Fault diagnosis of an ABS system using Petri nets

M.P. Cabasino, A. Giua, C. Seatzu, A. Solinas, K. Zedda

Abstract

In this paper we consider the brake system of a vehicle whose wheels are equipped with Anti-lock Braking Systems (ABS). We assume that the sensors that are responsible of the activation of the ABS are subject to faults.

We first show how such a system can be modeled using labeled Petri nets and the notion of concurrent composition. Then, we show how fault diagnosis and diagnosability analysis can be performed on such a system using appropriate techniques based on Petri nets.

Published as:

M.P. Cabasino, A. Giua, C. Seatzu, A. Solinas, M.K. Zedda, "Fault diagnosis of an ABS system using Petri nets," *CASE11: 7th IEEE Conference on Automation Science and Engineering* (Trieste, Italy), August 2011.

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; A. Solinas and K. Zedda are with Akhela s.r.l, Cagliari. E-mail:{antonio.solinas,katiuscia.zedda} @akhela.com.

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

I. INTRODUCTION

In automotive an X-by-Wire system is a system controlled through a communication channel [1]. “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 and to make him/her safer for all roads-users. 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 [2]–[4]. In particular, in [2] Jerath *et al.* model the ABS of a vehicle system using stochastic Petri nets. This developed model includes the failure modes and effects associated with the failure rates of critical components. In [3] and [4] Mihalache *et al.* model the mechanical, electronic and embedded software sub-systems, to design, to check and to estimate the reliability of the ABS. Their model, that is a stochastic Petri net system, takes into account the faulty behavior of the different components.

In this paper we first provide a description, in terms of finite state machine, of the brake system of a wheel. Then, we focus on the ABS and its interaction with the wheel in braking condition, and propose a Petri net (PN) model of its behavior. We also keep into account the reliability of the sensor that is responsible of the activation of the ABS. Finally, we discuss how such a PN model can be used to perform fault diagnosis and diagnosability analysis using the PN based approaches we proposed in [5]–[7]. We also show that, while certain faults can be detected locally, other faults need coordinating approaches. The application of appropriate coordinating approaches, e.g. [8]–[10], is left as a future work.

II. Background on Petri nets

In this section we briefly recall the formalism used in the paper. For more details on PNs we refer to [11].

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; $Pre: P \times T \rightarrow \mathbb{N}$ and $Post: P \times T \rightarrow \mathbb{N}$ are the pre– and $post$– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix.

A *marking* is a vector $M: P \rightarrow \mathbb{N}$ 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., $L(N, M_0) = \{\sigma \in T^* \mid M_0[\sigma\rangle\}$.

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 $R(N, M_0)$.

A PN having no directed circuits is called *acyclic*. A net system $\langle N, M_0 \rangle$ is *bounded* if there exists a positive constant k such that, for $M \in R(N, M_0)$, $M(p) \leq k$.

III. Fault diagnosis and diagnosability of PNs

In this section we provide a short overview of the main definitions and results that will be useful to perform diagnosis on the considered case study.

A. Fault diagnosis

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

We denote as 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 as 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. Note that in this paper we assume that the same label $l \in L$ can be associated

to more than one transition. In particular, 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., $\mathcal{L} : T^* \rightarrow L^* \cup \{\varepsilon\}$.

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 (modeling anomalous or fault behavior), 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.

***Definition** 3.1:* [6] Let $\langle N, M_0 \rangle$ be a labeled net system with labeling function $\mathcal{L} : T \rightarrow L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be an observed word. We define

$$\mathcal{S}(w) = \{\sigma \in L(N, M_0) \mid \mathcal{L}(\sigma) = w\}$$

the set of firing sequences *consistent* with $w \in L^*$. ■

***Definition** 3.2:* [6] A *diagnoser* is a function $\Delta : L^* \times \{T_f^1, T_f^2, \ldots, T_f^r\} \rightarrow \{N, U, F\}$ that associates to each observation $w \in L^*$ and to each fault class T_f^i, $i = 1, \ldots, r$, a *diagnosis state*.

- $\Delta(w, T_f^i) = N$ if $\forall\ \sigma \in \mathcal{S}(w)$ and $\forall\ t_f \in T_f^i$ it holds $t_f \notin \sigma$.
  In such a case the ith fault cannot have occurred, because none of the firing sequences consistent with the observation contains fault transitions of class i.
- $\Delta(w, T_f^i) = U$ if:
  (i) $\exists\ \sigma \in \mathcal{S}(w)$ and $t_f \in T_f^i : t_f \in \sigma$ but
  (ii) $\exists\ \sigma' \in \mathcal{S}(w) : \forall\ t_f \in T_f^i,\ t_f \notin \sigma'$.
  In such a case the ith fault can have occurred or not, because there exists at least one firing sequence consistent with the observation that contains at least one fault transition of class i, but there also exists at least one firing sequence consistent with the observation that contains no fault transition of class i.
- $\Delta(w, T_f^i) = F$ if $\forall\ \sigma \in \mathcal{S}(w)\ \exists\ t_f \in T_f^i : t_f \in \sigma$.
  In such a case the ith fault must have occurred, because all firable sequences consistent with the observation contain at least one fault in T_f^i. ■

Note that in [6] the above definition is slightly different because the uncertain state U is split into two different states with two different degrees of alarm. However, to simplify the notation,

such a distinction is not introduced here.

Several approached in the diagnosis framework have been proposed [6], [12]–[15]. In particular, in [6] a systematic approach was given to compute the diagnosis state associated to a certain observation w and a given fault class i. Such a procedure can be applied to all nets whose unobservable subnet, i.e., the net obtained removing all observable transitions and places only connected to them, is acyclic. It is based on the notions of justification and basis marking, and presents significant advantages in terms of computational complexity [16].

B. Diagnosability

Another problem, strictly related to that of fault diagnosis, is diagnosability.

***Definition** 3.3:* [17] A PN system $\langle N, M_0\rangle$ having no deadlock after the occurrence of any transition $t_f \in T_f^i$, for $i \in \{1, \ldots, r\}$, is *diagnosable with respect to the fault class* T_f^i if there do not exist two firing sequences σ_1 and $\sigma_2 \in T^*$ satisfying the following four conditions:

- $\mathcal{L}(\sigma_1) = \mathcal{L}(\sigma_2)$, i.e., the sequences have the same observable projection;
- $\sigma_1 \in (T \setminus T_f^i)^*$, i.e., σ_1 does not contain a fault transition in the fault class 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 $\sigma_2 = \sigma_2' t_f \sigma_2''$ such that given any $k \in \mathbb{N}$ you can always pick σ_2'' such that $|\sigma_2''| > k$.

■

The problem of deriving efficient procedures for the diagnosability analysis using PNs has been addressed in [18] where we consider only bounded PNs and in [7] where is presented a method that can be applied both to bounded and unbounded PNs.

C. Distributed diagnosis

Due to the intrinsic distributed nature of real systems, such as the application considered in this paper, several distributed diagnosis techniques, that take advantage of the natural decomposition of modular systems, have been studied both in the automata [19]–[22] and in the PN setting [8]–[10], [23]–[25].

In [8] and [9] we recently proposed an approach for diagnosis of PNs with decentralized information that combines the decentralized scheme for automata presented by Debouk *et al.* in [20] with the diagnosis approach for PNs presented by Cabasino *et al.* in [5] and [6]. Moreover

in [10] we investigated the diagnosability property under decentralization. Finally, we gave a procedure to detect the presence of failure ambiguous strings based on the construction of a particular net called *Modified Verifier Net* (MVN).

IV. The brake system of a wheel

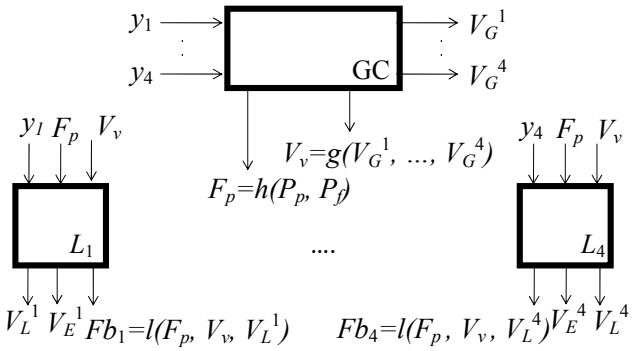
In this section we describe the functioning of a brake system of a wheel equipped with an Anti-lock Braking System (ABS).

The ABS 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, as sketched in Fig. 1. The global controller receives 4 different signals (square waves) from a fly wheel, denoted $y_1, \ldots, y_4$, respectively. Such signals are elaborated in a reliable way by the GC and 4 different estimates of the velocities of the 4 wheels are obtained, denoted $V_G^1, \ldots, V_G^4$, respectively. 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 i-th 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 i-th local controller the minimum expected value of the wheel velocity is denoted V_E^i.



GC = Global controller
L_i = i-th local controller
y_i = Signal from the i-th fly wheel
V_G^i = i-th velocity calculated by GC
F_p = pedal ratio
P_p = pedal position
P_f = pedal force
V_v = vehicle velocity
V_L^i = i-th velocity calculated by L_i
V_E^i = i-th min. exp. velocity calculated by L_i
Fb_i = i-th brake force

Fig. 1. A scheme of the global controller and the 4 local controllers of the considered Brake-by-Wire system.

The ABS of the i-th wheel should be activated whenever the driver is braking and $V_L^i < V_E^i$, that corresponds to the detection of the wheel in a locked condition by an appropriate sensor.

The finite state machine model of the brake system relative to the generic ith wheel is reported in Fig. 2. It consists of 5 states that correspond to 5 different operating conditions of the local controller: idle, normal braking, static braking, safety braking and release.

- The idle state s_0 corresponds to the condition when the brake is not active.
- Normal braking s_1 is the condition when the brake is active but the ABS is not operating.
- Static braking s_2 is the condition when the driver is braking and the vehicle velocity is under a given threshold V_{stop}.
- Safety braking s_3 is the condition when the ABS is on.
- Release state s_4 is achieved as soon as the driver stops braking. Such a condition is maintained no longer than a given time interval t_{re}.

Finally, the events corresponding to active or inactive brake are denoted b_{on} and b_{off}, respec-

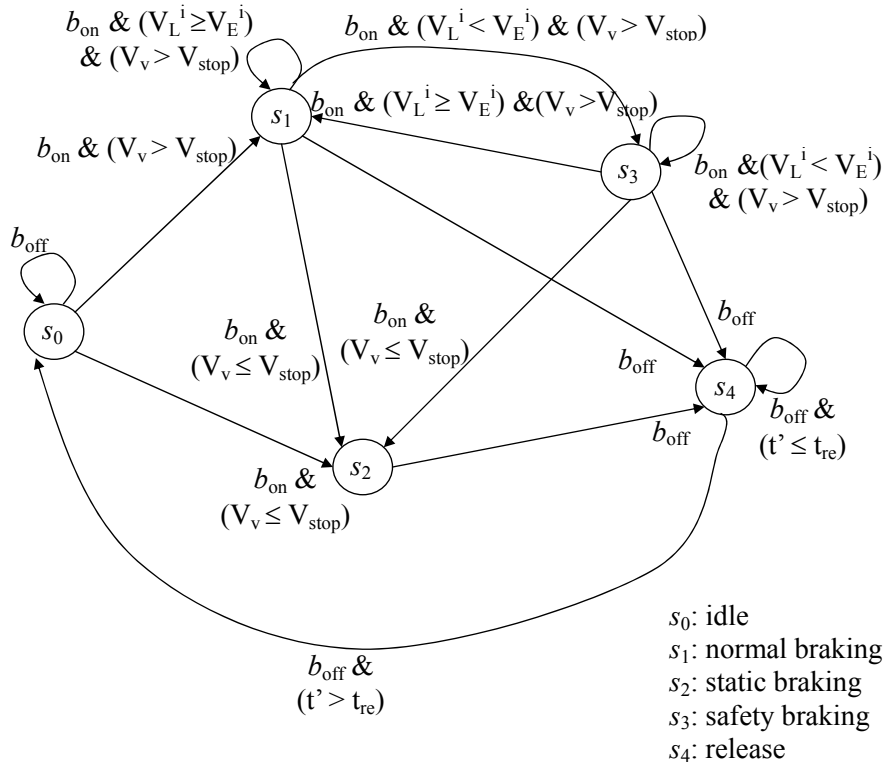


Fig. 2. The finite state machine model of the brake system relative to a generic wheel.

tively.

If the system is in the idle state s_0, it remains in such a state until the brake remains inactive (b_{off}). If the brake becomes active (event b_{on} happens), two different cases may occur, depending on the vehicle velocity V_v. If $V_v \leq V_{stop}$, then the system enters the static brake condition s_2; on the contrary, if $V_v > V_{stop}$, the system goes in the normal brake condition s_1. When the system is in s_1, three different cases may happen. First, the ABS may become active (the state s_3 is reached), and this occurs if the driver is still braking and the wheel is a locking condition, i.e., $V_L^i < V_E^i$ and $V_v > V_{stop}$. Second, if the driver is braking but the vehicle velocity is very low, the system enters in the static braking system s_2. Finally, if the driver stops braking, the system enters in the release state s_4. And so on.

V. Petri net model of the ABS in the presence of stuck-at on 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 (see states s_1 and s_3 in Fig. 2). The

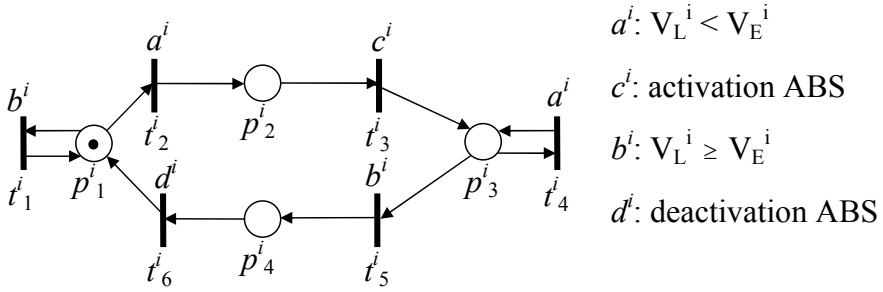


Fig. 3. Model 1: the ABS activation model

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 particular, we focus on stuck-at-on faults, i.e., the sensor permanently observes a locking condition on the wheel regardless of its actual condition. This implies that the ABS remains permanently active even if the wheel is not locked.

Such a behavior can be described by the parallel composition of three different systems:

- Model 1: the ABS activation model,
- Model 2: the sensor/wheel model,
- Model 3: the model of the grip loss and recovery.

A. Model 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. 3. 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 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 can 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. 3 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).

B. Model 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. 4 where a^i and b^i are the observable events introduced in the previous subsection, while the set of unobservable events includes:

ε_{gl}^i : represents the grip loss by the ith wheel;

ε_{gr}^i : represents the grip recovery by the ith wheel;

ε_f^i : 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.

Fig. 4 shows that the ith sensor/wheel can be in three different conditions: grip, skid or faulty. In particular, the grip condition is depicted in black, the skid condition in blue and the fault condition in red. Let us now describe the three conditions separately.

The grip condition implies that the speed detected locally is always greater than or equal to the minimum expected value, thus in such condition events 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 only one inaccurate measurement is allowed. 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).

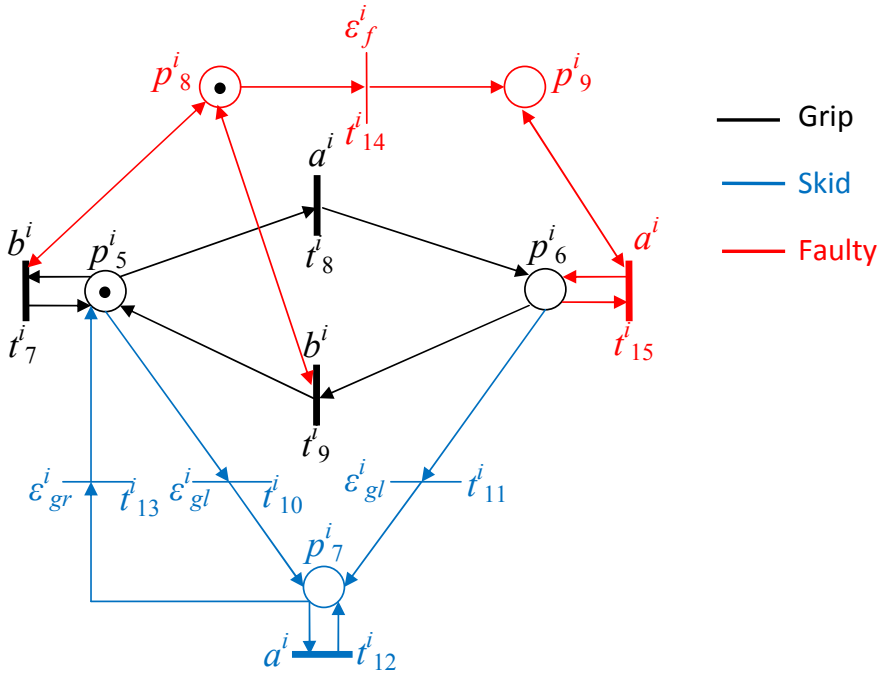


Fig. 4. Model 2: the sensor/wheel model

When the system is in grip condition it may happen that the wheel skids. 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, a stuck-at-on fault may occur. In particular, such a fault may occur both in grip and in skid condition. Since it is a stuck-at-on fault, its occurrence disables the occurrence of event b^i and enables the only event a^i both in grip and in skid condition.

C. *Model 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. 5. The events set is composed by: $a^i, b^i, \varepsilon^i_{gl}, \varepsilon^i_{gr}, \varepsilon^i_f$ already illustrated above.

As it can be easily argued by looking at Fig. 5, this model is based on the following assumptions:

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

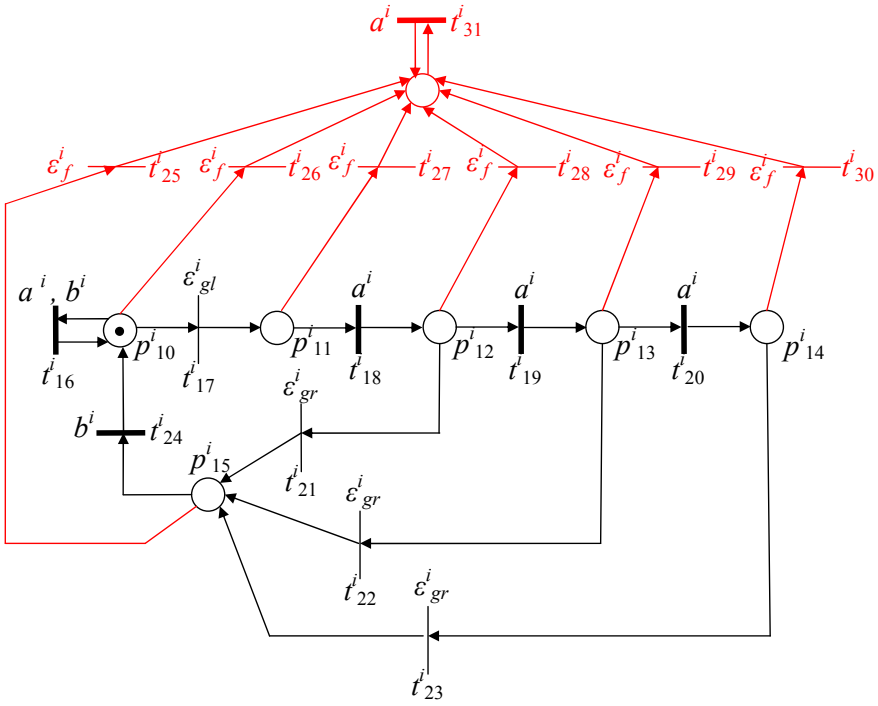


Fig. 5. Model 3: the model of the grip loss and recovery

(A3) Between the recovery of grip and a new loss of grip event b^i occurs at least once.

We want to remark that both the minimum and maximum number of steps have been chosen very small to keep the resulting PN small. However, this does not affect the generality of the model, indeed the same approach can be used when both these two parameters vary, slightly modifying the net structure in Fig. 5 with no relevant impact in the application of the fault diagnosis procedure presented in the following section. In particular, different numbers of such parameters do not change the results on the diagnosability analysis.

D. The global model: ABS system for the ith wheel

The ABS system for the ith wheel is modeled by the concurrent composition [11] of the PN systems shown in Fig. 3, 4 and 5, respectively. In particular, the global model has 16 places, equal to the sum of the number of places of the three models. The concurrent composition synchronizes all transitions of the three 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 global model has:

- 30 transitions relative to label a^i;
- 8 transitions relative to label b^i;
- 1 transitions relative to label c^i;
- 1 transitions relative to label d^i;
- 2 transitions relative to label ε^i_{gl};
- 3 transitions relative to label ε^i_{gr};
- 6 transitions relative to label ε^i_f.

For the sake of brevity the resulting PN system is not reported here. The reachability graph of the total model contains 24 states and it is not reported here as well for the sake of brevity.

VI. Diagnosis and diagnosability analysis of the ABS system

In this section we first discuss some preliminary results we obtained using the above PN model of the brake system to perform fault diagnosis and analyze diagnosability. Then, we discuss how the proposed PN model can be extended to deal with other, possibly more general, kinds of faults.

Diagnosis on the stuck-at-on fault can be carried out locally, i.e., considering the ABS system pertaining to a single wheel, using the procedure in [6].

Moreover, diagnosability analysis has been performed using the approach we proposed in [7]. Such a procedure requires the computation of a particular net, called Verifier Net (VN), and the analysis of its reachability graph. The VN has 32 places and 982 transitions and its reachability graph has 88 states. The approach allows us to determine that the stuck-at-on fault is locally diagnosable, i.e., its occurrence can be detected by only looking at the brake system of a single wheel, without interaction with the other wheels. In particular, it is diagnosable in 6 steps, i.e., after the fault occurs the maximum number of steps that occur after its detection is 6. In fact, after the fault occurs the global model will generate only event c^i or d^i at most once and event a^i an infinite number of times. However, in nominal condition the global model, according to assumption (A2), will recover the grip after at most three steps. Thus as soon as the occurrence of the fourth a^i is observed the fault is detected.

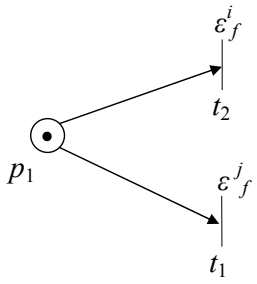


Fig. 6. Relation between the faults of a pair of wheels.

The above PN models can be easily modified to consider other kinds of faults. In particular, we already studied the diagnosability properties of the system subject to stuck-at-off fault on the sensor and proved that in such a case the fault is not locally diagnosable. Detailed results on this are omitted here for the sake of brevity. However, such a result enables us to conclude that in the presence of stuck-at-off faults we need to apply distributed diagnosis techniques to understand if a larger system, including more than one wheel, is diagnosable. To this purpose we may apply the approaches in [9] and [10], where local diagnosers communicate with a central coordinator to elaborate a global diagnosis state.

Finally, the above PN models, eventually modified, can also be used to investigate if the system is diagnosable when stuck-at-on and stuck-at-off faults are considered simultaneously.

An overview of the results we obtained and those that still represent an open issue, is summarized in Table I.

	Locally diagnosable	**Globally diagnosable**
Stuck at on	Yes	Yes
Stuck at off	No	?
Stuck at on & off	?	?

TABLE I

AN OVERVIEW OF KNOWN AND OPEN DIAGNOSABILITY RESULTS.

VII. Conclusions and future work

The main contribution of this paper is twofold. First, we present a PN model of an Anti-lock Braking Systems (ABS) whose sensor, that is responsible of the activation of the ABS, is subject to faults. Secondly, we show how fault diagnosis and diagnosability analysis can be performed on such a system using appropriate techniques based on Petri nets. It is also shown how, while in certain cases diagnosis may be performed locally, in other cases distributed diagnosis may be necessary.

Acknowledgments

We thank Corrado Esposito and Marianna Stara from Akhela s.r.l for their support in developing this model.

References

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

[2] K. Jerath and F. Sheldon, "Reliability analysis of an antilock braking system using stochastic Petri nets," in *In Proceedings of the PMCCS5*, Dec. 2001.

[3] 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 *Proceedings of the second IEEE International Conference on Systems, Man and Cybernetics (SMC'02), 2002, Hammamet, Tunisia, Volume 7*.

[4] 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, 2006*, 2006, pp. 140 –145.

[5] M. Cabasino, A. Giua, and C. Seatzu, "Fault detection for discrete event systems using Petri nets with unobservable transitions," *Automatica*, vol. 46, no. 9, pp. 1531–1539, 2010.

[6] M. Cabasino, A. Giua, M. Pocci, and C. Seatzu, "Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems," *Control Engineering Practice*, 2010, doi:10.1016/j.conengprac.2010.12.010. In press.

[7] M. Cabasino, A. Giua, S. Lafortune, and C. Seatzu, "Diagnosability analysis of unbounded Petri nets," in *Proc. 48th IEEE Conf. on Decision and Control*, Shanghai, China, dec 2009.

[8] M. Cabasino, A. Giua, A. Paoli, and C. Seatzu, "Decentralized diagnosis of Petri nets," in *2010 American Control Conference*, Baltimore, USA, June-July 2010.

[9] ——, "A new protocol for the decentralized diagnosis of labeled Petri nets," in *Proc. IFAC WODES'10: 10th Work. on Discrete Event Systems*, Berlin, Germany, August-September 2010.

[10] ——, "Decentralized diagnosability analysis of discrete event systems using Petri nets," in *Proc. 18th IFAC World Congress*, Milan, Italy, 2011.

[11] T. Murata, "Petri nets: Properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.

[12] T. Ushio, L. Onishi, and K. Okuda, "Fault detection based on Petri net models with faulty behaviors," in *Proc. SMC'98: IEEE Int. Conf. on Systems, Man, and Cybernetics (San Diego, CA, USA)*, Oct. 1998, pp. 113–118.

[13] A. Benveniste, E. Fabre, S. Haar, and C. Jard, "Diagnosis of asynchronous discrete event systems: A net unfolding approach," *IEEE Trans. on Automatic Control*, vol. 48, no. 5, pp. 714–727, 2003.

[14] M. Dotoli, M. Fanti, A. Mangini, and W. Ukovich, "On-line fault detection in discrete event systems by Petri nets and integer linear programming," *Automatica*, vol. 45, no. 11, pp. 2665–2672, 2009.

[15] F. Basile, P. Chiacchio, and G. D. Tommasi, "An efficient approach for online diagnosis of discrete event systems," *IEEE Trans. on Automatic Control*, vol. 54, no. 4, pp. 748–759, 2009.

[16] S. Lai, D. Nessi, M. Cabasino, A. Giua, and C. Seatzu, "A comparison between two diagnostic tools based on automata and Petri nets," in *Proc. IFAC WODES'08: 9th Work. on Discrete Event Systems*, May 2008, pp. 144–149.

[17] M. Cabasino, A. Giua, and C. Seatzu, "Diagnosability of bounded Petri nets," in *Proc. 48th IEEE Conf. on Decision and Control*, Dec. 2009.

[18] ——, "Diagnosability of bounded Petri nets," in *Proc. 48th IEEE Conf. on Decision and Control*, Shanghai, China, dec 2009.

[19] R. Boel and J. van Schuppen, "Decentralized failure diagnosis for discrete-event systems with costly communication between diagnosers," in *Proc. WODES'02: 6th Work. on Discrete Event Systems*, oct 2002, pp. 175–181.

[20] R. Debouk, S. Lafortune, and D. Teneketzis, "Coordinated decentralized protocols for failure diagnosis of discrete-event systems," *Discrete Events Dynamical Systems*, vol. 10, no. 1, pp. 33–86, Jan. 2000.

[21] R. Su, W. Wonham, J. Kurien, and X. Koutsoukos, "Distributed diagnosis for qualitative systems," in *in 6th International Workshop on Discrete Event Systems, Zaragoza*, 2002, pp. 169–174.

[22] Y. Wang, T.-S. Yoo, and S. Lafortune, "Diagnosis of discrete event systems using decentralized architectures," *Discrete Event Dynamic Systems*, vol. 17, no. 2, 2007.

[23] A. Benveniste, E. Fabre, S. Haar, and C. Jard, "Diagnosis of asynchronous discrete event systems, a net unfolding approach," *IEEE Trans. on Automatic Control*, vol. 48, no. 5, pp. 714–727, May 2003.

[24] S. Genc and S. Lafortune, "Distributed diagnosis of place-bordered Petri nets," *IEEE Trans. on Automation Science and Engineering*, vol. 4, no. 2, pp. 206–219, 2007.

[25] G. Jiroveanu and R. K. Boel, "A distributed approach for fault detection and diagnosis based on time Petri nets," *Mathematics and Computers in Simulation*, vol. 70, no. 5, 2006.