A COMPARISON AMONG DIFFERENT NOTIONS OF ROBUST DIAGNOSABILITY AGAINST SENSOR FAILURES

Wesley R. Silveira*, Públio M. Lima*, Marcos V. Moreira*

*Cidade Universitária, Av. Athos da Silveira Ramos, 149 - CT
Universidade Federal do Rio de Janeiro
Rio de Janeiro, RJ, Brazil

Emails: wesley08@poli.ufrj.br, publio@poli.ufrj.br, moreira.mv@poli.ufrj.br

Abstract— Recently, different notions of robust diagnosability of discrete event systems (DES) against permanent and intermittent sensor failures have been proposed in the literature. In these works, different assumptions are considered regarding event observation losses, and different strategies for verifying the diagnosability of the language of the system subject to uncertainties in the event observations are presented. In this paper, we present the relation between different notions of robust diagnosability proposed in the literature, and we show that robust diagnosability against intermittent and permanent loss of observations are equivalent. We also show that observation masks can always be replaced with projections in the case of non selective sensor failures to model the diagnoser observation of the system, and that even in the case of non selective sensor failures, the two definitions of robust diagnosability of DES against permanent sensor failures proposed in the literature are not equivalent.

Keywords— Fault diagnosis, Discrete event systems, Robust diagnosability, Sensor failures.

Resumo— Recentemente, noções diferentes de diagnosticabilidade robusta de Sistemas a Eventos Discretos (SED) a falhas permanentes e intermitentes de sensores foram propostas na literatura. Nesses trabalhos, hipóteses distintas são consideradas com relação às perdas de observação de eventos, e diferentes estratégias para verificação da diagnosticabilidade da linguagem do sistema sujeita às incertezas nas observações de eventos são apresentadas. Neste trabalho, são apresentadas as relações entre diferentes noções de diagnosticabilidade robusta propostas na literatura, e é mostrado que as noções de diagnosticabilidade robusta a perdas intermitentes e permanentes de observação de eventos são equivalentes. É mostrado também que máscaras de observação podem sempre ser substituídas por projeções no caso de falhas não seletivas de sensores para modelar a observação do sistema pelo diagnosticador, e que mesmo no caso de falhas de sensores não seletivas, as duas noções de diagnosticabilidade robusta de SED com relação a falhas permanentes de sensores propostas na literatura não são equivalentes.

Palavras-chave— Diagnóstico de Falhas, Sistemas a eventos discretos, Diagnosticabilidade robusta, Falha de sensores.

1 Introduction

The problem of fault diagnosis of discrete event systems (DES) have been addressed in several works proposed in the literature (Lin; 1994; Sampath et al.; 1995; Qiu and Kumar; 2006; Moreira et al.; 2011). In these works, it is considered that the sensors used to record the occurrence of events always work correctly. However, sensors are subject to failures due, for instance, to aging degradation, dirt or atmospheric interference. In these cases, the diagnoser constructed assuming perfect sensor operation may get stuck, or even provide wrong diagnosis decisions, being necessary to construct a robust diagnoser when some sensors of the system are not reliable for fault diagnosis.

The problem of fault diagnosis of systems subject to sensor failures have been considered in Carvalho et al. (2012), Carvalho et al. (2013), and Kanagawa and Takai (2015), where different assumptions regarding sensor failures are considered, yielding to different notions of robust diagnosability of DES, and verification algorithms. In Carvalho et al. (2012), the problem of fault diagnosis of DES subject to intermittent loss of observations is considered, *i.e.*, it is assumed in Carvalho et al. (2012) that a subset of the observable event set is associated with unreliable sensors that can intermittently fail, losing the observation of the corresponding events. In Carvalho et al. (2013), permanent sensor failures are considered under the assumption that these failures occur only prior to the first observation of the event recorded by the defective sensor, *i.e.*, the event that should be observed is never observed by the diagnosis system. We call in this paper this notion of robust diagnosability as robust diagnosability against uncertainty in the observable event set, since the possible existence of a defective sensor in the system, leads to an uncertain observable event set.

More recently, in Kanagawa and Takai (2015), the assumption of sensor failure only before the first occurrence of the event to be recorded by the defective sensor is relaxed, and a definition of robust diagnosability against permanent sensor failures is proposed. An example is used to show that the language of a system can be robustly diagnosable in the sense proposed in Carvalho et al. (2013), and not robustly diagnosable using the definition presented in Kanagawa and Takai (2015). In order to do so, it is considered that the same sensor can be used to identify the occurrence of different events, and that the sensor failure can affect the observation of only one of the events that are detectable by the defective sensor.

This sensor failure behavior is called in this paper as selective sensor failure.

In this work, we show that the verification of robust diagnosability against intermittent loss of observations (Carvalho et al.; 2012) is equivalent to the robust diagnosability against permanent loss of observations, which is a particular case of the robust diagnosability against uncertain observable event set (Carvalho et al.; 2013). Moreover, we show that in the case of non selective sensor failures, it is always possible to replace observation masks with projections to model the observation of the system by the diagnoser. This allows us to compare the notions of robust diagnosability against permanent sensor failures proposed in the literature in a more realistic way, and we show that the robust diagnosability against permanent sensor failures proposed in Kanagawa and Takai (2015) is not equivalent to the definition of robust diagnosability against uncertain observable event set, even if non selective sensor failures are considered.

This paper is organized as follows. In Section 2 we present some preliminary concepts, and the following definitions: (*i*) robust diagnosability against intermittent loss of observations (Carvalho et al.; 2012); (*ii*) robust diagnosability against uncertain observable event set (Carvalho et al.; 2013); and (*iii*) robust diagnosability against permanent sensor failures (Kanagawa and Takai; 2015). In Section 3, we compare the three notions of robust diagnosability proposed in the literature. The conclusions are drawn in Section 4.

2 Preliminaries

2.1 Notations and definitions

In this paper $G = (X, \Sigma, f, x_0)$ denotes a deterministic automaton of a DES, where X is the set of states, Σ is the finite set of events, $f : X \times \Sigma^* \to X$ is the partial transition function, where Σ^* denotes the Kleene-closure of Σ, and x_0 is the initial state. The language generated by G is defined as $L = \{s \in \Sigma^* : f(x_0, s) \text{ is defined}\}$. The prefix-closure of a language L is given by $\overline{L} = \{s \in \Sigma^* : (\exists t \in \Sigma^*) \wedge (st \in L)\}$. The active event function $\Gamma : X \to 2^{\Sigma}$ is given as $\Gamma(x) = \{\sigma \in \Sigma : f(x, \sigma) \text{ is defined}\}$. Let us assume, without loss of generality, that the language generated by automaton G, L, is live, i.e., $\Gamma(x) \neq \emptyset$, for all $x \in X$.

Let ε denote the empty trace. The projection operation $P_s^l : \Sigma_l^* \to \Sigma_s^*$, where $\Sigma_s \subset \Sigma_l$ is defined as $P_s^l(\varepsilon) = \varepsilon$, $P_s^l(\sigma) = \sigma$, if $\sigma \in \Sigma_s$ or $P_s^l(\sigma) = \varepsilon$, if $\sigma \in \Sigma_l \setminus \Sigma_s$, and $P_s^l(s\sigma) = P_s^l(s)P_s^l(\sigma)$, for all $s \in \Sigma_l^*$, and $\sigma \in \Sigma_l$. The projection can also be applied to language L, by applying the projection to all traces $s \in L$. The inverse projection $P_s^{l^{-1}} : \Sigma_s^* \to 2^{\Sigma_l^*}$ when applied to a trace $s \in \Sigma_s^*$ generates all traces of Σ_l^* whose projection is equal to s. The inverse projection can also be applied to languages.

Let $M : \Sigma \to \Delta \cup \{\varepsilon\}$ be a mask, where Δ is a set of symbols. There are two types of masks: projection masks and non-projection masks. If a mask M is a projection mask, then each event $\sigma \in \Sigma$ is mapped to a different symbol in Δ, or it is mapped to the empty trace ε. On the other hand, if M is a non-projection mask, then there are at least two different events $\sigma_1, \sigma_2 \in \Sigma$ that are mapped to the same symbol $\delta \in \Delta$, *i.e.*, $M(\sigma_1) = M(\sigma_2) = \delta$. Mask M can be extended to $M : \Sigma^* \to \Delta^*$ as $M(s\sigma) = M(s)M(\sigma)$, for all $s \in \Sigma^*$, $\sigma \in \Sigma$, and $M(\varepsilon) = \varepsilon$.

Let us suppose that the event set of G is partitioned as $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$, where Σ_o and Σ_{uo} denote the sets of observable and unobservable events, respectively. The set of fault events is denoted here as $\Sigma_f \subseteq \Sigma_{uo}$. For the sake of simplicity, it is assumed in this paper that there is only one fault event, *i.e.*, $\Sigma_f = \{\sigma_f\}$.

A fault trace is a sequence of events s such that σ_f is one of the events that form s. A fault-free trace, on the other hand, does not contain event σ_f.

2.2 Diagnosability of Discrete Event Systems

Let G_N be the subautomaton of G that models the fault-free behavior of the system with respect to the fault event set Σ_f, *i.e.*, the language generated by G_N is $L_N \subset L$ formed of all fault-free traces generated by the system. Thus, the set of all fault traces generated by the system is $L \setminus L_N$, where $\setminus$ denotes set difference.

The following definition of language diagnosability can be stated (Sampath et al.; 1995).

Definition 1 *(Diagnosability of DES) Let L be the prefix-closed and live language generated by automaton G, and let $L_N \subset L$ be the prefix-closed language formed of all fault-free traces generated by the system. Then, L is said to be diagnosable with respect to projection $P_o : \Sigma^* \to \Sigma_o^*$, and Σ_f if:*

$$(\exists z \in \mathbb{N})(\forall s \in L \setminus L_N)(\forall st \in L \setminus L_N, \|t\| \geq z) \Rightarrow D$$

where the diagnosability condition D is

$$P_o(st) \neq P_o(\omega), \ \forall \omega \in L_N,$$

where $\|.\|$ denotes the length of a trace. □

In the following example, presented in Kanagawa and Takai (2015), we illustrate the diagnosability definition.

Example 1 *Let G be the automaton depicted in Figure 1, where $\Sigma = \{a, b, c, \sigma_f\}$. Let $\Sigma_o = \{a, c\}$*

and $\Sigma_{uo} = \{b, \sigma_f\}$. Since for all fault traces $\sigma_f aac^k \in L \setminus L_N$, with $k \geq 1$, and $\omega \in L_N$, we have that $P_o(\omega) \neq P_o(\sigma_f aac^k)$, then, according to Definition 1, L is diagnosable wit respect to P_o and Σ_f. Notice that if we consider a different set of observable events $\hat{\Sigma}_o = \{c\}$, then, the fault-free trace $\omega = abbc^k$ has the same projection $\hat{P}_o : \Sigma^* \to \hat{\Sigma}_o^*$ than the fault trace $\sigma_f aac^k$ for all values of $k \in \mathbb{N}$, which implies that L is not diagnosable with respect to $\hat{P}_o$ and Σ_f.

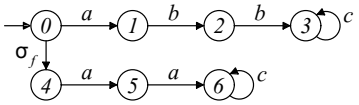


Figure 1: Automaton G.

2.3 Robust diagnosability against intermittent loss of observations

The problem of robust diagnosability subject to intermittent loss of observations (RDILO) has been introduced in Carvalho et al. (2012). In Carvalho et al. (2012), it is considered that some sensors, or the communication between sensors and diagnosers, may intermittently fail. In this case, the set of observable events is partitioned as $\Sigma_o = \Sigma_{ilo} \dot{\cup} \Sigma_{nilo}$, where Σ_{ilo} is the set of events subject to intermittent loss of observations, and Σ_{nilo} is the set of observable events that are not subject to intermittent loss of observations. In order to characterize the intermittent loss of observation, set $\Sigma'_{ilo} = \{\sigma' : \sigma \in \Sigma_{ilo}\}$ is created, where σ' is an unobservable event that models the loss of observation of event σ due to sensor malfunction or communication failure.

The following definition is presented in Carvalho et al. (2012) to obtain the language observed by the diagnoser due to the intermittent loss of observations of the events in Σ_{ilo}.

Definition 2 *(Dilation) Let $\Sigma = \Sigma_{ilo} \dot{\cup} \Sigma_{nilo} \dot{\cup} \Sigma_{uo}$, $\Sigma'_{ilo} = \{\sigma' : \sigma \in \Sigma_{ilo}\}$, and $\Sigma_{dil} = \Sigma \cup \Sigma'_{ilo}$. Then, the dilation D is the mapping $D : \Sigma^* \to 2^{\Sigma^*_{dil}}$ where*

$$D(\varepsilon) = \varepsilon,$$
$$D(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \Sigma \backslash \Sigma_{ilo}, \\ \{\sigma, \sigma'\}, & \text{if } \sigma \in \Sigma_{ilo}, \end{cases}$$
$$D(s\sigma) = D(s)D(\sigma), s \in \Sigma^*, \sigma \in \Sigma.$$

□

The dilation operation D can be extended from traces to languages by applying it to all traces in the language, that is, $D(L) = \bigcup_{s \in L} D(s)$.

According to Definition 2, the language observed by the diagnoser, when the sensors of the system associated with Σ_{ilo} are subject to intermittent failures, is given by $P_{dil,o}(D(L))$, where $P_{dil,o} : \Sigma^*_{dil} \to \Sigma^*_o$ is a projection.

In the sequel we present the definition of RDILO presented in Carvalho et al. (2012).

Definition 3 *(Robust diagnosability of DES against intermittent loss of observations) A prefix-closed and live language L is robustly diagnosable with respect to dilation D, projection $P_{dil,o} : \Sigma^*_{dil} \to \Sigma^*_o$ and Σ_f if the following holds true:*

$$(\exists z \in \mathbb{N})(\forall s \in L \backslash L_N)(\forall st \in L \backslash L_N, \|t\| \geq z) \Rightarrow R_I,$$

where the robust diagnosability condition R_I is

$$P_{dil,o}(D(st)) \cap P_{dil,o}(D(\omega)) = \emptyset, \forall \omega \in L_N$$

□

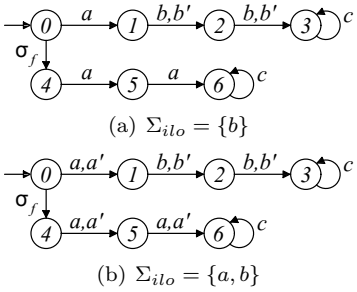
According to Definition 3, a system is said to be robustly diagnosable with respect to D, $P_{dil,o}$, and Σ_f if, and only if, there does not exist an arbitrarily long length fault trace st with the same observation, obtained considering the intermittent loss of observation of the events in Σ_{ilo}, computed as $D(st)$, than a fault-free trace ω, whose observation also considers the possible intermittent loss of observation modeled by $D(\omega)$. In Carvalho et al. (2012), to verify the RDILO of the language generated by automaton G, an automaton whose generated language is $D(L)$, G_{dil}, is computed by adding unobservable transitions labeled with $\sigma' \in \Sigma'_{ilo}$ in parallel to all transitions labeled with $\sigma \in \Sigma_{ilo}$ of G. Then, the verification algorithm proposed in Moreira et al. (2011) is applied to G_{dil}.

The following example illustrates the RDILO definition.

Example 2 *Let G be the plant automaton presented in Figure 1, and let us first consider that the sensor used to record the occurrence of event b is subject to intermittent failure, i.e. $\Sigma_{ilo} = \{b\}$, $\Sigma_{nilo} = \{a, c\}$, and $\Sigma_{uo} = \{\sigma_f\}$. Automaton G_{dil}, whose generated language is the dilation of L, $D(L)$, is depicted in Figure 2(a), where b' is the unobservable event that models the loss of observation of event b. In this case, the fault trace $\sigma_f aac^k \in L \setminus L_N$ has projection $P_{dil,o}(D(\sigma_f aac^k)) = \{aac^k\}$, for all values of $k \in \mathbb{N}$. In addition, it is not difficult to see that $P_{dil,o}(D(\sigma_f aac^k)) \cap P_{dil,o}(D(\omega)) = \emptyset$, for all $\omega \in L_N = \overline{abbc^*}$. Thus, L is robustly diagnosable against the intermittent loss of observation of event b.*

Let us now consider that events a and b are subject to intermittent loss of observations. In this case, the automaton that generates language $D(L)$, G_{dil}, is presented

in Figure 2(b), where it can be seen that $P_{dil,o}(D(\sigma_f aac^k)) = \{c^k, ac^k, aac^k\}$. *Moreover, since* $P_{dil,o}(D(abbc^k)) = \{c^k, ac^k, bc^k, bbc^k, abc^k, abbc^k\}$, *then* $P_{dil,o}(D(\sigma_f aac^k)) \cap P_{dil,o}(D(abbc^k)) \neq \emptyset$, *for all values of* $k \in \mathbb{N}$, *which implies, according to Definition 3, that* L *is not robustly diagnosable against the intermittent loss of observations of events* a *and* b.



(a) $\Sigma_{ilo} = \{b\}$

(b) $\Sigma_{ilo} = \{a, b\}$

Figure 2: Automata G_{dil}.

2.4 Robust diagnosability against uncertainty in the observable event set

In Carvalho et al. (2013), the problem of robust diagnosis against permanent loss of observations is considered, and the following assumption is carried out.

A1. Any loss of observations, when it occurs, takes place before the first occurrence of the (initially observable) event associated with the sensor that has failed, and it is permanent, *i.e.*, the event remains unobservable.

In this case, the actual set of observable events is unknown, *i.e.*, Σ_o denotes the set of potentially observable events of the system, and the objective is to construct a diagnosis scheme for the DES subject to an uncertain observable event set. For this reason, this problem is called in this paper as robust diagnosis against uncertainty in the observable event set (RDUOES).

Let us suppose that there are m possible losses of observation of events of Σ_o, $\Sigma^j_{plo} \subset \Sigma_o$, for $j = 1, \ldots, m$, where Σ^j_{plo} can be equal to the empty set, and let us suppose that one of them corresponds to the actual loss of observation of the system events. Thus, $\Sigma^j_o = \Sigma_o \setminus \Sigma^j_{plo}$, for $j = 1, \ldots, m$ denotes a possible set of observable events of the system. Then, the following definition of RDUOES can be presented Carvalho et al. (2013).

Definition 4 *(Robust diagnosability against uncertainty in the observable event set) Let* Σ^j_o, $j = 1, \ldots, m$, *denote a possible set of observable events of an automaton* G, *and let* $\Sigma^j_{plo} = \Sigma_o \setminus \Sigma^j_o$, $j = 1, \ldots, m$, *denote a possible permanent loss of observation of the events of* Σ_o. *Then, the prefix-closed and live language* L *generated by* G *is robustly diagnosable with respect to* $P^j_o : \Sigma^* \to \Sigma^{j*}_o$, $j = 1, \ldots, m$, *and* Σ_f, *or equivalently with respect to the permanent loss of observation of the events of all sets* Σ^j_{plo}, $j = 1, \ldots, m$, *and* Σ_f *if:*

$$(\exists z \in \mathbb{N})(\forall s \in L \setminus L_N)(\forall st \in L \setminus L_N, \|t\| \geq z) \Rightarrow R_P$$

where the robust diagnosability condition R_P *is*

$$(\forall k, l \in \{1, \ldots, m\})[P^k_o(st) \neq P^l_o(\omega),\ \forall \omega \in L_N].$$

□

According to Definition 4, if there exists an arbitrarily long length trace st, and a fault-free trace ω such that $P^k_o(st) = P^l_o(\omega)$, then we are not sure if the fault trace st has been executed by the system and the correct observable event set is Σ^k_o, or if the fault-free trace ω has been executed and the correct observable event set is Σ^l_o. Thus, in this case, the language of the system L is not robustly diagnosable against uncertainty in the observable event set.

Example 3 *Consider the same system presented in Figure 1 where* $\Sigma_o = \{a, b, c\}$, *and let us assume that we are uncertain about the observation of event* b, *i.e., we have two different possible permanent observation losses* $\Sigma^1_{plo} = \emptyset$, *and* $\Sigma^2_{plo} = \{b\}$. *Thus, in order to verify if* L *is robustly diagnosable with respect to* P^1_o, P^2_o, *and* Σ_f, *it is necessary to investigate if the fault event can be detected even if we are not sure about the observation of* b. *In this example, if the fault trace* $\sigma_f aa$ *is executed, then* $P^1_o(\sigma_f aa) = P^2_o(\sigma_f aa) = aa$, *and there is no fault-free trace* $\omega \in L_N$ *such that* $P^1_o(\sigma_f aa) = P^1_o(\omega)$, *or* $P^1_o(\sigma_f aa) = P^2_o(\omega)$, *or* $P^2_o(\sigma_f aa) = P^1_o(\omega)$, *or* $P^2_o(\sigma_f aa) = P^2_o(\omega)$. *Thus, we are sure that the fault has occurred after the execution of trace* $\sigma_f aa$, *being* b *observable or not, and* L *is robustly diagnosable against uncertainty in the observation of* b.

Let us now assume that we are uncertain about the observation of events a *and* b, *i.e., we have the following four possible losses of observation of events:* $\Sigma^1_{plo} = \emptyset$; $\Sigma^2_{plo} = \{a\}$; $\Sigma^3_{plo} = \{b\}$; *and* $\Sigma^4_{plo} = \{a, b\}$. *In this case, it can be seen that it is not possible to know if trace* $\sigma_f aac^k$ *has been executed by the system and event* a *became unobservable, or if trace* $abbc^k$ *has been executed and both events* a *and* b *became unobservable. This reasoning is expressed as* $P^2_o(\sigma_f aac^k) = P^4_o(abbc^k) = c^k$, *for all* $k \in \mathbb{N}$. *Thus, according to Definition 4,* L *is not robustly diagnosable with respect to* P^j_o, $j = 1, \ldots, 4$, *and* Σ_f.

2.5 Robust diagnosability against permanent sensor failures

A different notion of robust diagnosability against permanent sensor failures (RDPSF) is addressed in Kanagawa and Takai (2015). In Kanagawa and

Takai (2015) assumption **A1** is relaxed, and the sensor failure can occur at any time, even after the first observation of the event recorded by the defective sensor, leading to the loss of observation of the event. In addition, differently from Carvalho et al. (2013) and Carvalho et al. (2012), that assume projections to model the observation of events, in Kanagawa and Takai (2015) masks are considered to model the observation of events, *i.e.*, different events can be observed by the diagnoser using the same symbol. Based on this fact, the sensor failures considered in Kanagawa and Takai (2015) can be selective in the sense that the observation of only one of the events that are recorded by the same defective sensor can be lost. In order to relax assumption **A1**, the following definition of observation mask subject to permanent sensor failure is presented in Kanagawa and Takai (2015).

Definition 5 *(Mask subject to permanent sensor failures) Let $M : \Sigma \to \Delta \cup \{\varepsilon\}$ denote the nominal observation mask obtained considering that none of the observable events lose observation, and let $M_i : \Sigma \to \Delta_i \cup \{\varepsilon\}$, where $\Delta_i \subset \Delta$ and $i \in I = \{1, 2, \ldots, m\}$, represent a possible loss of observation of events due to permanent sensor failures. Then, the observation mask subject to permanent sensor failures $M_f : \Sigma^* \to 2^{\Delta^*}$ is defined as $M_f(s) = \{M(s_1)M_i(s_2) : s_1 s_2 = s \wedge i \in I\}$.* □

According to Definition 5, the set of all observed traces due to permanent sensor failures of a language L is given by $M_f(L) = \bigcup_{s \in L} M_f(s)$. Notice that the transition from mask M to M_i after the occurrence of s_1 represents the instant when the permanent sensor failure occurs, and mask M_i indicates which observations have been lost.

In the sequel, we present the definition of RDPSF proposed in Kanagawa and Takai (2015).

Definition 6 *A prefix-closed and live language L is said to be robustly diagnosable with respect to the observation mask $M_f : \Sigma^* \to 2^{\Delta^*}$, and Σ_f if:*

$$(\exists z \in \mathbb{N})(\forall s \in L \backslash L_N)(\forall st \in L \backslash L_N, \|t\| \geq z) \Rightarrow R_S$$

where condition R_S is given as

$$[M_f(st) \cap M_f(\omega) = \emptyset, \forall \omega \in L_N)].$$

□

Example 4 *Consider the system presented in figure 1, where $\Sigma = \{a, b, c, \sigma_f\}$, $\Delta = \{\alpha, \beta\}$ and the nominal mask M is such that $M(a) = M(b) = \alpha$, $M(c) = \beta$, and $M(\sigma_f) = \varepsilon$. Notice that event c is identified from the observation of β while events a and b cannot be distinguished. Let us consider that event b becomes unobservable due to a selective sensor failure, i.e., the sensor that observes both a and b loses the capability of sensing only event b, and is always capable of observing event a. Then, M_1 is given as $M_1(a) = \alpha$, $M_1(c) = \beta$, and $M_1(\sigma_f) = M_1(b) = \varepsilon$. In this case, if the system executes the fault-free trace $abbc^k$, and the observation of event b is lost after the first observation of b, then the diagnoser observes trace $M(ab)M_1(bc^k) = \alpha\alpha\beta^k$. Since $M(\sigma_f aac^k) = \alpha\alpha\beta^k$, then L is not robustly diagnosable with respect to mask M_f and Σ_f.*

In the next section we compare the three notions of robust diagnosability proposed in the literature.

3 Relation among the robust diagnosability notions

In this section, we compare the notions of robust diagnosability presented in the previous section. We show first that language L is robustly diagnosable against the intermittent loss of observations of the events in set Σ_{ilo} if, and only if, L is diagnosable with respect to projection $P_{nilo} : \Sigma^* \to \Sigma^*_{nilo}$ and Σ_f, *i.e.*, the intermittent observation of the events in Σ_{ilo} does not contribute to the robust diagnosability of L.

Theorem 1 *Let L be a prefix-closed and live language, and $\Sigma = \Sigma_{ilo} \dot{\cup} \Sigma_{nilo} \dot{\cup} \Sigma_{uo}$. Then, L is robustly diagnosable with respect to dilation D, projection $P_{dil,o} : \Sigma^*_{dil} \to \Sigma^*_o$, and Σ_f if, and only if, L is diagnosable with respect to projection $P_{nilo} : \Sigma^* \to \Sigma^*_{nilo}$, and Σ_f.*

Proof: ($\Rightarrow$) Let us assume that L is robustly diagnosable with respect to D, $P_{dil,o}$ and Σ_f. Then, there exists $z \in \mathbb{N}$ such that for all fault trace $st \in L \setminus L_N$, where $\|t\| \geq z$, $P_{dil,o}(D(st)) \cap P_{dil,o}(D(\omega)) = \emptyset$, for all $\omega \in L_N$. Since $P_{nilo}(st) \in P_{dil,o}(D(st))$, and $P_{nilo}(\omega) \in P_{dil,o}(D(\omega))$, then it is straightforward to see that $P_{nilo}(st) \neq P_{nilo}(\omega)$, for all $\omega \in L_N$, and thus, L is diagnosable with respect to P_{nilo} and Σ_f.

($\Leftarrow$) Let us assume now that L is diagnosable with respect to P_{nilo} and Σ_f. Then, there exists $z \in \mathbb{N}$ such that for all $st \in L \setminus L_N$, where $\|t\| \geq z$, $P_{nilo}(st) \neq P_{nilo}(\omega)$, for all $\omega \in L_N$. Since, $\Sigma_{ilo} \cap \Sigma_{nilo} = \emptyset$, and according to the definitions of D (Definition 2) and $P_{dil,o}$, all traces in $P_{dil,o}(D(st))$ and $P_{dil,o}(D(\omega))$, are obtained by adding events in Σ_{ilo} to the traces of $P_{nilo}(st)$ and $P_{nilo}(\omega)$, respectively, then $P_{dil,o}(D(st)) \cap P_{dil,o}(D(\omega)) = \emptyset$. Thus, according to Definition 3, L is robustly diagnosable with respect to D, $P_{dil,o}$ and Σ_f. ■

Notice that the diagnosability of L with respect to P_{nilo} and Σ_f is equivalent to the robust diagnosability of L against permanent loss of observations of the events in Σ_{ilo} under Assumption **A1**, which is a particular case of the RDUOES

presented in Definition 4. Thus, Theorem 1 shows that the robust diagnosability of L against intermittent loss of observations of the events in Σ_{ilo} is equivalent to the robust diagnosability of L against uncertainty in the observable event set, considering Σ_{ilo} as the unique possible loss of observation of events, Σ_{plo}. In this particular case, the verification of RDILO can be carried out using any diagnosability verification procedure proposed in the literature (Qiu and Kumar; 2006; Moreira et al.; 2011), being not necessary to compute G_{dil} as it is done in Carvalho et al. (2012). In Figure 3 we show the implications of theorem 1.

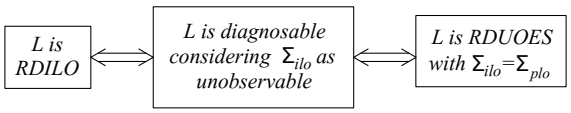


Figure 3: Relation between RDILO and RDUOES of Theorem 1.

In the sequel we compare the definitions of RDUOES and RDPSF. First of all, notice that it is always possible to replace a non projection mask $M : \Sigma \to \Delta \cup \{\varepsilon\}$ with a projection $P : (\Delta \cup \Sigma_{uo})^* \to \Delta^*$, and obtain an equivalent automaton G_{eq}, such that $M(L) = P(L_{eq})$, where L_{eq} is the language generated by G_{eq}. In order to compute G_{eq}, all transitions of G labeled with observable events in Σ_o are replaced with their corresponding symbol in Δ, and all transitions of G labeled with unobservable events remain unaltered. In the sequel, the equivalent projection P is computed as: (i) if for $\sigma \in \Sigma$ and $\delta \in \Delta$, we have that $M(\sigma) = \delta$, then $P(\delta) = \delta$; (ii) if $M(\sigma) = \varepsilon$, then $P(\sigma) = \varepsilon$. The following example illustrates the replacement of the observation mask with a projection that does not alter the observation of the language generated by the system.

Example 5 *Let us consider the same problem presented in Example 4, where $M(a) = M(b) = \alpha$, $M(c) = \beta$, and $M(\sigma_f) = \varepsilon$. In this case, the domain for the equivalent projection P is $\{\alpha, \beta, \sigma_f\}$, and $P(\alpha) = \alpha$, $P(\beta) = \beta$ and $P(\sigma_f) = \varepsilon$. In order to obtain an automaton G_{eq} whose observed language considering projection P is equal to the observed language for the automaton G of Figure 1 using mask M, it suffices to replace events a and b with α, and event c with β, as shown in Figure 4.*

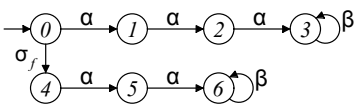


Figure 4: Automaton G_{eq}, where $P(L_{eq}) = M(L)$.

The sensor failures considered in Carvalho et al. (2013) are related with sensor malfunction, that can be caused by aging degradation, dirt, atmospheric interference, or problems in the communication between sensor and diagnoser. In this regard, even if the same sensor is used to detect the occurrence of different events, then any occurrence of these events may be permanently lost. This sensor failure behavior is non selective, and projections can be used to model the observation of the system events. However, if a very specific kind of sensor failure occurs, that makes the sensor be capable of always identifying the occurrence of one of the events that it can record, and never be capable of recording the occurrence of a different event, then projections cannot be used to model the observed behavior of the system, since the knowledge of which event observation is lost is not preserved using projections. Thus, only in this very special case of selective sensor failure, we cannot use projections to model the diagnoser observation of the events generated by the system. In the sequel, we consider that the sensor failure is non selective, and, in order to compare the notions of RDUOES and RDPSF, we rewrite Definitions 5 and 6 using projections instead of masks to model the observation of the events, and define the robust diagnosability against non selective permanent sensor failures (RDNSPSF).

Definition 7 *(Projection subject to permanent sensor failures) Let $P_o : \Sigma^* \to \Sigma_o^*$ denote the nominal projection obtained considering that none of the observable events lose observation, and let $P_o^j : \Sigma^* \to \Sigma_o^{j*}$, where $\Sigma_o^j \subset \Sigma_o$ and $j \in I = \{1, 2, \ldots, m\}$, represent a possible loss of observation of events due to permanent sensor failures. Then, the projection subject to permanent sensor failures $P_f : \Sigma^* \to 2^{\Sigma_o^*}$ is defined as $P_f(s) = \{P_o(s_1)P_o^j(s_2) : s_1 s_2 = s \wedge j \in I\}$.* □

Definition 8 *(Robust diagnosability against non selective permanent sensor failures) A prefix-closed and live language L is said to be robustly diagnosable with respect to projection $P_f : \Sigma^* \to 2^{\Sigma_o^*}$, and Σ_f if:*

$$(\exists z \in \mathbb{N})(\forall s \in L \setminus L_N)(\forall st \in L \setminus L_N, \|t\| \geq z) \Rightarrow S_f$$

where condition S_f is

$$[P_f(st) \cap P_f(\omega) = \emptyset, \forall \omega \in L_N)].$$

□

The following result shows that if L is robustly diagnosable against non selective permanent sensor failures, then L is robustly diagnosable against uncertain observable event sets.

Theorem 2 *If L is robustly diagnosable with respect to P_f and Σ_f, then L is robustly diagnosable with respect to $P_o^j : \Sigma^* \to \Sigma_o^{j*}$, $j = 1, \ldots, m$, and Σ_f.*

Proof: Suppose that L is robustly diagnosable with respect to P_f and Σ_f. Then, there exists $z \in \mathbb{N}$ such that for all fault trace st, where $\|t\| \geq z$, we have that $P_f(st) \cap P_f(\omega) = \emptyset$, for all $\omega \in L_N$. Since, according to Definition 7, $P_o^k(st) \in P_f(st)$, and $P_o^l(\omega) \in P_f(\omega)$, for $k, l \in I$, then it is straightforward to see that $P_o^k(st) \neq P_o^l(\omega)$, which implies, according to Definition 4, that L is robustly diagnosable with respect to P_o^j and Σ_f. ■

In Figure 5, we show the implications of Theorem 2.

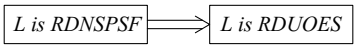


Figure 5: Relation between RDNSPSF and RDUOES of Theorem 2.

The converse of Theorem 2, however, is not true. In order to show this fact, in Kanagawa and Takai (2015) a selective sensor failure and a non projection mask are considered, which are unrealistic from the practical point of view. In the following example we show that even when projections are used and non selective sensor failures are considered, the RDUOES does not necessarily imply in the RDNSPSF.

Example 6 *Consider automaton G depicted in Figure 6, where $\Sigma = \{a, b, c, d, \sigma_f\}$, $\Sigma_o = \{b, c, d\}$, and $\Sigma_{uo} = \{\sigma_f, a\}$. Let us suppose that we are uncertain about the observation of events c and d, and we have defined the following possible permanent loss of observation $\Sigma_{plo}^1 = \{d\}$, and $\Sigma_{plo}^2 = \{c\}$. Thus, $P_o^1 : \Sigma^* \to \Sigma_o^{1*}$, and $P_o^2 : \Sigma^* \to \Sigma_o^{2*}$, where $\Sigma_o^1 = \{b, c\}$, and $\Sigma_o^2 = \{b, d\}$, denote the projections associated with the permament loss of events d and c, respectively. In this case, it is easy to see that if the permanent loss of observation occurs after the execution of trace cd, then $P_o(cd)P_o^1(\sigma_f(bd)^k) = cdb^k$, which is equal to $P_o(cd)P_o^2(a(cb)^k) = cdb^k$. Thus, according to Definition 8, L is not robustly diagnosable against the permanent loss of observation of events d and c relaxing Assumption* **A1**. *However, if Assumption* **A1** *is considered, i.e., the loss of observation occurs prior to the first observation of the event, then we have that $P_o^1(cd\sigma_f(bd)^k) = cb^k$, $P_o^1(cda(cb)^k) = c(cb)^k$, $P_o^2(cd\sigma_f(bd)^k) = d(bd)^k$, and $P_o^2(cda(cb)^k) = db^k$. Thus, according to Definition 4, L is robustly diagnosable against permanent sensor failure under Assumption* **A1**.

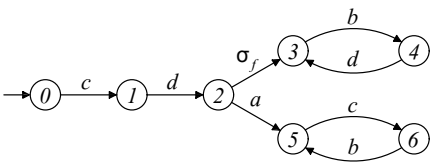


Figure 6: Automaton G.

In the sequel, we present a condition that implies that if L is not robustly diagnosable in the sense of Kanagawa and Takai (2015), then L is also not robustly diagnosable in the sense of Carvalho et al. (2013).

Theorem 3 *Let $st \in L \setminus L_N$, and $\omega \in L_N$, be written as $st = u_1u_2$ and $\omega = v_1v_2$. If there exists an arbitrarily long length trace st, and a trace ω such that $P_o(u_1)P_o^k(u_2) = P_o(v_1)P_o^l(v_2)$, for $k, l \in I$, and $P_o(u_1) \in \Sigma_o^{k\star}$ and $P_o(v_1) \in \Sigma_o^{l\star}$, then L is not robustly diagnosable with respect to P_o^j, $j = 1, \ldots, m$, and Σ_f.*

Proof: Notice that if $P_o(u_1) \in \Sigma_o^{k\star}$ and $P_o(u_2) \in \Sigma_o^{l\star}$, then $P_o(u_1) = P_o^k(u_1)$, and $P_o(v_1) = P_o^l(v_1)$. Thus, if $P_o(u_1)P_o^k(u_2) = P_o(v_1)P_o^l(v_2)$, we have that $P_o^k(u_1u_2) = P_o^l(v_1v_2)$, which implies, according to Definition 4, that L is not robustly diagnosable with respect to P_o^j and Σ_f. ■

In Example 6, the condition of Theorem 3 is not satisfied. In order to see this fact, notice that the fault trace $st = cd\sigma_f(bd)^k$ and the fault-free trace $\omega = cda(cb)^k$ can be divided, respectively, as $st = u_1u_2$, where $u_1 = cd$ and $u_2 = \sigma_f(bd)^k$, and $\omega = v_1v_2$, where $v_1 = cd$ and $v_2 = a(cb)^k$. Since $P_o(cd) \notin \Sigma_o^{j*}$, for $j = 1, 2$, we have that the condition of Theorem 3 is not satisfied. However, in the cases that the condition of Theorem 3 is satisfied, RDUOES and RDNSPSF are equivalent.

4 Conclusions

In this paper, we present a comparison between different notions of robust diagnosability proposed in the literature. We show that robust diagnosability against intermittent and permanent observation losses are equivalent. We also show that under a more realistic type of sensor failure, called non selective sensor failure, observation masks can always be replaced with projections to represent event observation losses. Moreover, we show that under non selective sensor failure, the language of a system can be robustly diagnosable against uncertain observable event sets and not against permanent sensor failures.

Acknowledgments

The authors would like to thank the anonymous reviewers for their useful comments and suggestions. This work has been partially supported by CNPq.

References

Carvalho, L. K., Basilio, J. C. and Moreira, M. V. (2012). Robust diagnosis of discrete-event systems against intermittent loss of observations, *Automatica* **48**(9): 2068–2078.

Carvalho, L. K., Moreira, M. V., Basilio, J. C. and Lafortune, S. (2013). Robust diagnosis of discrete-event systems against permanent loss of observations, *Automatica* **49**(1): 223–231.

Kanagawa, N. and Takai, S. (2015). Diagnosability of discrete event systems subject to permanent sensor failures, *International Journal of Control* **88**(12): 2598–2610.

Lin, F. (1994). Diagnosability of discrete event systems and its applications, *Discrete Event Dynamic Systems* **4**(2): 197–212.

Moreira, M. V., Jesus, T. C. and Basilio, J. C. (2011). Polynomial time verification of decentralized diagnosability of discrete event systems, *IEEE Transactions on Automatic Control* **56**(7): 1679–1684.

Qiu, W. and Kumar, R. (2006). Decentralized failure diagnosis of discrete event systems, *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans* **36**(2): 384–395.

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