	Yes	Yes	*Uncertain*
5	$t_1t_3t_3t_3$	No	Yes	*Faulty*
6	$t_1t_3t_3t_3t_{15}$	Yes	No	*Normal*
7	$t_1t_3t_3t_3t_3t_{15}$	No	Yes	*Faulty*
8	$t_1t_3t_{15}$	Yes	No	*Normal*
9	$t_1t_3t_{15}t_1$	Yes	No	*Normal*
10	$t_1t_3t_{15}t_1t_3$	Yes	No	*Normal*
11	$t_1t_3t_{15}t_1t_3t_{15}$	Yes	No	*Normal*

Table 1. shows different observed sequences and the diagnoses state estimated in each case. By looking at the Petri net in the figure, when the diagnoser observes no sequence ($\mathbf{s} = \varepsilon$), the diagnosis state is *Normal*, i.e. no violation of the constraint ϕ has happened. In which case, the diagnoser is certain that for all sequences having no observable transitions, ϕ is evaluated to true as $x_2 = 0$ and $x_{15} = 0$ for these sequences.

The same diagnosis state is estimated when observing the sequences 2, 3, 6, 8, 9, 10 and 11. For instance, in case of $\mathbf{s} = t_1$, only two sequences, namely $\sigma_1 = t_1$ and $\sigma_2 = t_1t_2$, have $\pi(\sigma_1) = \pi(\sigma_2) = \mathbf{s}$. But, both of them have the value of ϕ true because $x_2 = \#(t_2, \sigma_1) = 0, x_{15} = \#(t_{15}, \sigma_1) = 0$ and $x_2 = \#(t_2, \sigma_2) = 1, x_{15} = \#(t_{15}, \sigma_2) = 0$. In other words, both $\#(\sigma_1), \#(\sigma_2) \vDash \phi$. Thus, the diagnosis state is *Normal*.

On the other hand, suppose that the sequence 5 is observed. In that case, there exists three sequences $\sigma_1 = t_1t_2t_3t_6t_2t_3t_6t_2t_3t_6t_2$, $\sigma_2 = t_1t_2t_3t_6t_2t_3t_6t_2t_3t_7$ and $\sigma_3 = t_1t_2t_3t_6t_2t_3t_6t_2t_3t_7t_{12}$ with $\pi(\sigma_1) = \pi(\sigma_2) = \pi(\sigma_3) = t_1t_3t_3t_3$. By looking at $x_2 = \#(t_2, \sigma_i)$ and $x_{15} = \#(t_{15}, \sigma_i)$, we find that $\#(\sigma_i) \vDash \neg\phi$ for $i = 1, 2, 3$. As a result, a violation of ϕ has certainty happened.

Now let us explore the case where the sequence 4 is observed. Again, we have three sequences $\sigma_1 = t_1t_2t_3t_6t_2t_3t_6t_2$, $\sigma_2 = t_1t_2t_3t_6t_2t_3t_7$ and $\sigma_3 = t_1t_2t_3t_6t_2t_3t_7t_{12}$ with $\pi(\sigma_1) = \pi(\sigma_2) = \pi(\sigma_3) = t_1t_3t_3$. Obviously, $\#(\sigma_1) \vDash \phi'$, but $\#(\sigma_2), \#(\sigma_3) \vDash \phi$. This is *Uncertain* state because the diagnoser cannot decide whether a violation of ϕ happened or not.

Note that the same results shown in Table 1. can be obtained by replacing the transition t_3 by t_4 or t_5. For instance, the observed sequences t_1t_4 and t_1t_5 do not violate ϕ as t_1t_3 does not.

5 Related Works

The notion of diagnosis of violations of constraints (diagnosis of failures which are not captured as events) might resemble the notion of diagnosis of supervision patterns presented in [Jéron *et al.*2006]. These patterns define the language to which the sequences of events including failures belong. Five supervision patterns have been defined to model different forms of failures. For each pattern an Automaton is identified which accepts the language representing by the pattern. Taking a product composition between this Automaton and the Automaton modelling the system, the resulting structure can be used for diagnosis of the sequences having that pattern.

To compare, the work presented in this paper is based on Petri nets model and not Automata-based. Also, the violations of constraints to be diagnosed is modelled by inequalities. These inequalities express relations between the number of occurrences of given transitions in the model. In this sense, the order relation between these transitions is not taken into account. However, using the inequalities, a broad range of patterns can be efficiently modelled. In addition, our approach outperforms the supervision pattern method mentioned above for detecting the same pattern because we do not perform a product composition.

Finally, we wish to point out that there is a strong relationship between using Integer Linear Programming (ILP) and IFME method. Nevertheless, in our work failure diagnosis problem is NOT reduced to ILP problem. In effect, we use IFME method to project sets of inequalities on variables corresponding to observable transitions in Petri nets models. That is, our approach does not use IFME method to solve ILP problem.

6 Conclusions

A different form of failures in partially observable Discrete-Event Systems modelled using Petri nets has been presented in this paper. In this form, failures are no longer modelled as events but as violations of constraints. In order to diagnose such failures, IFME approach has been extended to cope the presented failures form. Using IFME approach, the diagnoser is represented by two sets of inequalities in variables corresponding to observable transitions. These sets are obtained as follows. First, two sets of inequalities, derived from *state equations*, are augmented by the inequalities expressing the constraint and its violation. Then IFME method is applied to eliminate the variables corresponding to unobservable transitions. The resulting sets represent the diagnoser. The notion presented in this paper has been explained with the aid of a running example.

References

[Al-Ajeli and Bordbar, 2016] Ahmed Al-Ajeli and Behzad Bordbar. Fourier-motzkin method for failure diagnosis in petri net models of discrete event systems. In *Proceedings of the 13th International Workshop on Discrete Event Systems*, pages 165–170, Xi'an, China, 2016.

[Alodib and Bordbar, 2009] M. Alodib and B. Bordbar. A model-based approach to fault diagnosis in service oriented architectures. In *Proceedings of the IEEE European Conference on Web Services (ECOWS)*, pages 129–138, Netherlands, 2009.

[Basile *et al.*, 2008] Francesco Basile, Pasquale Chiacchio, and Gianmaria De Tommasi. Sufficient conditions for diagnosability of Petri nets. In *Proceedings of the 9th International Workshop on Discrete Event Systems*, Göteborg, Sweden, May 2008.

[Cabasino *et al.*, 2009] Maria Paola Cabasino, Alessandro Giua, Stephane Lafortune, and Carla Seatzu. Diagnosability analysis of unbounded Petri nets. In *48th IEEE Conference on Decision and Control*, pages 1267–1272, Shanghai, China, December 2009.

[Cabasino *et al.*, 2010] Maria Paola Cabasino, Alessandro Giua, and Carla Seatzu. Fault detection for discrete event systems using petri nets with unobservable transitions. *Automatica*, 46(9):1531–1539, 2010.

[Clarke *et al.*, 1999] Edmund M Clarke, Orna Grumberg, and Doron Peled. *Model checking*. MIT press, 1999.

[Dantzig, 1972] George B Dantzig. Fourier-motzkin elimination and its dual. Technical report, DTIC Document, 1972.

[Dotoli *et al.*, 2009] Mariagrazia Dotoli, Maria Pia Fanti, Agostino Marcello Mangini, and Walter Ukovich. On-line fault detection of discrete event systems by Petri nets and integer linear programming. *Automatica*, 45(11):2665–2672, 2009.

[Duffin, 1974] R.J. Duffin. On fourier's analysis of linear inequality systems. In M.L. Balinski, editor, *Pivoting and Extension*, volume 1 of *Mathematical Programming Studies*, pages 71–95. Springer Berlin Heidelberg, 1974.

[Genc and Lafortune, 2007] Sahika Genc and Stephane Lafortune. Distributed diagnosis of Place-Bordered Petri nets. *IEEE Transactions on Automatic Science and Enginnering*, 4(2):206–219, 2007.

[Jéron *et al.*, 2006] Thierry Jéron, Hervé Marchand, Sophie Pinchinat, and M-O Cordier. Supervision patterns in discrete event systems diagnosis. In *Discrete Event Systems, 2006 8th International Workshop on*, pages 262–268. IEEE, 2006.

[Jiroveanu *et al.*, 2008] George Jiroveanu, René K. Boel, and Behzad Bordbar. On-line monitoring of large Petri net models under partial observation. *Discrete Event Dynamic Systems*, 18:323–354, 2008.

[Kohler, 1967] David A Kohler. Projections of convex polyhedral sets. Technical report, DTIC Document, 1967.

[Kuhn, 1956] H. W. Kuhn. Solvability and consistency for linear equations and inequalities. *The American Mathematical Monthly*, 63(4):217–232, 1956.

[Murata, 1989] T. Murata. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, April 1989.

[Pugh, 1991] William Pugh. The omega test: a fast and practical integer programming algorithm for dependence analysis. In *Proceedings of the 1991 ACM/IEEE conference on Supercomputing*, pages 4–13. ACM, 1991.

[Sampath *et al.*, 1995] Meera Sampath, Raja Sengupta, Stephane Lafortune, Kasim Sinnamohideen, and Demosthenis Teneketzis. Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, 40(9):1555–1575, 1995.

[Tsuji and Murata, 1993] Kohkichi Tsuji and Tadao Murata. On reachability conditions for unrestricted petri nets. In *Circuits and Systems, 1993., ISCAS'93, 1993 IEEE International Symposium on*, pages 2713–2716. IEEE, 1993.

[Williams, 1976] H Paul Williams. Fourier-motzkin elimination extension to integer programming problems. *Journal of Combinatorial Theory, Series A*, 21(1):118–123, 1976.