Diagnosability analysis of an ABS system modeled using Petri nets

Maria Paola Cabasino, Alessandro Giua, Carla Seatzu*

August 27, 2013

Abstract

We consider the braking system of a vehicle equipped with an ABS. In a previous paper we presented a Petri net model of such a device assuming that the sensor that activates the ABS can be affected by a stuck-at-on fault. Here, the case in which the ABS sensor can be affected by both a stuck-at-on and a stuck-at-off fault is considered. Firstly, we consider the case in which the braking subsystems of different wheels cannot exchange information neither between them, nor with a coordinator. We show that in this local setting, where diagnosis is performed independently at each wheel, faults are not diagnosable. Secondly, we show that in a centralized setting, where the diagnoser can monitor each single wheel, the overall system is diagnosable. Finally, we assume that the braking systems of two wheels on the same side of the vehicle can exchange information and propose a communication protocol that makes the overall system diagnosable assuming both wheels are always in the same grip condition.

Published as:
M.P. Cabasino, A. Giua, C. Seatzu, "Diagnosability analysis of an ABS system modeled using Petri nets," *SAFEPROCESS12: 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes* (Mexico City, Mexico), Aug 2012.

*M.P. Cabasino, A. Giua and C. Seatzu are with the Department of Electrical and Electronic Engineering, University of Cagliari, Piazza D'Armi, 09123 Cagliari, Italy. E-mail:{cabasino,giua,seatzu}@diee.unica.it.

This work has been partially supported by the European Community's Seventh Framework Programme under project DISC (Grant Agreement n. INFSO-ICT-224498).

1 Introduction

In automotive an X-by-Wire system is a system controlled through a communication channel [7]. "By wire" denotes a control system that replaces traditional hydraulic or mechanical linkage with electronic connections between control units that drive electromechanical actuators. Such new systems have received a lot of attention by the car manufacturers for several reasons. First, the purpose of an X-by-Wire system is to assist the driver in different situations. This increases the overall vehicle safety, as the driver does not have to be concerned of the routine task any more. Another advantage are the lower costs of production of this type of systems. Furthermore, an X-by-Wire system is also called a dry system, as the hydraulic are no longer necessary: this leads to a simpler and more easily maintained system.

In this paper we focus on a Brake-by-Wire system combined with a high level brake function: the Anti-lock Braking System (ABS). The main purpose of ABS is to prevent the wheels on a motor vehicle from locking up while braking. In modern cars the whole system is composed of four different ABS, one for each wheel, that work locally and independently. The reliability of ABS has been studied by several authors [6, 5, 8]. In particular, in [6] Jerath and Sheldon model the ABS of a vehicle system using stochastic Petri nets (PNs). Their model includes the failure modes and effects associated with the failure rates of critical components. In [5] and [8] respectively Guerin *et al.* and Mihalache *et al.* model the mechanical, electronic and embedded software sub-systems, to design, check and estimate the reliability of the ABS. Their model, that is a stochastic PN system, takes into account the faulty behavior of the different components.

In [4] we presented a PN model of the ABS sensor taking into account its unreliability in the case of stuck-at-on fault. In this paper we extend the preliminary results obtained in [4] also considering the faulty behavior in the case of stuck-at-off fault. We first analyze the model considering only the stuck-at-off fault and then both stuck-at faults. For both models we analyze their diagnosability properties concluding that are locally non diagnosable. To do this we use the approach in [1]. Finally, on the basis of the results obtained studying the diagnosability of the centralized system, we propose a distributed communication protocol that, applied to the front and the rear wheels on the same axle of the car, makes the system locally diagnosable with communication.

2 Background on Petri nets

In this section we briefly recall the formalism used in the paper. For more details on PNs we refer to [9].

A *Place/Transition net* (P/T net) is a structure $N = (P, T, Pre, Post)$, where P is a set of m places; T is a set of n transitions; $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the *pre*– and *post*– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a P/T net a nonnegative integer

number of tokens, represented by black dots. We denote $M(p)$ the marking of place p. A P/T *system* or *net system* $\langle N, M_0 \rangle$ is a net N with an initial marking M_0. A transition t is enabled at M iff $M \geq Pre(\cdot, t)$ and may fire yielding the marking $M' = M + C(\cdot, t)$. We write $M\ [\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and we write $M\ [\sigma\rangle\ M'$ to denote that the firing of σ yields M'. We also write $t \in \sigma$ to denote that a transition t is contained in σ. The set of all sequences that are enabled at the initial marking M_0 is denoted $L(N, M_0)$, i.e., $L(N, M_0) = \{\sigma \in T^* \mid M_0[\sigma\rangle\}$. Given a sequence $\sigma \in T^*$, we call $\pi : T^* \to \mathbb{N}^n$ the function that associates with σ a vector $y \in \mathbb{N}^n$, named the *firing vector* of σ. In particular, $y = \pi(\sigma)$ is such that $y(t) = k$ if the transition t is contained k times in σ.

A marking M is *reachable* in $\langle N, M_0 \rangle$ iff there exists a firing sequence σ such that $M_0\ [\sigma\rangle\ M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0 \rangle$ and is denoted $R(N, M_0)$. Finally, a net system $\langle N, M_0 \rangle$ is *bounded* if there exists a positive constant k such that, for $M \in R(N, M_0)$, $M(p) \leq k$.

3 Fault diagnosis and diagnosability of Petri nets

In this section we provide a short overview of the main definitions that will be used in the rest of the paper. For more details we refer to [1, 2].

3.1 Fault diagnosis

A *labeling function* $\mathcal{L} : T \to L \cup \{\varepsilon\}$ assigns to each transition $t \in T$ either a symbol from a given alphabet L or the empty string ε.

We denote T_u the set of transitions whose label is ε, i.e., $T_u = \{t \in T \mid \mathcal{L}(t) = \varepsilon\}$. Transitions in T_u are called *unobservable* or *silent*. We denote T_o the set of transitions labeled with a symbol in L. Transitions in T_o are called *observable* because when they fire their label can be observed. We assume that the same label $l \in L$ can be associated with more than one transition. Two transitions $t_1, t_2 \in T_o$ are called *undistinguishable* if they share the same label, i.e., $\mathcal{L}(t_1) = \mathcal{L}(t_2)$. When a sequence σ is generated the word $w = \mathcal{L}(\sigma)$ is observed, where $\mathcal{L}(\sigma)$ is the natural extension of the labeling operator to the sequences, i.e., $\mathcal{L} : T^* \to L^*$.

Assume that the set of unobservable transitions is partitioned into two subsets, namely $T_u = T_f \cup T_{reg}$ where T_f includes all fault transitions, while T_{reg} includes all transitions relative to unobservable but regular events. The set T_f is further partitioned into r different subsets T_f^i, where $i = 1, \ldots, r$, that model the different fault classes.

Let $\langle N, M_0, \mathcal{L} \rangle$ be a labeled net system with labeling function $\mathcal{L}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$.

• Let $w = \mathcal{L}(\sigma)$ the word of events associated with the sequence σ. We define $\mathcal{S}(w) = \{\sigma \in L(N, M_0) \mid \mathcal{L}(\sigma) = w\}$ the set of sequences consistent with $w \in L^*$.

• Given a word $w \in L^*$, let $\sigma_o \in T_o^*$ be a sequence of observable transitions such that $\mathcal{L}(\sigma_o) = w$. We call *justification of* w a sequence σ_u of unobservable transitions interleaved with σ_o whose firing enables σ_o and whose firing vector is minimal. Since in general σ_o is not unique and more than one σ_u may be associated with each σ_o, then the set of justifications of w is not a singleton.

• Let $w \in L^*$ be a given observation. Let $\sigma \in T^*$, we denote $P_u(\sigma)$, resp., $P_o(\sigma)$, the projection of σ over T_u, resp., T_o. We define

$$\begin{aligned}\hat{\mathcal{J}}(w) \quad = \{\ (\sigma_o, \sigma_u)\ \mid [\exists \sigma \in \mathcal{S}(w)\ :\ \sigma_o = P_o(\sigma),\\ \sigma_u = P_u(\sigma)] \wedge\ [\nexists \sigma' \in \mathcal{S}(w) :\ \sigma_o = P_o(\sigma'),\\ \sigma'_u = P_u(\sigma') \wedge\ \pi(\sigma'_u) \lneq \pi(\sigma_u)]\}\end{aligned}$$

the set of pairs (sequence $\sigma_o \in T_o^*$ with $\mathcal{L}(\sigma_o) = w$, corresponding *justification* of w). Finally, we define

$$\hat{Y}_{\min}(M_0, w) = \{(\sigma_o, y) \mid \exists (\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w) : \pi(\sigma_u) = y\}$$

the set of pairs (sequence $\sigma_o \in T_o^*$ with $\mathcal{L}(\sigma_o) = w$, corresponding *j-vector*).

3.2 Diagnosability

Definition 3.1 *[3] A labeled PN system $\langle N, M_0, \mathcal{L}\rangle$ having no deadlock after the occurrence of any transition $t_f \in T_f^i$, for $i \in \{1, \ldots, r\}$, is* not diagnosable with respect to the fault class T_f^i *if given any $k \in \mathbb{N}$ there exist two firing sequences σ_1 and $\sigma_2 \in T^*$ satisfying the following four conditions:*

- $\mathcal{L}(\sigma_1) = \mathcal{L}(\sigma_2)$;
- $\sigma_1 \in (T \setminus T_f^i)^*$;
- *there exists at least one fault transition $t_f \in T_f^i$ such that $t_f \in \sigma_2$,*
- *σ_2 is of "arbitrary length" after fault $t_f \in T_f^i$, i.e., there exists at least one decomposition $\sigma_2 = \sigma'_2 t_f \sigma''_2$ with $|\sigma''_2| > k$.* ■

4 Problem statement

The Anti-lock Braking System is an electronic brake safety system which prevents the wheels on a motor vehicle from locking up while braking. The whole system is composed of four different ABS, one for each wheel, that work locally and independently. Usually in a braking system with ABS there are two brake conditions:

•*Normal brake* is the condition when the ABS is not operating and the braking force is continuously applied to the wheel.
•*Safety Brake* is the condition when the ABS is operating and in this case the braking force applied to the wheel is modulated in order to prevent the wheel to lock.

The considered system consists of a global controller (GC) and 4 local controllers ($L_1, \ldots, L_4$), each one corresponding to a different wheel. The global controller receives 4 different signals (square waves) from a fly wheel. Such signals are elaborated in a reliable way by the GC and 4 different estimates of the velocities of the 4 wheels are obtained. On the basis of them GC computes an estimate of the vehicle velocity V_v. Finally, the value of the pedal ratio F_p is obtained on the basis of the pedal position P_p and the pedal force P_f.

The generic ith local controller has three different inputs. The first one is equal to y_i and comes from the fly wheel; the other two inputs come from GC and are the same for all wheels, i.e., F_p and V_v. The local controller L_i elaborates its brake force Fb_i and its own estimate of the wheel velocity V_L^i on the basis of y_i. Note that the estimates of the wheel velocity performed by local controllers are always less reliable than the estimates performed by the global controller, and this depends on the computational capabilities of the single micro-controllers. Furthermore, each local controller computes a *minimum expected* value of the corresponding wheel velocity based on the current values of the pedal force and the vehicle velocity. In the case of the generic ith local controller the minimum expected value of the wheel velocity is denoted V_E^i.

The ABS of the ith wheel should be activated whenever the driver is braking and $V_L^i < V_E^i$, i.e., the sensor of the ith wheel detected the wheel in a locked condition.

5 Petri net model of the ABS in the presence of stuck-at faults

In this section we present a PN model representative of the overall behavior of the ABS and its interaction with the wheel in braking conditions. The proposed model also includes the behavior of a sensor whose observations are responsible of the activation/deactivation of the ABS.

We assume that such a sensor is subject to faults. In [4] we studied the behavior of the system when a stuck-at-on occurs. In this paper, we introduce also the stuck-at-off fault and we consider the behavior system when both faults can occur in the system. We say that the sensor is in a stuck-at-on condition when the sensor permanently observes a locking condition on the wheel regardless of its actual condition. On the contrary, we say that the sensor is in a stuck-at-off condition when the sensor permanently observes a grip condition on the wheel regardless of its actual condition. This implies that the ABS remains permanently on or permanently off, respectively, even if the wheel is not locked or is locked.

The ABS sensor system behavior can be described by the parallel composition of four different subsystems:

- Subsystem 1: the ABS activation model,
- Subsystem 2: the sensor/wheel model,
- Subsystem 3: the model of the grip loss and recovery,
- Subsystem 4: the sample time model.

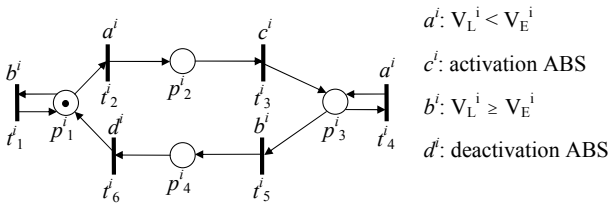

Figure 1: Subsystem 1: the ABS activation model

5.1 Subsystem 1: the ABS activation model

The ABS activation model describes the events that lead to the activation and deactivation of the ABS. In this case the braking system with ABS is changing its condition from normal braking to safety braking and viceversa. The PN system modeling the ABS activation is shown in Fig. 1. The set of events, that are all observable, includes:

- a^i : represents the condition $V_L^i < V_E^i$ (observed locked wheel);
- c^i : represents the activation of the ABS on the ith wheel;
- b^i : represents the condition $V_L^i \geq V_E^i$ (observed unlocked wheel);
- d^i : represents the deactivation of the ABS on the ith wheel.

We denote event a^i as *observed locked wheel* because when such an event is observed, we conclude that the wheel is locked and the ABS needs to be activated. On the contrary, we denote event b^i as *observed unlocked wheel* to point out that when such an event is observed, we conclude that the wheel is unlocked, thus the ABS should not be active.

The functioning of the ABS activation model for the ith wheel is depicted in Fig. 1 and can be summarized as follows. When the driver brakes two different cases may happen. First, the speed V_L^i locally detected is greater than or equal to the minimum expected value V_E^i: in such a case event b^i occurs, i.e., no lock of the wheel is detected. Alternatively, the speed measured locally V_L^i is smaller than the minimum expected value V_i^E, i.e., the locking of the wheel is detected (event a^i occurs) and the ABS should be activated (event c^i). Once the ABS is activated, either we continue to observe the wheel in a locking state (event a^i), thus the ABS remains active, or no locking is observed (event b^i) and the ABS has to be deactivated (event d^i).

5.2 Subsystem 2: the sensor/wheel model

Let us now consider an abstraction of the physical conditions of the wheel and the sensor that detects possible locking conditions of the wheel modeled by a PN system. This system is shown in Fig. 2 where a^i and b^i are the observable events introduced in the previous subsection, while the set of unobservable events includes:

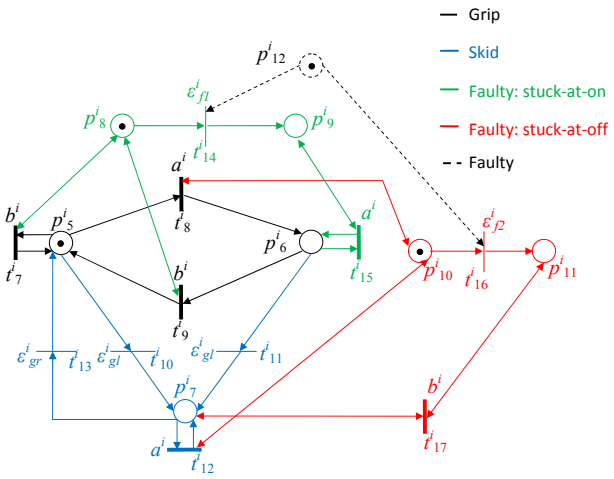

Figure 2: Subsystem 2: the sensor/wheel model

ε^i_{gl} : represents the grip loss by the ith wheel;

ε^i_{gr} : represents the grip recovery by the ith wheel;

ε^i_{f1} : models the stuck-at-on fault of the sensor pertaining to the ith wheel: the occurrence of such an event implies that the sensor permanently observes the wheel in a locking condition;

ε^i_{f2} : models the stuck-at-off fault of the sensor pertaining to the ith wheel: the occurrence of such an event implies that the sensor permanently observes the wheel in a grip condition.

Fig. 2 shows that the ith sensor/wheel can be in three different conditions: grip, skid or faulty. Let us now describe the three conditions separately.

The grip condition, depicted in Fig. 2 with the black color (non dashed line), implies that the speed detected locally is always greater than or equal to the minimum expected value, thus in such condition event b^i is generated (observed unlocked wheel). However, it may happen that event a^i (observed locked wheel) is also generated according to the following assumption.

(A1) When the system is in grip condition one inaccurate measurement may occur. This means that event a^i may be observed even if the system is in grip condition but this could happen only for one cycle. This is a realistic assumption due to the inaccuracy of the measurement system (fly wheel).

When the system is in grip condition it may happen that the wheel skids (grip loss occurs). The skid behavior is depicted in Fig. 2 with the blue color. The loss of grip is modeled by the unobservable event labeled ε^i_{gl}. After its occurrence, the only event that can be generated is a^i. The wheel may pass from skid to grip with the unobservable event ε^i_{gr} that models a recovery of grip.

Finally, due to the sensor reliability, either a stuck-at-on or a stuck-at-off fault may occur. They may occur both in grip and in skid condition. The stuck-at-on fault occurrence disables the

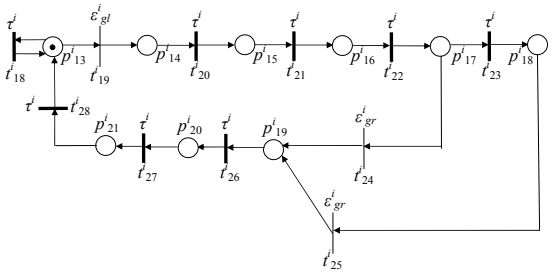

Figure 3: Subsystem 3: the model of the grip loss and recovery

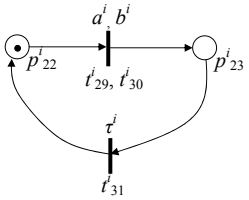

Figure 4: Subsystem 4: the sample time model

occurrence of event b^i and enables the only event a^i both in grip and in skid condition. It is modeled in Fig. 2 by green color. On the contrary, the stuck-at-off fault occurrence disables the occurrence of event a^i and enables the only event b^i both in grip and in skid condition. It is modeled in Fig. 2 by red color. Obviously if the sensor is in stuck-at-on it cannot occur a stuck-at-off fault and viceversa. This fact is modeled in Fig. 2 by place p^i_{12} and by its dashed black pre arcs.

5.3 Subsystem 3: the model of the grip loss and recovery

Let us now consider the model of the grip loss and recovery whose PN system is shown in Fig. 3. The events set is composed by: τ that is the sample time of the ABS sensor system, $\varepsilon^i_{gl}, \varepsilon^i_{gr}$ already illustrated above. The model of the sample time of the ABS sensor system is represented in Fig. 4, where a^i and b^i have already been illustrated above.

As it can be easily argued by looking at Fig. 3, this model is based on the following assumptions:

(A2) The minimum number of sample instants in which the grip can be recovered is three, while the maximum number of steps in which the grip can be recovered is four.

(A3) At least three sample instants occur between the grip recovery and a new loss of grip.

5.4 The first model: ABS system for the ith wheel with stuck-at-off fault

The ABS system for the ith wheel with stuck-at-off fault is modeled respectively by the concurrent composition [10] of the PN systems shown in Fig. 1, 2, 3 and 4 except for the green part and the

dashed black part in Fig. 2 that represent the stuck-at-on fault. The composed model has 20 places. The concurrent composition synchronizes all transitions of the four models having the same label. Moreover, we apply the synchronization also to the unobservable transitions having the same "unobservable label". This is because, although they correspond to unobservable events, when they occur, e.g. a grip loss ε_{gl}, all models have to take into account it. Thus, the whole model has:

- 6 transitions relative to label a^i;
- 4 transitions relative to label b^i;
- 1 transition relative to label c^i and label d^i;
- 8 transition relative to label τ^i;
- 2 transitions relative to label ε^i_{gl} and label label ε^i_{gr};
- 1 transition relative to label ε^i_{f2}.

For the sake of brevity the resulting PN system and its reachability graph (that contains 116 states) are not reported here.

5.5 The second model: ABS system for the ith wheel with stuck-at-on and stuck-at-off faults

The ABS system for the ith wheel is modeled by the concurrent composition of the PN systems shown in Fig. 1, 2, 3 and 4 respectively. In particular, the whole model has 23 places. As in the previous subsection the concurrent composition synchronizes all transitions of the four nets having the same label and also the unobservable transitions having the same "unobservable label". Thus, the whole model has:

- 6 transitions relative to label a^i and label b^i;
- 1 transition relative to label c^i and label d^i;
- 8 transition relative to label τ^i;
- 2 transitions relative to label ε^i_{gl} and label ε^i_{gr};
- 1 transition relative to label ε^i_{f1} and label ε^i_{f2}.

As for the previous subsection the resulting PN system and the reachability graph of the total model, that has 165 states, are not reported here for the sake of brevity.

6 Diagnosability analysis of the ABS system

In this section we analyze the diagnosability of the models presented in Subsections 5.4 and 5.5. We first show that these models are locally non diagnosable, then we prove that they are diagnosable in a centralized way and finally we discuss how they can be diagnosable in a distributed way following an algorithm that leads the communication between the ABS sensors of two different wheels.

6.1 Stuck-at-off fault

Diagnosability analysis of the whole model where only the stuck-at-off fault is considered has been performed using the approach we proposed in [1]. It is easy to see that this system is not diagnosable. In fact, when the stuck-at-off fault occurs only observable events b^i can be generated and this situation can be explained either by a non faulty behavior, i.e., the sensor is always in grip condition, or by a faulty behavior, i.e., a stuck-at-off fault has occurred. This violates the definition of diagnosability.

Because the PN model is not locally diagnosable, we look for alternative solutions.

First we need to determine if the system is diagnosable in a centralized fashion, when the information coming from two or more local diagnosers is sent to a centralized agent that has a global model of the system. If such is the case, then we try to determine if the same diagnosis that a centralized diagnoser could provide, can also be determined by the local diagnosers extended with communication capabilities. Although we do not have still a general procedure to do this, we show how in the case of the two ABS models we consider in this paper such an approach is viable.

We have considered the centralized system composed by two wheels on the same side of the vehicle under the following assumptions:

(B1) Both wheels are in the same road conditions, i.e., the events grip loss ε_{gl} and grip recovery ε_{gr} of the two wheels have to be synchronized;

(B2) Only one ABS sensor can be faulty at a time.

Both assumptions are realistic. In particular, assumption B1 is made thinking that when the front wheel encounters a certain road situation, e.g. a oil stain, also the rear wheel in the same axle encounters the same road situation. We obtain this system by the concurrent composition among the model described in Subsection 5.4 for the rear wheel, the model described in Subsection 5.4 for the front wheel and the PN in Fig. 5, that models assumption B2, where only transitions $\varepsilon_{f2}^{i,j}$ (relative to the stuck-at-off fault of the two wheels) are considered. We synchronize the events of grip loss ε_{gl} and grip recovery ε_{gr} by assumption B1.

Using a MATLAB tool that implements the approach presented in [1], we verify that the system is diagnosable in a centralized way. Since we do not want to consider the centralized system,

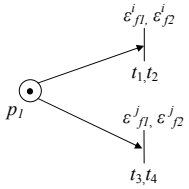

Figure 5: Petri net modeling assumption B2

due to cost requirements, we have investigated a way to make the system diagnosable in a distributed way. Namely, we want to consider the two wheels as local systems and we want to make the system globally diagnosable through communication between the two wheels. Since the centralized system, obtained synchronizing the occurrence of the grip loss and recovery events, is diagnosable, we deduced that the local systems have to exchange information on these events. In particular, we note that the necessary information to be exchanged to make the system globally diagnosable regards the grip loss event.

Here we present a communication protocol between the ABS sensors of the front wheel and the rear wheel on the same side of the vehicle. In the following, we use the superscript i when we deal with the front wheel and the superscript j when we deal with the rear wheel, while no superscript is used when we refer to a generic wheel.

The communication protocol is summarized in Algorithms 6.1 and 6.2 for the ith wheel.

Algorithm 6.1 [First part of the communication algorithm for ith wheel]

1. Let $w = \varepsilon$.
2. Let $\hat{Y}^i_{\min}(M_0, w) = \{(\varepsilon, \vec{0}^{|T_u|})\}$
3. Wait until a new label l is observed.
4. Let $w' = w$ and $w = w'l$.
5. Compute $\hat{Y}^i_{\min}(M_0, w)$.
6. For all pairs $(\sigma^i_o, y^i) \in \hat{Y}^i_{\min}(M_0, w)$, do
  6.1. compute $\min(y^i(\varepsilon^i_{gl}))$
    6.1.1. if $\min(y^i(\varepsilon^i_{gl})) > \min(y^{i'}(\varepsilon^i_{gl}))$,
      where $y^{i'} \in (\sigma^{i'}_o, y^{i'}) \in \hat{Y}^i_{\min}(M_0, w')$
        then send $\min(y^i(\varepsilon^i_{gl}))$ to the jth wheel. ■

Algorithm 6.2 [Second part of the communication algorithm for ith wheel]

1. When $\min(y^j(\varepsilon^j_{gl}))$ is received by ABS sensor j,
2. If $\min(y^j(\varepsilon^j_{gl})) > \min(y^i(\varepsilon^i_{gl}))$ and it remains
  greater for the next *ten* observations,
  then ABS sensor i is in stuck-at-off. ■

Algorithm 6.1 computes the minimum number of times that ε^i_{gl} is reconstructed and each time this number increases a message is sent to the jth wheel. In particular, the number of occurrences of ε^i_{gl} is reconstructed using the j-vectors (see [2]). For each observed word w we compute

all j-vectors $y^i \in (\sigma_o^i, y^i) \in \hat{Y}^i_{\min}(M_0, w)$, namely the firing vectors of those sequences of unobservable transitions that are strictly necessary to enable w. Among all j-vectors we select the minimum component corresponding to the unobservable transition ε^i_{gl}. Algorithm 6.2 describes what happens when the wheel i receives a message from wheel j containing an update on the number of times that the wheel j has reconstructed ε^j_{gl}. When this happens the ith wheel checks if $\min(y^j(\varepsilon^j_{gl})) > \min(y^i(\varepsilon^i_{gl}))$, i.e., if the jth wheel has reconstructed an higher number of occurrences of grip loss. If such is the case, and this situation does not change for the next ten observations, it means that the ABS sensor of the ith wheel is in stuck-at-off. Note that even if $\min(y^j(\varepsilon^j_{gl})) > \min(y^i(\varepsilon^i_{gl}))$ we wait the occurrence of ten observable events to prevent false alarms. In fact, it could happen that the ith ABS sensor is not faulty but it has not reconstructed yet the occurrence of the grip loss because the frequency of the occurrence of the observed events is lower with respect to the frequency of the observations of the jth wheel.

Clearly, for the rear wheel we apply Algorithms 6.1 and 6.2 where the superscript i and j are reversed.

6.2 Stuck-at-on and stuck-at-off fault

Consider the case of the ABS sensor where both stuck-at faults can occur. Assumptions B1 and B2 still hold. Let consider $T^1_f = \{\varepsilon^i_{f1}\}$ and $T^2_f = \{\varepsilon^i_{f2}\}$ that correspond respectively to the stuck-at-on and stuck-at-off faults. Obviously the system is not locally diagnosable being not locally diagnosable in presence of the only fault class T^2_f.

The stuck-at-on fault is diagnosable in 21 steps, i.e., 21 are the transition (both observable and unobservable) firings necessary to detect the occurrence of the fault. Note that the stuck-at-on fault is not diagnosable if the grip can be recovered in less than 3 sample instants and less than 3 sample instants are considered between a grip recovery and a grip loss (see Fig. 3). This means that the sample time has to be small enough to allow the ABS sensor system to distinguish between a grip loss and a stuck-at-on fault.

The stuck-at-off fault is not locally diagnosable but also in this case we use the communication protocol presented in Algorithms 6.1 and 6.2 that makes the system locally diagnosable with communication. Note that, in such a case step 2 of Algorithm 6.2 should be modified as follows:

• If $\min(y^j(\varepsilon^j_{gl})) > \min(y^i(\varepsilon^i_{gl}))$ and it remains greater for the next *eighteen* observations, then ABS sensor i is in stuck-at-off.

When considering both stuck-at faults the minimum number of observed events that are needed before the reconstruction of ε^i_{gl} is 10 (as in the case where only the stuck-at-off fault is considered) and the maximum number is 18 that is equal to the number of observable events needed to diagnose the stuck-at-on fault. In fact, in such a case when two consecutive a are observed one cannot conclude that a grip loss has been reconstructed because the observed behavior can be due either to a grip loss or to a stuck-at-on fault, so we may have to wait until the observation of eighteen events before the reconstruction of the grip loss. Table 1 summarizes the results we

obtained.

	Locally diagnos.	**Loc.diagn. with comm.**
Stuck-at-on	Yes	Yes
Stuck-at-off	No	Yes
Stuck-at-on & off	No	Yes

Table 1: Diagnosability results.

7 Conclusions and future work

This paper is the continuation of our previous work where we presented a PN model of an ABS whose sensor, that is responsible of the activation of the ABS, was subject to a stuck-at-on fault. Here we examine the case of stuck-at-off fault and both stuck-at faults. We discuss the whole model and prove local non-diagnosability. Finally, starting from the diagnosability of the centralized system, we present a communication protocol that makes the distributed system, composed by the rear and the front wheels on the same axle of the car, locally diagnosable with communication.

References

[1] M.P. Cabasino, A. Giua, S. Lafortune, and C. Seatzu. A New Approach for Diagnosability Analysis of Petri Nets Using Verifier Nets. *IEEE Trans. on Automatic Control*, 2012. to appear.

[2] M.P. Cabasino, A. Giua, M. Pocci, and C. Seatzu. Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems. *Control Engineering Practice*, 19(9):989–1001, 2011.

[3] M.P. Cabasino, A. Giua, and C. Seatzu. Diagnosability of bounded Petri nets. In *Proc. 48th IEEE Conf. on Decision and Control*, Shanghai, China, dec 2009.

[4] M.P. Cabasino, A. Giua, C. Seatzu, A. Solinas, and K. Zedda. Fault diagnosis of an ABS system using Petri nets. In *Proc. 7th IEEE Conf. on Automation Science and Engineering*, Trieste, Italy, aug 2011.

[5] F. Guerin, M. Barreau, J.-Y. Morel, A. Mihalache, B. Dumon, and A. Todoskoff. Reliability analysis for complex industrial real-time systems : application on an antilock brake system. In *Proc. 2nd IEEE Int. Conf. on Sys., Man and Cybernetics*, Hammamet, Tunisia, 2002.

[6] K. Jerath and F.T. Sheldon. Reliability analysis of an antilock braking system using stochastic Petri nets. In *Proceedings of the PMCCS5*, December 2001.

[7] R.K. Jurgen. *X-By-Wire Automotive Systems*. SAE International, 2009.

[8] A. Mihalache, F. Guerin, M. Barreau, and A. Todoskoff. Reliability analysis of mechatronic systems using censored data and Petri nets: application on an antilock brake system (abs). In *Reliability and Maintainability Symposium*, Newport Beach, California, 2006.

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

[10] J. L. Peterson. *Petri Net Theory and the Modeling of Systems*. Englewood Cliffs, NJ: Prentice Hall, Inc., 1981.