

# Active diagnosis for a class of switched systems\*

Jeremy Van Gorp<sup>1</sup>, Alessandro Giua<sup>2</sup>, Michael Defoort<sup>1</sup> and Mohamed Djemai<sup>1</sup>

## Abstract

This paper deals with active diagnosis for a class of switched systems which may not satisfy the classical diagnosability conditions. A Mealy Machine modeling is used to define an appropriate diagnoser which reduces the uncertain state subset. An algorithm combining the proposed diagnoser and a testing procedure is introduced to solve the fault identification problem. A study on the multicellular converter is carried out to detect and isolate faulty cells. Simulation results show the effectiveness of the proposed scheme.

Published as:

J. Van Gorp, A. Giua, M. Defoort, M. Djemai, "Active diagnosis for a class of switched systems," *52nd IEEE Conf. on Decision and Control* (Florence, Italy), Dec. 10-13, 2013.

\*This work has been supported by International Campus on Safety and Intermodality in Transportation, the European Community, the "Delegation Regionale a la Recherche et a la Technologie, the Ministere de l'Enseignement superieur et de la Recherche", the Region Nord Pas de Calais, the "Centre National de la Recherche Scientifique".

<sup>1</sup>Univ. Lille Nord de France, F-59000 Lille, France; CNRS, UMR 8201, UVHC, LAMIH, F-59313 Valenciennes, France

<sup>2</sup>Department of Electrical and Electronic Engineering, University of Cagliari, Piazza d'Armi, 09123 Cagliari, Italy and LSIS, Aix-Marseille University, France.

## I. INTRODUCTION

Occurrence of faults can be extremely detrimental, not only to the equipment and surroundings but also to the human operator if they are not detected and isolated in time. Moreover, usually, a fault tolerant controller [1] cannot be applied if the fault is not isolated, i.e., if the exact nature of the fault that has occurred is not identified. Fault detection and isolation (FDI) have been widely investigated using various methods [2], [3]. Observer-based FDI techniques rely on the estimation of outputs from measurements with the observer in order to detect the fault.

Switched systems are systems involving both continuous and discrete dynamics. They can describe a wide range of physical and engineering systems. The observability and observer design problems for switched systems have been studied using different approaches. The  $Z$ -observability concept was introduced in [4] to study the observability of some particular classes of hybrid systems. Using a similar approach, [5] provided a generalization of observability concepts. Analytical redundancy, i.e., mathematical relations between measured and estimated variables in order to detect possible faults, can be computed by the analysis of the parity space [6] for instance.

Several contributions have also been presented in the discrete event systems (DES) framework. Necessary and sufficient conditions for diagnosability, in the case of multiple failures, are developed both for automata [7] (I-diagnosability) and Petri nets [8], [9]. For DES, the diagnosability analysis and the online diagnosis are computed by a diagnoser where the available measurements are considered as inputs of the diagnoser. It leads to an estimated state which could be either “normal” or “faulty” after the occurrence of every observable event.

The classical model used in DES diagnosis are finite state machines (FSMs) and a system is seen as a spontaneous generator of events. In many physical systems, however, the evolution is driven by a control input and the diagnosability conditions depend both on the system structure and on the control strategy. Hence, some studies proposed an active diagnosis, using a supervisor [10], [11], to simultaneously ensure the control and the diagnosability of the system.

In this paper, an active diagnosis algorithm for switched systems is proposed. We assume that the only control input that drives the evolution of the system is represented by the switching function that specifies the active mode. Discrete outputs are also available as a result of each mode transition. Under these assumptions, an abstract model of the system can be represented

by a Mealy machine (MM). Some transitions of the automaton, including those corresponding to faults, may occur in the absence of a control input and may be unobservable.

In a nominal situation, the control input is selected by the controller according to a given specification and a diagnoser observes the evolution. Although the state of the diagnoser may be uncertain, (i.e., a fault may have or may have not occurred), as long as the observed evolution can be explained by the nominal model, no alarm is generated by the diagnoser. Hence such a system may be nondiagnosable in the sense of [7]. However, as soon as the diagnoser detects an abnormal behavior, i.e., an evolution that cannot be explained without the occurrence of some fault, an alarm is generated and the control objective becomes to isolate the fault if necessary. A fault isolating sequence can be determined using the well known notion of *homing sequences* defined in testing theory [12]. To the best of our knowledge, there is no work combining a diagnoser and a testing procedure for MMs. Interlinking a diagnoser and a testing algorithm online is interesting to isolate every fault for switched systems.

Multicellular converter is an interesting benchmark to show the effectiveness of the proposed strategy. Since the 1950s, power converters are used in traction systems, power supplies, or numerical amplifiers. Among these systems, multicellular converters, which appeared at the beginning of the 1990s are based on the association in series of elementary commutation cells. Due to the particular structure of this switched system, the state components are only partially observable for every fixed configuration of the switches. Hybrid observers have been proposed for this class of systems [13], [14] but they cannot be easily applied in real-time to solve the fault observation.

The paper is organized as follows. Section II deals with the problem formulation and introduces the system and diagnoser modeling. In Section III, a testing condition is defined and an algorithm combining a MM diagnoser and a testing procedure is proposed in order to solve the fault diagnosis problem. Simulation results on the multicellular converter are presented in Section IV to highlight the efficiency of the proposed approach.

## II. PROBLEM STATEMENT AND MODELING

### A. Preliminaries on DES diagnosis

The classical DES approach for diagnosis [10], considers a system modeled by a deterministic finite automaton (DFA):

$$G = (X, \Sigma, \delta, x_0) \quad (1)$$

where  $X$  is the state set,  $\Sigma$  is the set of events,  $\delta : X \times \Sigma \rightarrow X$  is the (partial) transition function and  $x_0$  is the initial state of the system.

The model  $G$  accounts for the normal and faulty behavior of the system, described by the *prefix-closed language*  $L(G)$  generated by  $G$ , i.e., a subset of  $\Sigma^*$  where  $\Sigma^*$  denotes the Kleene closure of  $\Sigma$ . The event set  $\Sigma$  is partitioned as  $\Sigma = \Sigma_o \cup \Sigma_{uo}$  where  $\Sigma_o$  represents the set of the observable events and  $\Sigma_{uo}$  the unobservable events. The *fault event set* is defined as  $\Sigma_f \subseteq \Sigma_{uo}$  and may be partitioned into  $m$  different fault classes  $\Sigma_f = \Sigma_{f_1} \cup \Sigma_{f_2} \cup \dots \cup \Sigma_{f_m}$ .

Let us define the *projection operator*  $P : \Sigma^* \rightarrow \Sigma_o^*$  such that:

$$\begin{aligned} P(\epsilon) &= \epsilon \\ P(\sigma) &= \sigma && \text{if } \sigma \in \Sigma_o \\ P(\sigma) &= \epsilon && \text{if } \sigma \in \Sigma_{uo} \\ P(s\sigma) &= P(s)P(\sigma) && \text{if } s \in \Sigma^*, \sigma \in \Sigma \end{aligned}$$

where  $\epsilon$  is the empty word. Therefore,  $P$  simply erases the unobservable events from a trace. The *inverse projection operator* with codomain in  $L(G)$  is the relation  $P^{-1} : \Sigma_o^* \rightarrow 2^{L(G)}$  that associates to each word of observable events  $w$  the set of traces that may have generated it  $P^{-1}(w) = \{s \in L(G) \mid P(s) = w\}$ . In the following, we will denote by  $s \in \Sigma^*$  a trace of events generated by the DFA and by  $w = P(s) \in \Sigma_o^*$  an observed word, i.e., the observable projection of a generated string.

The diagnosis problem for a DFA  $G$  consists in determining if, given an observed word  $w \in \Sigma_o^*$ , a fault has occurred or not, i.e., if a transition labeled with a symbol in  $\Sigma_f \subseteq \Sigma_{uo}$  has fired or not and find the class of the fault.

This may be done using a *diagnoser*, i.e., a DFA on the alphabet of observable events.

*Definition 1:* Given a DFA  $G$  with set of events  $\Sigma = \Sigma_o \cup \Sigma_{uo}$  and set of fault events  $\Sigma_f = \Sigma_{f_1} \cup \Sigma_{f_2} \cup \dots \cup \Sigma_{f_m}$ , let  $\mathcal{F} = \{F_1, F_2, \dots, F_m\}$  the labels associated to the faults. A

diagnoser for the DFA (1) is a DFA

$$\mathcal{D}(G) = (Y, \Sigma_o, \delta_y, y_0)$$

such that

- $Y \subseteq (X \times \{N\}) \cup (X \times 2^{\mathcal{F}})$ , i.e., each state of the diagnoser is a set of pairs

$$y = \{(x_1, \gamma_1), (x_2, \gamma_2), \dots, (x_k, \gamma_k)\},$$

where  $x_i \in X$  and  $\gamma_i = N$  or  $\gamma_i \subseteq \mathcal{F}$  (with  $\gamma_i \neq \emptyset$ ), for  $i = 1, 2, \dots, k$ .

- $\delta_y^*(y_0, w) = y_w$  if and only if

$$\begin{aligned} y_w = & \\ & \{(x, N) \mid (\exists s \in P^{-1}(w)) \delta^*(x_0, s) = x, s \cap \Sigma_f = \emptyset\} \\ & \cup \{(x, \gamma) \mid (\exists s \in P^{-1}(w)) \delta^*(x_0, s) = x \wedge \\ & \quad \emptyset \subsetneq \gamma \subseteq \mathcal{F} \wedge (\forall F_j \in \gamma), s \cap \Sigma_{f_j} \neq \emptyset\}, \end{aligned}$$

i.e., the execution in  $\mathcal{D}(G)$  of a word  $w$  yields a state  $y_w$  containing:

- all pairs  $(x, N)$  where  $x$  can be reached in  $G$  executing a string in  $P^{-1}(w)$  that does not contain a fault event;
- all pairs  $(x, \gamma)$  where  $x$  can be reached in  $G$  executing a string in  $P^{-1}(w)$  that contains, for each  $F_j \in \gamma$ , a fault event of class  $\Sigma_{f_j}$ .

For each state  $y = \{(x_1, \gamma_1), (x_2, \gamma_2), \dots, (x_k, \gamma_k)\}$  of  $\mathcal{D}(G)$ , a diagnosis value  $\varphi(y)$  is associated such that:

- $\varphi(y) = N$  (no fault state): if  $\gamma_i = N$  for all  $i = 1, 2, \dots, k$ ,
- $\varphi(y) = U$  (uncertain state): if there exist  $i, j \in \{1, 2, \dots, k\}$  such that  $\gamma_i = N$  and  $\gamma_j \subseteq \mathcal{F}$ ,
- $\varphi(y) = F$  (isolated fault state): if  $\gamma_i \neq N$  and  $\gamma_i = \gamma_j$  for all  $i, j = 1, 2, \dots, k$ ,
- $\varphi(y) = U_F$  (uncertain fault state): if  $\gamma_i \neq N$  for all  $i = 1, 2, \dots, k$  and there exist  $i, j = 1, 2, \dots, k$  such that  $\gamma_i \neq \gamma_j$ . ▲

Thus, a diagnoser allows one to associate to each observed word  $w$  a diagnosis state  $\varphi(w) = \varphi(y_w)$  where  $y_w = \delta_y^*(y_0, w)$  is the state reached in  $\mathcal{D}(G)$  by executing word  $w$ .

## B. Switched systems modeling

The objective of this paper is to design an algorithm which solves the fault diagnosis problem for a large class of switched systems. These systems can be modeled as MMs, where the input event corresponds to the switching input and the output event to the sensor readings.

Formally a MM is a structure:

$$M = (X, I, O, \zeta, \lambda, x_0) \quad (2)$$

where  $X$  is the state set,  $I$  and  $O$  are the set of input and output events,  $\zeta : X \times I \rightarrow X$  is the transition function,  $\lambda : X \times I \rightarrow O$  is the output function and  $x_0$  is the initial state of the system.

Here, we consider that the set of input events can be partitioned as  $I = I_c \cup I_{uc}$ . Events in  $I_c$  are *controllable* events, i.e., they denote controlled transitions that are triggered by an external control input. Events in  $I_{uc}$  are *uncontrollable* events, i.e., they denote autonomous transitions that may occur without being triggered by an external control input. The set of fault events  $I_f = I_{f,1} \cup \dots \cup I_{f,m}$  is a subset of  $I_{uc}$ . Note that the transition function of a MM is total on the set of controllable input events, i.e., for all  $x \in X$  and for all  $i \in I_c$ ,  $\zeta(x, i)$  is defined. This means that a controllable input may be applied regardless of the state of the machine. We also assume that the set of output events  $O$  may contain the special symbol  $\emptyset$  that denotes transitions whose occurrence does not generate as output a measurable event.

One can easily convert, for the purpose of diagnosis, a MM to an equivalent DFA with the same state set and alphabet  $\Sigma = I \times O$ . A transition of the MM  $\zeta(x, i) = \bar{x}$  with output function  $\lambda(x, i) = o$  can be represented in the DFA by a transition  $\delta(x, (i, o)) = \bar{x}$ . The set of unobservable events of the DFA is  $\Sigma_{uo} = I_{uc} \times \{\emptyset\}$ , and the set of fault events is  $\Sigma_f = \{I_f \times \{\emptyset\}\} \cup \{I_q \times O_q\}$ , where  $I_q \in I_c$  and  $O_q \in O$  such that  $\{I_q \times O_q\} \in \Sigma_o$ . The set, noted,  $\{I_q \times O_q\}$ , contains the observable faults based on physical considerations of the system between the input and output. An expert can associate these faults with the different fault classes. Once a MM has been converted into an equivalent DFA, a diagnoser can be designed to solve the diagnosis problem.

The objective of this paper is to design an algorithm in order to detect and isolate faults in spite of the presence of (cycles of) uncertain fault states in the diagnoser.

### III. ACTIVE DIAGNOSIS ALGORITHM

It is assumed that in normal conditions the control inputs of the MM (i.e., the switching sequence of the system) is selected by a controller to satisfy a given objective. In parallel to the controller, a diagnoser is used to detect the evolution of the system. There is no interaction between the diagnoser and the controller when no fault has been detected, i.e., while the diagnoser is in a state with label  $N$  or  $U$ . In such a condition, in fact, the diagnoser behavior may be explained by a nominal evolution and in many applications there is no need to generate an alarm. However, when a fault has been detected, the control objective is suspended for safety reasons and a fault isolation procedure is applied.

In particular, if the diagnoser is in a state  $F$ , the fault has been isolated because it is known exactly which fault has occurred. On the contrary, when the diagnoser is in one of uncertain fault states  $U_F$ , the control input sequence will be selected on the basis of a testing procedure to design an active diagnoser that isolate the fault identifying the class of the fault that has occurred.

#### A. Testing condition

In this subsection, it is described the active diagnosis procedure for the MM (2), that consists in finding a control input sequence which isolates the fault.

*Definition 2:* Given the diagnoser (1) associated with the DFA equivalent to the MM (2), we define the following function  $f : Y \times I_c^* \rightarrow 2^{Y \times O^*}$  as follows. For all  $y \in Y$  and all  $\alpha \in I_c^*$ :

$$\begin{aligned} f(y, \alpha) &= \{(y', \beta) \mid \delta_y(y, \sigma) = y', \\ &\quad \sigma = (i_1, o_1)(i_2, o_2) \dots (i_k, o_k), \\ &\quad \alpha = i_1 i_2 \dots i_k, \beta = o_1 o_2 \dots o_k\}. \end{aligned} \quad (3)$$

Function  $f$  specifies, for each state  $y$  of the diagnoser and for each control input sequence  $\alpha$ , the set of pairs  $(y', \beta)$  where  $y'$  is the state of diagnoser reached if  $\beta$  has been observed.

*Proposition 1:* The input sequence  $\alpha \in I_c^*$  isolates the faults from state  $y_u \in Y$  such that  $\varphi(y_u) = U_F$  if and only if

$$f(y_u, \alpha) = \{(y_i, \beta_i) \mid \varphi(y_i) = F\} \quad (4)$$

*Proof:* Obviously, condition (4) is a necessary condition for sequence  $\alpha$  to isolate the fault. Since the diagnoser is a deterministic automaton,  $(y', \beta), (y'', \beta) \in f(y, \alpha)$  implies  $y' = y''$ , i.e.,

the state of the diagnoser, reached by applying a given input  $\alpha$ , is known from the observed output sequence  $\beta$ . This ensures that condition (4) is also sufficient.  $\blacktriangle$

For a system which satisfies condition (4), a sequence that isolates the fault can be determined, using some standard approaches to compute homing sequences (see [12]). However, for sake of brevity a formal procedure to determine a fault isolating sequence is not discussed in this paper.

### B. Algorithm

Before introducing our proposed algorithm, let us consider the following example given in Fig. 1. There are two different fault classes, i.e.,  $\Sigma_{f_1} = f_1$  and  $\Sigma_{f_2} = f_2$ .  $X = \{1, 2, 3, 4, 5, 6\}$ ,  $I = \{a, b, \varepsilon_{f_1}, \varepsilon_{f_2}\}$  with  $I_{f,1} = \{\varepsilon_{f_1}\}$  and  $I_{f,2} = \{\varepsilon_{f_2}\}$ ,  $I_c = \{a, b\}$ ,  $O = \{o_1, o_2, o_3, o_4, o_6, \emptyset\}$  and  $x_0 = \{1\}$ . The associated diagnoser has an uncertain fault state (3f1, 5f2). The green transitions allow directly isolating the fault and the blue ones are connected to the uncertain fault state. Considering the system Fig. 1 with the initial state 1, the sequence of observable events  $(b, o_1)(a, o_2)(b, o_3)$ , for instance, allows detecting a fault but not to isolate it. On the diagnoser (Fig. 1(right)), this sequence leads to the uncertain state (3f1, 5f2) with  $\varphi(y) = U_F$ . When the fault is detected, the nominal control objective is suspended for safety reason. Considering the condition (4) on the diagnoser, the control input event  $a$  can be applied as a fault isolating sequence. Indeed, in this case, if the corresponding output event is  $o_4$ , we can isolate the fault  $f_1$  and if the output event is  $o_6$ , then the fault  $f_2$  can be isolated.

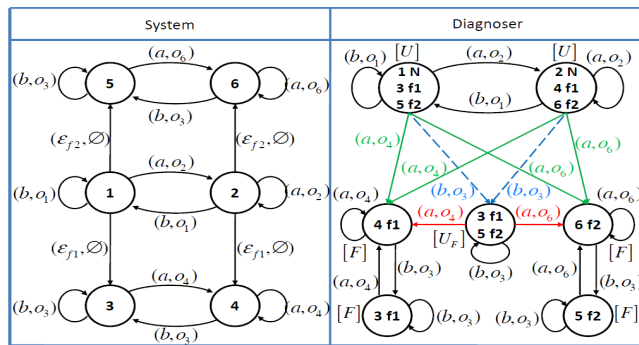


Fig. 1. Example of a system and its MM active diagnoser which satisfies condition (4).

The proposed idea is to compute a fault isolating sequence using the testing theory approaches



based on homing sequences (i.e., sequence such that the final state can be uniquely determined using the output).

This paper deals with the active diagnosis of a class of switched systems. The details on computation of a fault isolating sequence will be given in a future work. The proposed MM active diagnoser algorithm can be summarized by the Algorithm 1.

---

**Algorithm 1** Active diagnoser

---

**loop**

Nominal control (according to the control objective)

Observation of the system

**if** a fault is detected **then**

Stop the control objective

**if**  $\varphi(y) = F$  **then**

The fault is isolated using the MM diagnoser

**End**

**else**

**if** condition (4) holds **then**

Active diagnosis: Compute and apply a fault isolating sequence

The fault is isolated using the active diagnoser

**End**

**end if**

**end if**

**end if**

**end loop**

---

In a nominal situation, the control input follows a given objective and the MM diagnoser uses the output signal to observe the system. In this case, the diagnosis value  $\varphi(y)$  (associated to the diagnoser) can be equal to  $N$  or  $U$ . If a fault is detected, the control objective is suspended. If the diagnosis value  $\varphi(y) = F$ , the fault class is isolated and the algorithm is ended. If the fault is only detected (i.e.,  $\varphi(y) = U_F$ ) and if there exists an input sequence which isolates the fault (i.e., condition (4) holds), then a fault isolating sequence can be computed and applied in order

to achieve the diagnosis objective.

#### IV. APPLICATION TO THE MULTICELLULAR CONVERTER

In this section, the proposed diagnosis algorithm is applied on a multicellular converter.

##### A. Multicellular converter modeling

The multicellular converter is based on the combination of  $p$  elementary cells of commutation. The current flows from the source  $E$  toward the output through the different switches. The converter shows, by its structure, a hybrid behavior due to the discrete variables, i.e., switches. Note that because of the presence of the floating capacitors, there are also continuous variables, i.e., currents and voltages.

Without loss of generality, in this paper, we only consider the case  $p = 2$  in order to simplify notations. Anyway, the proposed approach can be easily applied for any  $p$ . Figure 2 depicts the topology of the 2-cells converter associated to an inductive load.

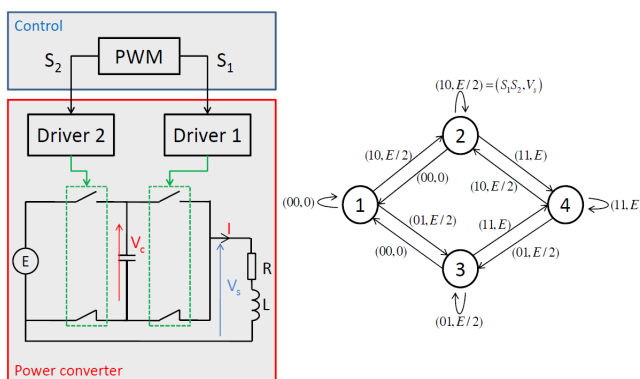


Fig. 2. Topology of a 2-cells converter with a PWM based control and the corresponding MM.

Each commutation cell is controlled by the binary signal  $S_1, S_2 \in \{0, 1\}$ . Signal  $S_j = 1$  means that the upper switch of the  $j$ -th cell is "on" and the lower switch is "off" whereas  $S_j = 0$  means that the upper switch is "off" and the lower switch is "on". A driver applies the control strategy on the two switches in each cell.  $[S_1, S_2]^T$  is a boolean vector describing the configuration or mode of the system. The discrete control laws  $S_1$  and  $S_2$  ensure the simultaneous regulation of the load current and the balancing capacitor voltage such that:  $V_{c,ref} = \frac{E}{2}$ . The dynamics of the

converter, with a load consisting in a resistance  $R$  and an inductance  $L$ , can be expressed by the following differential equations:

$$\dot{V}_c = \frac{I}{c}(S_2 - S_1) \quad (5)$$

$$\dot{I} = -\frac{R}{L}I + \frac{E}{L}S_2 - \frac{V_c}{L}(S_2 - S_1) \quad (6)$$

where  $I$  is the load current,  $c$  is the capacitance,  $V_c$  is the internal voltage and  $E$  is the voltage of the main source. Here, it is assumed that only the output voltage  $V_s$  can be measured:

$$V_s = ES_2 - V_c(S_2 - S_1) \quad (7)$$

Assuming that the control law is computed using a PWM module, the switching sequence, which depends on the desired load current, is known. Since the transient period is very short, one can only consider the steady state value for each mode. Therefore, the hybrid control strategy is defined by 4 modes (states 1, 2, 3 and 4 in Fig. 2(right)). It creates a stairs behavior of the output voltage, i.e.,  $V_s \in \{0, \frac{E}{2}, E\}$ . In order to reduce the harmonic contents and the switching losses of semiconductors during the different commutations, the control limits the variation of the output voltage to  $\frac{E}{2}$ . Indeed, the control operates one cell at a time. Figure 2(right) shows the nominal mode and depicts the corresponding MM where, the control signals  $S_1S_2$  represent the input events and the discrete value, associated to  $V_s$ , is the output set.

*Remark 1:* System (5)-(7) is not observable in the classical sense. Indeed, if  $S_1 = S_2$  then the internal voltage  $V_c$  cannot be estimated.

### B. Active fault diagnosis algorithm

In this work, only faults which occur on a commutation cell are considered. It is possible that a commutation cell is blocked due to a faulty driver. For the 2-cells converter, four faults can be defined. The fault event set is  $\Sigma_f = f_1 \cup f_2 \cup \bar{f}_1 \cup \bar{f}_2$ , where  $f_j$  (resp.  $\bar{f}_j$ ) indicates that the j-cell is blocked in  $S_j = 1$  (resp.  $S_j = 0$ ). The fault states are denoted according to the corresponding nominal state. For instance, the fault state  $2\bar{f}_2$  is the equivalent state of 2 in the presence of fault  $\bar{f}_2$ .

Figure 3 shows the MM representation of the 2-cells converter. The output set is  $O = \{\emptyset, 0, 1, 2\}$  and corresponds to Table I. The output set represents the output voltage variations.

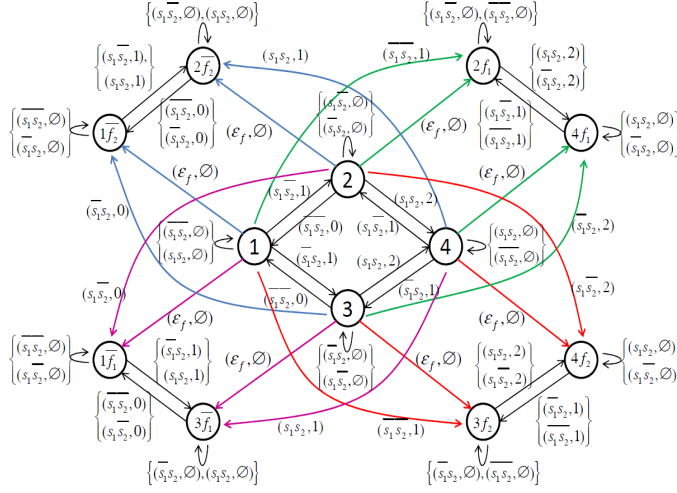


Fig. 3. MM modeling for the 2-cells converter considering  $((S_2, S_1), V_s)$  as the observable quantity (MM modeling).

The input set is  $I = \{\varepsilon_f, s_1 s_2, \bar{s}_1 \bar{s}_2, s_1 \bar{s}_2, \bar{s}_1 s_2\}$  with  $I_{uc} = \{\varepsilon_f\}$ .  $s_j$  (resp.  $\bar{s}_j$ ) indicates a control law  $S_j = 1$  (resp.  $S_j = 0$ ). Each transition edge is labeled with the values of the input and output. The system has unobservable faults, noted by the pair  $(\varepsilon_f, \emptyset)$  and observable faults represented by the events associated with their fault classes in Table II. In the case of failure, two control signals lead to the same voltage level.

TABLE I  
OUTPUT VOLTAGE VARIATIONS AND THE OUTPUT SET.

| $O = \{\emptyset, 0, 1, 2\}$ | $V_s$ variation   |
|------------------------------|-------------------|
| $\emptyset$                  | no variation      |
| 0                            | $E/2$ to 0        |
| 1                            | 0 or $E$ to $E/2$ |
| 2                            | $E/2$ to $E$      |

*Remark 2:* If the fault  $\bar{f}_1$  or  $\bar{f}_2$  occurs, then  $V_s \in \{0, \frac{E}{2}\}$ . If the fault  $f_1$  or  $f_2$  occurs then  $V_s \in \{\frac{E}{2}, E\}$ .

The MM modeling allows taking into account the change in sensor readings when the same control is applied. It improves the fault detection procedure.

TABLE II  
OBSERVABLE FAULTS ASSOCIATED WITH THE FAULT CLASSES.

|               |                        |                  |                  |             |       |                        |
|---------------|------------------------|------------------|------------------|-------------|-------|------------------------|
| Input Events  | $\bar{s}_1, \bar{s}_2$ | $s_1, \bar{s}_2$ | $\bar{s}_1, s_2$ | $s_1, s_2$  |       |                        |
| Output Events | 1                      | 0                | 2                | 0           | 2     | 1                      |
| Fault Classes | $f_1, f_2$             | $\bar{f}_1$      | $f_2$            | $\bar{f}_2$ | $f_1$ | $\bar{f}_1, \bar{f}_2$ |

Figure 4 shows the diagnoser corresponding to the 2-cells converter, modeled by its equivalent DFA and assuming that the control is broken off if a fault is detected. Each state of the diagnoser is a set of pairs  $(x_i, \gamma_i)$  where  $x_i \in X$  and  $\gamma_i \in \{N, f_1, \bar{f}_1, f_2, \bar{f}_2\}$ . It should be pointed out that it has two uncertain fault states, i.e.,  $(2\bar{f}_2, 3\bar{f}_1)$  and  $(2f_1, 3f_2)$ . Indeed, if the state of the system is, for instance, 1 or 4, a fault event with an output 1, when the same input is applied (i.e.  $(s_1s_2)$  or  $(\bar{s}_1\bar{s}_2)$ ), enables to detect a fault but does not enable to isolate it. Using the proposed diagnoser, the states  $4f_1, 4f_2, 1\bar{f}_1$  and  $1\bar{f}_2$  can be directly isolated using the observations  $(\bar{s}_1s_2, 0)$ ,  $(s_1\bar{s}_2, 0)$ ,  $(\bar{s}_1s_2, 2)$  and  $(s_1\bar{s}_2, 2)$  (see Fig. 4). By a classical approach [10], from the state of the system 2 or 3, the observations  $(\bar{s}_1\bar{s}_2, \emptyset)$  and  $(s_1s_2, \emptyset)$  also lead to the fault diagnosis. Therefore, a fault can always be detected but may not directly be isolated.

This system satisfies condition (4). Therefore, a fault isolating sequence associated to the diagnoser can be computed to eliminate the uncertainty between states  $(2\bar{f}_2, 3\bar{f}_1)$  and  $(2f_1, 3f_2)$  (see Fig. 5).

*Remark 3:* The diagnoser given in Fig. 4 cannot isolate a fault if the initial state  $x_0$  is unknown. Indeed, the first observation is ambiguous. A synchronizing sequence, based on the testing theory, can be computed to synchronize the diagnoser with the system. The computation of this sequence is based on the same idea as the homing sequence. For the converter, the sequence defined by  $(s_1\bar{s}_2, s_1s_2, \bar{s}_1s_2, \bar{s}_1\bar{s}_2)$  leads to the same state, i.e., mode 1, for all initial conditions of the nominal system. If this sequence is observed, then no fault has occurred and the diagnoser is well synchronized.

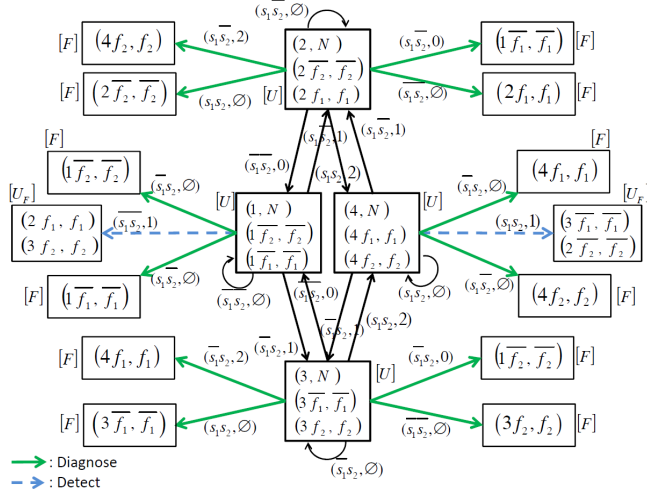


Fig. 4. Diagnoser associated to the 2-cells converter when the fault detection locks the control.

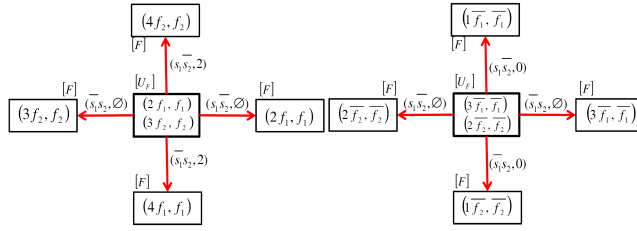


Fig. 5. Homing sequences allowing faults isolation  $((s_1\bar{s}_2)$  and  $(\bar{s}_1s_2)$ .

### C. Simulation results

In this section, some simulations are carried out to show the effectiveness of the proposed approach. Equations (5)-(7) are written using Matlab/Simulink, a PWM module controls the 2-cells converter and a Stateflow module is used to model the FSM. The parameters used in the simulation are as follow:  $E = 60V$ ,  $c = 400\mu F$ ,  $R = 200\Omega$ ,  $L = 0.1H$ . Figure 6(a) depicts the evolution of faults. In order to highlight the efficiency of the diagnoser, the simulation takes into account all kind of faults. Indeed, a reset of the system is realized between each fault and a synchronizing sequence is applied. The state is re-initialized at  $x_0 = [V_{cref}, I_{ref}]^t = [30, 0.2]^t$ . Figure 7 shows the evolution of the actual mode of the FSM.

One can see, in Fig. 6, that the diagnoser, using the MM representation, fulfils the objective, i.e., the faulty modes are well detected and isolated. In Fig. 7, one can note that faults  $\bar{f}_1$  and

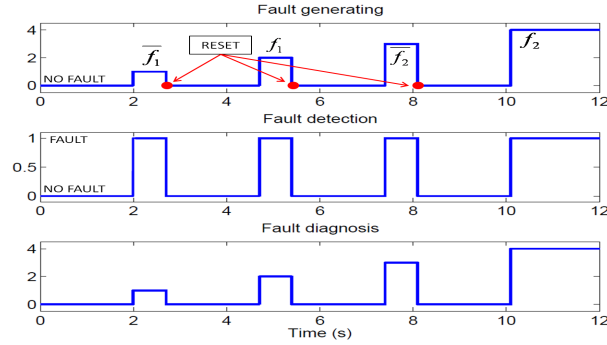


Fig. 6. Fault detection and isolation, using the proposed active diagnosis algorithm. (a) Actual mode. (b) Fault detection using the proposed diagnoser. (c) Isolation using the diagnoser and the homing sequences (Figs. 4-5).

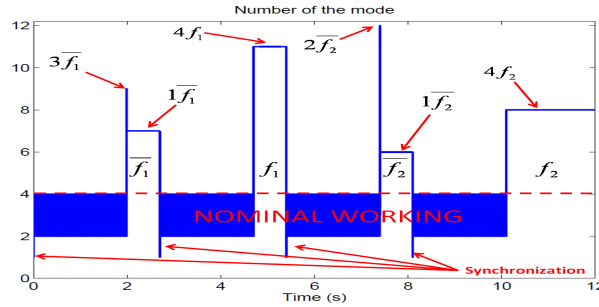


Fig. 7. Mode commutations (nominal and faulty).

$\bar{f}_2$  are identified using the proposed fault isolating sequence. Indeed, these faults generate an uncertain fault state in the diagnoser. Using the testing theory, a sequence is applied, among the fault isolating sequences given in Fig. 5, i.e.,  $(s_1\bar{s}_2)$  or  $(\bar{s}_1s_2)$ . This sequence depends on the uncertain state of the diagnoser. It enables to eliminate the uncertain states and isolate the corresponding fault.

## V. CONCLUSION

An active diagnosis for a class of switched systems which may not satisfy the classical diagnosability conditions (that applied to autonomous switched system) is designed. A Mealy Machine modeling is used to define an appropriate diagnoser which reduces the uncertain state subset. Some diagnosability conditions of faults are deduced using this representation. If the MM diagnoser satisfy these conditions, an algorithm combining the proposed diagnoser and a

testing procedure can be used in order to solve the fault diagnosis problem. A study on the cascade multicellular converter is carried out to detect and isolate faulty cells. Simulation results highlight the effectiveness of the proposed algorithm. Further works aim at implementation of the proposed active diagnosis on a 3 cells converter.

## REFERENCES

- [1] Song W. and Huang A.Q., "Fault-Tolerant Design and Control Strategy for Cascaded H-Bridge Multilevel Converter-Based STATCOM", *IEEE Trans. on Power Elect.*, **57**(8), pp. 2700-2708, 2010.
- [2] Franck P. "Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy-a survey and some new results", *Automatica*, **26**, pp. 459-474, 1990.
- [3] Isermann R. "Fault diagnosis of technical process-applications", *Springer, Heidelberg*, 2006.
- [4] Kang W., Barbot J.P. and Xu L., "On the Observability of Nonlinear and Switched Systems", *Lecture Notes in Control and Information Sciences, Springer Berlin*, 2009.
- [5] Tanwani A. and Liberzon D., "Invertibility of switched nonlinear systems", *Automatica*, **46**(12), pp. 1962–1973, 2010.
- [6] Gertler, J., "Fault detection and isolation using parity relations", *Cont. Eng. Pract.*, **5**, pp. 653-661, 1997.
- [7] Sampath M., Sengupta R., Lafortune S., Sinnamohideen K. and Teneketzis D.C., "Failure diagnosis using discrete-event models", *IEEE Trans. on Cont. Syst. Tech.*, **4**(2), pp. 105-124, 1996.
- [8] Cabasino M.P., Giua A., Lafortune S. and Seatzu C., "A New Approach for Diagnosability Analysis of Petri Nets Using Verifier Nets," *IEEE Trans. on Auto. Cont.*, **57**(12), pp. 3104-3117, 2012.
- [9] Cabasino M.P., Giua A. and Seatzu C., "Diagnosis using labeled Petri nets with silent or undistinguishable fault events", *IEEE Tran. on Systems Man & Cybernetics, Part A*, **43**(2), pp. 345–355, 2013.
- [10] Sampath M., Lafortune S., and Teneketzis D., "Active diagnosis of discrete-event systems", *IEEE Trans. on Auto. Cont.*, **43**(7), pp. 908-929, 1998.
- [11] Bayouhd M. and Travé-Massuyès L., "An Algorithm for Active Diagnosis of Hybrid Systems Casted in the DES Framework", *2nd IFAC Workshop on Dependable Control of Discrete Systems*, pp. 329-334, 2009.
- [12] Broy M., Jonsson B., Katoen J.-P., Leucker M. and Pretschner A. (Eds.), "Model-Based Testing of Reactive Systems", *Lecture Notes in Computer Science, Vol. 3472*, Springer, 2005.
- [13] Van Gorp J., Defoort M., Djemai M. and Manamanni N., "Hybrid observer for the multicellular converter", *IEEE Conf. ADHS 12*, 2012.
- [14] Defoort M., Van Gorp J., Djemai M. and Veluvolu K., "Hybrid Observer for Switched Linear Systems with Unknown Inputs", *IEEE Conf. on Ind. Elect. and App.*, 2012.