Active Diagnosis for Switched Systems Using Mealy Machine Modeling

Jérémy van Gorp, Alessandro Giua, Michael Defoort, Mohamed Djemai

Active diagnosis for switched systems using Mealy machine modeling

Jeremy Van Gorp, Alessandro Giua, Michael Defoort, Mohamed Djemaï

Abstract Generally, fault diagnosis schemes play an important role in ensuring the safety of physical or engineering systems. The study of diagnosis problem for switched systems is interesting and allows considering a more wide range of systems. This chapter deals with the active diagnosis for a class of switched systems which may not satisfy the classical diagnosability conditions usually considered in the Discrete-Event-Systems setting. In the first part, the modeling approach we propose is introduced. We propose to use an abstract representation of a switched system using a Mealy Machine where discrete faults may occur. An appropriate diagnoser is designed in order to reduce the uncertain state subset. In the second part, some diagnosability conditions are deduced. Based on the Mealy Machine, a new active diagnosis strategy is designed in order to ensure the fault detection and isolation for a class of switched systems. An algorithm combining the proposed diagnoser and a testing procedure is introduced in order to solve the fault identification problem. A study on the cascade multicellular converter is carried out to detect and isolate faulty cells. Illustrative simulation results, on a two cells converter, show the details of the algorithm and experimental results, on a three cells converter, present the effectiveness, in real time, of the proposed scheme.

Jeremy Van Gorp
Conservatoire National des Arts et Métiers (CNAM), CEDRIC - LAETITIA, 292, rue St-Martin, 75141 Paris Cedex 03, e-mail: jeremy.van_gorp@cnam.fr

Alessandro Giua
Aix Marseille Université, CNRS, ENSAM, Université de Toulon, LSIS UMR 7296, 13397, Marseille, France and DIEE, University of Cagliari, 09123 Cagliari, Italy e-mail: alessandro.giua@lsis.org, e-mail: giua@diee.unica.it

Michael Defoort
Univ. Valenciennes, CNRS, UMR 8201 - LAMIH, F-59313 Valenciennes, France e-mail: michael.defoort@univ-valenciennes.fr

Mohamed Djemaï
Univ. Valenciennes, CNRS, UMR 8201 - LAMIH, F-59313 Valenciennes, France, e-mail: mohamed.djemai@univ-valenciennes.fr

1 Introduction

Switched systems are systems involving both continuous and discrete dynamics. They can describe a wide range of physical and man-made systems (i.e., power converters, multi-tank systems, transmission systems, etc.). They have been widely studied during the last decade (see for instance [15]). Most of the attention has been focused on stability and stabilization problems [2, 14, 15, 18]. In the power electronic field, 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. The *multicellular converter* is an interesting switched system widely studied in the literature on control, observation and diagnosis. Its structure enables the reduction of the losses due to the commutations of power semiconductors while allowing low cost components. A blocked cell or a blocked switch or the internal components ageing can lead to critical situations for the system if the control law is not broken off or adapted (tolerant control).

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 [16, 23] 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 [8, 11, 12]. Observer-based FDI techniques rely on the estimation of outputs from measurements with the observer in order to detect the fault. The observability and observer design problems for hybrid systems have been studied using different approaches. The $Z-$observability concept was introduced in [13] to study the observability of some particular classes of hybrid systems. Using a similar approach in [24], it is provided a generalization of observability concepts. Analytical redundancy, i.e., mathematical relationship between measured and estimated variables in order to detect possible faults, can be computed by the analysis of the parity space [9, 29] or using a Bond Graph [17] for instance. However, due to the particular structure of the multicellular converter, the state components are only partially observable for every fixed configuration of the switches. Hybrid observers have been proposed for this system [7, 25, 26, 27] but they cannot be easily applied in real-time to solve the fault observation problem.

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 [21] (I-diagnosability) and Petri nets [4, 5]. 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” or “uncertain” after the occurrence of every observable event.

The classical model used in DES diagnosis is finite state machine (FSM) and a system is seen as a spontaneous generator of events. However, in many physical systems, the system evolution is driven by the 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, to simultaneously ensure the control and the diagnosability of the system. It is proposed, in [1], an algorithm that controls the system toward diagnosable states when a fault is detected. However, following this approach, the system may cross nondiagnosable regions in order to isolate the fault. In [6, 20], a diagnoser was used to block controllable events that drive the system into nondiagnosable regions. For the multicellular converter, the control law design, satisfying the stability conditions associated with the diagnosability, is complex. Indeed, the unobservable events, related to the system, define uncertain states in the diagnoser and the diagnosability conditions cannot be satisfied. In our approach, the algorithm of [1] is extended. The set of uncertain states, associated to the diagnoser, is partitioned in order to distinguish *uncertain states*, which may be explained by a fault but consistent with the evolution of the nominal model, from *uncertain fault* state where the occurrence of a fault has been detected and a suitable control input can be applied to identify it.

In this chapter, an active diagnosis algorithm for switched systems is proposed. The introduced algorithm in [28] is extended and an experimental validation is developed. Here, we assume that the only control input that drives the evolution of the system is represented by the switching function. This function specifies the active mode. Furthermore, discrete outputs are also available, as a result of each transition between modes, in order to detect and isolate the fault. Under these assumptions, a Mealy Machine (MM), i.e., an automaton with inputs and outputs, may be used to represent the system. Indeed, if suitably selected, an input applied to the MM may be used to steer the diagnoser out of the set of uncertain states, thus improving the detection procedure. In this context, the diagnoser, presented in [20], is re-defined in order to introduce the uncertain states and the uncertain fault states. Some transitions of the automaton, including those corresponding to faults, may occur in the absence of a control input and may be unobservable.

In the 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 [21]. However, as soon as the diagnoser detects an abnormal behavior, i.e., an evolution that cannot be explained without the occurrence of a fault, an alarm is generated and the control objective becomes to isolate the fault if necessary. A fault isolating sequence can be determined based on the well-known notion of *homing sequences* defined in testing theory [3].

The study of testing procedure for FSM has been first motivated as fundamental research in computer science [3]. In [10], a fault diagnosis algorithm based on testing was investigated. In [22] the testing theory was applied for diagnosis using Input/Output automata. They consider state faults contrary to our approach where a fault is modeled by an unobservable event on transitions and thus is more general. The problem of determining a synchronizing sequence for interpreted Petri nets, i.e., an input sequence that drives the system to a known state is considered in [19]. In this paper, an adapted algorithm to compute the fault isolating sequences for MMs,

and a generic algorithm, for the active diagnosis, are presented. If a corresponding isolating sequence can be computed for each uncertain fault state of the diagnoser, using interconnection between a diagnoser and an online testing algorithm we are able to isolate every fault for switched systems.

The chapter 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. An algorithm is presented in order to compute the fault isolating sequences. An algorithm combining a MM diagnoser and a testing procedure is also proposed in order to solve the fault diagnosis problem. Simulation results, on the 2-cells converter, and experimentation results, on the 3-cells converter, are presented in Section IV to highlight the efficiency of the proposed approach.

2 Problem statement and modeling

2.1 Preliminaries on DES diagnosis

Hereafter, some definitions from [20] and the diagnoser modeling are reformulated to account for faulty uncertain states. The classical DES approach for diagnosis [20, 21], considers a system modeled by a deterministic finite automaton (DFA):

$$G = (X, \Sigma, \delta, x_0) \tag{1}$$

where X is the state set, Σ is the set of events, $\delta : X \times \Sigma \to X$ is the (partial) transition function and x_0 is the initial state of the system. The state x_0 is assumed to be known.

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 Σ^* where Σ^* denotes the Kleene closure of Σ. The event set Σ is partitioned as $\Sigma = \Sigma_o \cup \Sigma_{uo}$ where Σ_o represents the set of the observable events and Σ_{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 $\Sigma_f = \Sigma_{f_1} \cup \Sigma_{f_2} \cup \ldots \cup \Sigma_{f_m}$.

Let us re-define ([20]) the *projection operator* $P : \Sigma^* \to \Sigma_o^*$ such that:

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

where ε 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 $P^{-1} : \Sigma_o^* \to 2^{L(G)}$ that associates to each word of observable events w the set of traces that may have generated it, i.e., $P^{-1}(w) = \{s \in L(G) \mid P(s) = w\}$. 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 trace.

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 fault event in $\Sigma_f \subseteq \Sigma_{uo}$ has been fired or not and find the fault class. 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 $\Sigma_f = \Sigma_{f_1} \cup \Sigma_{f_2} \cup \ldots \cup \Sigma_{f_m}$. Let $\mathscr{F} = \{F_1, F_2, \ldots, F_m\}$ be the set of labels associated to the fault classes. A diagnoser for the DFA defined by Eq. (1) is a DFA

$$Diag(G) = (Y, \Sigma_o, \delta_y, y_0)$$

such that

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

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

  where $x_i \in X$ and $\gamma_i = N$ or $\gamma_i \subseteq \mathscr{F}$ (with $\gamma_i \neq \emptyset$), for $i = 1, 2, \ldots, k$. Here N is interpreted as meaning Normal (no fault has occurred), while F_i as meaning that a failure of class F_i has occurred.
- The initial state y_0 of the diagnoser is defined to be $\{(x_0, N), (x_1, \gamma_1), \ldots, (x_k, \gamma_k)\}$, i.e., from a known initial state x_0, if there exist unobservable traces s_i, for $i = 1, \ldots, k$, whose projections are ε, the initial state y_0 also contains all pairs (x_i, γ_i) such that $x_i \in X$ is reachable with an unobservable trace s_i and γ_i denotes the fault classes that may have occurred in s_i or N if no fault has occurred in s_i.
- $\delta_y(y_0, w) = y_w$ if and only if

  $$\begin{aligned} &y_w = \\ &\{(x, N) \mid (\exists s \in P^{-1}(w))\ \delta(x_0, s) = x \wedge s \cap \Sigma_f = \emptyset\} \\ &\cup \{(x, \gamma_i) \mid (\exists s \in P^{-1}(w))\ \delta(x_0, s) = x\ \wedge i \in \{1, 2, \ldots, m\}, s \cap \Sigma_{f_i} \neq \emptyset \wedge \gamma_i = F_i\}, \end{aligned}$$

  i.e., the execution in $Diag(G)$ 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, γ_i) where x can be reached in G executing a string in $P^{-1}(w)$ that contains, for each $\gamma_i \subseteq \mathscr{F}$, a fault event of class Σ_{f_i}.

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

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

- $\varphi(y) = U_F$ (uncertain fault state): if $\gamma_i \neq N$ for all $i = 1,2,\ldots,k$ and there exist $i, j = 1,2,\ldots,k$ such that $\gamma_i \neq \gamma_j$.

Thus, a diagnoser allows one to associate to each observed word w a diagnosis state $\varphi(y_w)$ where $y_w = \delta_y(y_0, w)$ is the state reached in $Diag(G)$ by executing word w from the diagnoser initial state y_0.

Remark 1. Following *Definition* 1, if the diagnosis value is $\varphi(y) = U_F$, it means that the detection of the fault is ensured whereas its isolation is only possible when $\varphi(y) = F$. A fault is not diagnosable if there does no exist a corresponding state in the diagnoser with $\varphi(y) = F$.

The objective of this chapter is to design an algorithm which solves the fault diagnosis problem for a large class of switched systems.

2.2 Switched system modeling

In this chapter, the proposed approach can address the diagnosis problem of a class of switched systems which is generally represented by the following model:

$$\begin{array}{l} \dot{\mathfrak{x}}(t) \ = \mathfrak{A}_{\eta(t)}(\mathfrak{x}(t), \mathfrak{f}(t)) \\ \mathfrak{O}(t) = \mathfrak{C}_{\eta(t)}(\mathfrak{x}(t), \mathfrak{f}(t)) \end{array} \tag{2}$$

where $\mathfrak{x}(t)$ is the continuous state, $\mathfrak{O}(t)$ is the continuous output, $\mathfrak{f}(t)$ is the fault vector and $\eta(t)$ represents the switching function which is piecewise constant and $\eta(t) : [0,\infty) \rightarrow \{1,2,\ldots,\mathfrak{N}\}$. $\mathfrak{N}$ denotes the known number of discrete modes or subsystems. In general, function $\eta(t)$ could depend on an external control input and/or the state $\mathfrak{x}(t)$ and/or the fault vector $\mathfrak{f}(t)$. The measured variables are the output signal $\mathfrak{O}(t)$ and eventually the continuous state $\mathfrak{x}(t)$ if it is observable. Here, a fault can be considered on the system parameters, actuators or sensors. The multiple fault occurrences are not considered. Hereafter, we assume that all continuous variables of system (2) can be represented by sets of discrete variables.

In most of the existing studies on the diagnosis in the DES framework, the set of events is only based on one information from the system (input or output signal). The hybrid models allow representing the complex dynamics (continuous and discrete) of a system. It can appear that this class of systems needs a more accurate method for the diagnosis. In order to design a new approach of diagnosis using the formalism of DFA for the class of switched systems, it is interesting to consider the system as a MM. Using this particular modeling, the set of discrete events can be enriched with the combination of input and output signals. An event will be defined by a pair input/output. The idea is to highlight the equivalence between DFA and MM in order to deduce a MM diagnoser using the formalism of DFA previously redefined.

The switched systems can be modeled as MMs, where the input event corresponds to the active mode of the system and the output event to the sensor readings.

Formally a Mealy Machine is a structure:

$$M = (X, I, O, \zeta, \lambda, x_0) \tag{3}$$

where X is the set of discrete states, I and O are the set of input and output events, $\zeta : X \times I \to X$ is the transition function, $\lambda : X \times I \to O$ 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 $I_f = I_{f_1} \cup \ldots \cup I_{f_m}$ 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 $\Sigma_{uo} = I_{uc} \times \{\emptyset\}$, the set of fault events can be redefined as $\Sigma_f = \{I_f \times \{\emptyset\}\}$ and $\Sigma_o = \Sigma \setminus \Sigma_{uo}$. Once a MM has been converted into an equivalent DFA, a diagnoser can be designed to solve the diagnosis problem. Below, an example is given in order to highlight the equivalence between MM and DFA. The corresponding MM diagnoser is illustrated.

Example 1. Consider the MM $M = (X, I, O, \zeta, \lambda, x_0)$ with $X = \{1,2,3\}$, $I = \{a, b, \varepsilon_1, \varepsilon_f\}$, $I_c = \{a, b\}$, $I_{uc} = \{\varepsilon_1\}$, $I_f = \{\varepsilon_f\}$, $O = \{o_1, o_2, o_3, \emptyset\}$, $x_0 = \{1\}$, transition and output function:

ζ	a	b	ε_1	ε_f
1	3	2		
2	1	2	1	
3	2	3		1

λ	a	b	ε_1	ε_f
1	o_1	o_2		
2	o_3	o_2	$\emptyset$	
3	o_2	o_1		$\emptyset$

Using the first line of the left table, one can see that, in the MM M, there exist transitions from the state 1 to states 2 and 3 using input events noted b and a with $\zeta(1,a) = 3$, $\zeta(1,b) = 2$. Associated to the second table, the corresponding output event is represented with $\lambda(1,a) = o_1$, $\lambda(1,b) = o_2$. Using the proposed modeling, an equivalent DFA of this MM can be deduced. Couples (a,o_1) and (b,o_2) are two events of Σ_o in the new representation using the formalism of DFA.

The equivalent DFA is shown in Fig. 1(left) where the set of observable events is $\Sigma_o = \{(a,o_1), (a,o_2), (a,o_3), (b,o_1), (b,o_2)\}$, the set of unobservable events is $\Sigma_{uo} = \{(\varepsilon_1,\emptyset), (\varepsilon_f,\emptyset)\}$ and the set of fault events is $\Sigma_{f_1} = \{(\varepsilon_f,\emptyset)\}$ (here we have a single fault class). The diagnoser for this DFA is shown in Fig. 1(right), where each state y of $Diag(G)$ is labelled with its corresponding diagnosis value $\varphi(y)$ in square brackets.

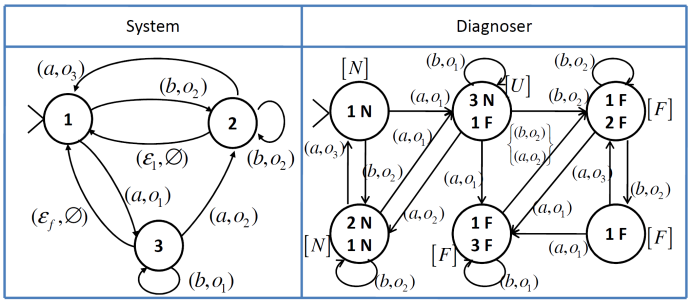


Fig. 1 On the left, a DFA G. On the right, its diagnoser automaton $Diag(G)$.

The objective of the following section is to design an algorithm in order to detect and isolate faults in spite of the presence of uncertain fault states (i.e., $\varphi(y) = U_F$) in the diagnoser.

3 Active diagnosis

It is assumed that in normal conditions the control inputs of the MM (i.e., the switching sequence of the system) are 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 diagnosis value N or U. In such a condition, in fact, the diagnoser behavior may be explained by a nominal evolution and no alarm is generated. However, when a fault has been detected (when $\varphi(y) = U_F$ or F), the control objective is suspended for safety reasons and a fault isolation procedure is applied. Here, the trade-off between the control objective and the active diagnosis is not studied.

In particular, if the diagnoser is in a state F, the fault has been isolated because it is known exactly which fault classes have occurred. On the contrary, when the diagnoser is in one of the uncertain fault states U_F, the control input sequence will be selected on the basis of a testing procedure to design an active diagnoser [20] that isolates the fault identifying the class of the fault that has occurred.

3.1 Testing condition

In this subsection, the active diagnosis procedure for the MM defined in Eq. (3) is described. It consists in finding a control input sequence which isolates the fault.

In order to design the proposed algorithm, we need to define a function which specifies, for each state $y \in Y$ of the diagnoser and for each control input sequence

$\alpha \in I_c$, the set of pairs (y', β) where $y' \in Y$ is the state of the diagnoser reached if $\beta \in O$ has been observed.

Definition 2. Given the diagnoser (*Def*. 1) associated with the DFA equivalent to the MM Eq. (3), we define the following function $f : Y \times I_c^* \to 2^{Y \times O^*}$ as follows. For all $y \in Y$ and all $\alpha \in I_c^*$:

$$\begin{aligned} f(y,\alpha) = \{(y',\beta) \mid\ & \delta_y(y,\sigma) = y', \\ & \sigma = (i_1,o_1)(i_2,o_2)\dots(i_k,o_k), \\ & \alpha = i_1 i_2 \dots i_k,\ \beta = o_1 o_2 \dots o_k\}. \end{aligned} \tag{4}$$

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

$$f(y_u,\alpha) \subseteq \{(y_i,\beta_i) \mid \varphi(y_i) = F\}. \tag{5}$$

Proof: Obviously, condition (5) is a necessary condition for sequence α 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 control input sequence α, is perfectly known from the observed output sequence β. This ensures that condition (5) is also sufficient.

From *Proposition* 1, an active diagnosability condition for the MM Eq. (3) can be deduced.

Proposition 2. A switched system modeled by a MM Eq. (3) is actively diagnosable, using the MM diagnoser (corresponding to Def. 1), if there is at least one control input sequence which verifies *Proposition* 1 for each uncertain fault state of its diagnoser.

Remark 2. The above *Proposition* 2 is slightly different from the active diagnosability definitions usually considered in the literature [1, 20]. In this study, a MM modeling is used for the system and its diagnoser in order to highlight input/output transitions and to design an adapted algorithm which solves the active diagnosis problem for the class of switched systems.

The proposed approach is inspired by the notion of homing sequence that is studied in testing theory [3]. A homing sequence is an input sequence that brings a MM (with outputs) from an unknown state to a known state, i.e., after the input sequence is applied by observing the output sequence, one can unambiguously determine the current state of the MM (see [3] for further details). Indeed, our objective consists in finding a control input sequence in the MM diagnoser which isolates the fault or disambiguates the fault class by observing the output sequence.

For a system which satisfies *Proposition* 2, a sequence that isolates the fault can be determined, using the following approach to compute all fault isolating sequences corresponding to the set of uncertain fault states.

3.2 Algorithm

Before introducing our proposed algorithm, let us consider the following example.

Example 2. Consider the MM given in Fig. 2. There are three different fault classes, i.e., $\Sigma_{f_1} = F1$, $\Sigma_{f_2} = F2$ and $\Sigma_{f_3} = F3$. $X = \{1,2,3,4,5,6,7\}$, $I = \{a,b,c,d,F_1,F_2,F_3\}$ with $I_{f1} = \{F_1\}$, $I_{f2} = \{F_2\}$ and $I_{f3} = \{F_3\}$, $I_{uc} = I_f$, $I_c = \{a,b,c,d\}$, $O = \{1,2,\emptyset\}$ and $x_0 = \{1\}$. The corresponding diagnoser contains 41 states and it is not detailed here. Our approach consists in applying an algorithm which detects and isolates the fault that has occurred. On the following figures, we have chosen to decompose the diagnoser in steps in order to explain the algorithm. Figs. 3 and 4 illustrate two parts of the diagnoser during its construction in order to achieve the fault detection and isolation. Fig. 3 presents the *MM diagnoser of detection* in the detection step. It has an unique nominal state $(1\ N, 2\ F1, 3\ F2, 5\ F3)$ since we assume that an uncertain state U in the MM diagnoser is not a faulty situation. This diagnoser shows transitions which allow the fault diagnosis or only detection. It has four uncertain fault states U_F and three isolated fault states F.

Considering the system in Fig. 2 with initial state 1, the sequence of observable events $(b,\emptyset)(d,2)$, for instance, allows detecting a fault but not to isolate it. On the diagnoser (Fig. 3), this sequence leads to the uncertain fault state $(6\ F1, 7\ F2)$ with $\varphi(y) = U_F$. When a fault is detected, the nominal control objective is suspended for safety reason.

The proposed approach is to compute a fault isolating sequence from the MM diagnoser. Fig. 4 presents the *MM active diagnoser* when a sequence $\alpha \in I_c^*$, defined by $k = 1$ event, can be observed for the isolation step. It highlights the set of reachable states from the detection step after observation of $\|\alpha\| = k = 1$ event, where $\|.\|$ is the length of a string. Our off-line objective is to analyze this part of the diagnoser in order to find a fault isolating sequence for each uncertain fault state of the *MM diagnoser of detection* (Fig. 3). The idea is to increment k while no input sequence $\alpha \in I_c^*$ with $\|\alpha\| = k$ verifying *Proposition* 1 can be found for an uncertain fault state U_F of the detection step.

Following this *MM active diagnoser* Fig. 4, all sequences of one event can be tested from each uncertain fault state. Considering condition (5) on the diagnoser, the control input event b can be applied as a fault isolating sequence for the states $(4\ F1, 7\ F3)$ (blue state) and $(6\ F1, 7\ F2)$ (green state). Indeed, observing if the corresponding output event is $\emptyset$ or 1, we can isolate the fault $F1$ or $F2$ or $F3$. The event b is not a valid isolating sequence for the uncertain fault states $(4\ F2, 6\ F3)$ (magenta state) and $(2\ F1, 3\ F2, 5\ F3)$ (red state). This sequence does not verify *Proposition* 1 because it leads to uncertain fault states $(4\ F2, 6\ F3)$ or $(2\ F2, 2\ F3)$. The input event c can be taken as a fault isolating sequence for the state $(4\ F2, 6\ F3)$. If the corresponding output event is $\emptyset$, we can isolate the fault $F3$ and if the output event is 1, then the fault $F2$ can be isolated. Following this strategy, the uncertain fault state $(2\ F1, 3\ F2, 5\ F3)$ requires $\|\alpha\| = 2$. Hereafter, the corresponding diagnoser with $k = 2$ is not presented but from Fig. 4, we can propose the fault isolating sequence bc whereas bb is not a valid isolating sequence.

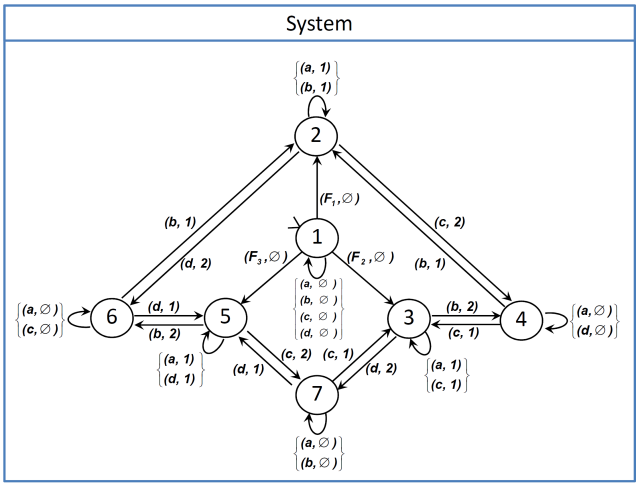


Fig. 2 Example of a MM with three fault classes.

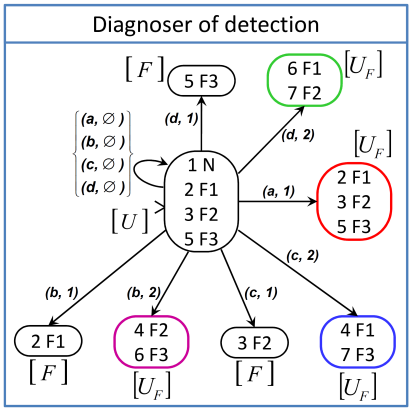


Fig. 3 MM diagnoser for the detection step.

The proposed idea is to compute a minimal fault isolating sequence for each uncertain fault states (U_F) of the MM diagnoser in the detection step using the testing theory and based on homing sequences.

Function HomingSequence can be applied off-line to compute all fault isolating sequences.

Function $HomingSequence(Diag(G))$

---

1. **Input:** The diagnoser $Diag(G) = (Y, \Sigma_o, \delta_y, y_0)$

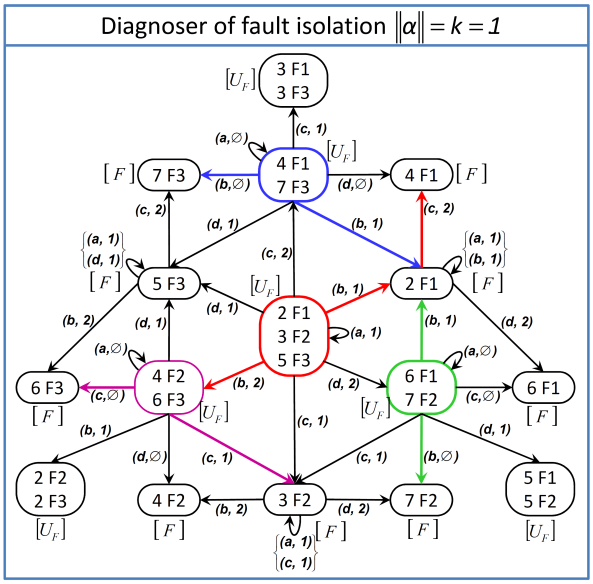


Fig. 4 MM active diagnoser for the isolation step, condition (5) is satisfied.

2. Create a set $\mathscr{I}' = \emptyset$
3. **For** all $y_{ui} \in Y$

3.1. **If** $\varphi(y_{ui}) = U_F$ and $\exists \sigma \in \Sigma_o$, $\exists y \in Y$ with $\varphi(y) = N$ or U *s.t.* $\delta_y(y,\sigma) = y_{ui}$
3.1.1. Let $\alpha_{ui} = \varepsilon$ (ε is the empty word)
3.1.2. Let k=1
3.1.3. **While** $\alpha_{ui} = \varepsilon$
- **If** $\exists \alpha \in I_c^*$ *s.t.* $\|\alpha\| = k$ and α verifies *Proposition 1* for the state y_{ui}
  $\alpha_{ui} \leftarrow \alpha$
- **Else**
  $k \leftarrow k+1$
  End if

End while
3.1.4. $\mathscr{I}' = \mathscr{I}' \cup \{(y_{ui}, \alpha_{y_{ui}})\}$
End if

End for
4. **Output:** $\mathscr{I}' = \{(y_{u1}, \alpha_{y_{u1}}), (y_{u2}, \alpha_{y_{u2}}), \ldots, (y_{ui}, \alpha_{y_{ui}}), \ldots\} \rightarrow$ all pairs combining an uncertain fault state y_{ui} with a minimal fault isolating sequence $\alpha_{y_{ui}}$.

For a system which satisfies *Proposition* 2, *Function HomingSequence* allows finding the set of minimal fault isolating sequences in order to isolate the fault as quickly as possible after its detection. Indeed, in *Function HomingSequence*, step

3.1. verifies that there exists a transition between the uncertain fault state y_{ui} and a state y such that $\varphi(y) = N$ or U. This function is designed in order to increment the size k of the sequence when no sequence can be found for an uncertain fault state y_{ui}. A set of pairs can be proposed in order to combine each uncertain fault state with a fault isolating sequence. If a fault is not diagnosable, this function could return an empty set and the variable k goes to infinity.

According to the example (Fig. 2), the *Function HomingSequence* can be applied on the MM diagnoser (Fig. 3) in order to find all minimal fault isolating sequences. The following algorithm is an application of the proposed example. The function is illustrated just for 2 uncertain fault states (steps between lines 3.1.4 and 4 correspond to others uncertain fault states of the MM diagnoser, these are not detailed in this chapter in order to simplify notations). The computed output in line 4 is for all uncertain fault states.

Function $HomingSequence(Diag(G))$ applied on the MM diagnoser (Fig. 3)

---

1. **Input:** The diagnoser $Diag(G)$ corresponding to the MM Fig. 2
2. Create a set $\mathscr{I}' = \emptyset$
3. **For** $y_{ui} = (6\ F1, 7\ F2)$ (or $y_{ui} = (4\ F1, 7\ F3)$)

   3.1. $\varphi(y_{ui}) = U_F$ and $\exists \sigma = (d,2)$ (or $\exists \sigma = (c,2)$), $\exists y = (1\ N, 2\ F1, 3\ F2, 5\ F3)$ with $\varphi(y) = U$ such that $\delta_y(y,\sigma) = y_{ui}$

   3.1.1. Let $\alpha_{ui} = \varepsilon$

   3.1.2. Let k=1

   3.1.3. **While** $\alpha_{ui} = \varepsilon$

   - $\exists \alpha = b$ such that $\|b\| = 1$ and b verifies *Proposition 1* for the state $(6\ F1, 7\ F2)$ (or $(4\ F1, 7\ F3)$)

     $\alpha_{ui} \leftarrow b$

   End while

   3.1.4. $\mathscr{I}' = \mathscr{I}' \cup \{((6\ F1, 7\ F2), b)\}$ (or $\cup\{((4\ F1, 7\ F3), b)\}$)

   ⋮

4. **Output:** $\mathscr{I}' = \{((6\ F1, 7\ F2), b), ((4\ F1, 7\ F3), b), ((4\ F2, 6\ F3), c), ((2\ F1, 3\ F2, 5\ F3), bc)\}$

The proposed MM active diagnoser algorithm can be summarized by *Algorithm* 1.

Algorithm 1 *Active Diagnoser*

---

1. Compute $\mathscr{I} = HomingSequence(Diag(G))$
2. **Loop**

   2.1. Nominal control of the system (defined according to the control objective)

   2.2. Follow the occurred events (i,o) in the MM active diagnoser

2.3. **If** a fault is detected ($\varphi(y) = U_F$ or F)
2.3.1. Stop the control objective
2.3.2. **If** $\varphi(y) = F$
- The fault is isolated using the MM diagnoser

2.3.3. **Else**
- Apply the homing sequence α_y corresponding to the pair $(y, \alpha_y) \in \mathscr{I}$
- Follow the occurred events (i, o) in the MM diagnoser in order to reach a final state $y_f \in Y$ such that $\varphi(y_f) = F$ and the fault is isolated

End if
2.3.4. **STOP**
End if

End loop

Following *Algorithm* 1, in the first step, all minimal fault isolating sequences are computed off-line using *Function Homing Sequence* for each uncertain fault state of the MM diagnoser computed for the detection step. In the second step, the nominal control can be applied and the MM diagnoser follows the occurred events (i, o) (the diagnosis value $\varphi(y)$ can be equal to N, U, U_F or F). If a fault is detected, the control objective is broken off. 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., $\varphi(y) = U_F$), then corresponding fault isolating sequence can be applied in order to achieve the diagnosis objective.

4 Application to the multicellular converter

In this section, the proposed diagnosis algorithm is applied to the multicellular converter. The details of the algorithm are presented with simulation results using a 2 cells converter (4 modes). Experimental results on a 3 cells converter (8 modes) highlight the effectiveness of the proposed approach and show that the algorithm can be generalized for this class of switched system and applied in real time.

4.1 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 illustrated Fig. 5, a hybrid behavior due to the discrete variables, i.e., switches. Note that because of the presence of $(p-1)$ floating capacitors, there are also continuous variables, i.e., currents and voltages.

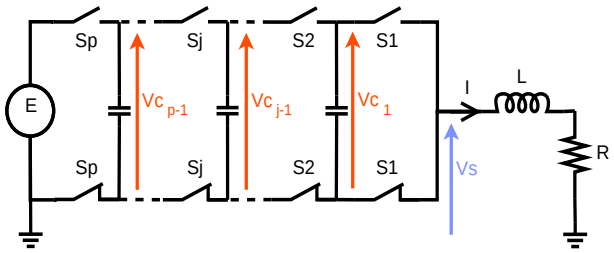


Fig. 5 Multicellular converter associated to an inductive load.

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:

$$\begin{cases} \dot{I} &= -\frac{R}{L}I + \frac{E}{L}S_p - \sum_{j=1}^{p-1} \frac{V_{c_j}}{L}(S_{j+1} - S_j) \\ \dot{V}_{c_j} &= \frac{I}{c_j}(S_{j+1} - S_j), \quad j = 1, \ldots, p-1 \end{cases} \tag{6}$$

where I is the load current, c_j is the capacitance, V_{c_j} is the voltage in the $j-$th capacitor and E is the voltage of the source. Here, it is assumed that only the output voltage V_s can be measured:

$$V_s = ES_p - \sum_{j=1}^{p-1} V_{c_j}(S_{j+1} - S_j) \tag{7}$$

Each commutation cell is controlled by the binary signal $S_j \in \{0,1\}$. 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".

Remark 3. System defined by (6) and (7) is not observable in the classical sense. Indeed, if $\forall j \in \{1, \ldots, p\}$, $S_j = 0$ or $S_j = 1$, then the internal voltages V_{c_j} cannot be estimated.

It is important to highlight that in order to standardize the industrial production, the electrical switches constraints should be similar in each cell. This requirement implies a unique voltage switch constraint of $\frac{E}{p}$. Thus, the discrete control laws, which determine the evolution of the control signals S_j, ensure the simultaneous regulation of the load current and capacitor voltages such that:

$$V_{c_j,ref} = j\frac{E}{p}, \quad \forall j \in \{1, \ldots, p\} \tag{8}$$

A driver applies the control strategy on the switches of each cell (see Fig. 6(left) for the 2-cells converter). $[S_1, \ldots, S_p]^T \in \{0,1\}^p$ is a boolean vector describing the configuration or mode of the system.

Assuming that the control law is computed using a PWM module (Fig. 6(left)), 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 2^p modes. It creates a stairs behavior of the output voltage, i.e., $V_s \in \{0, \frac{E}{p}, \frac{2E}{p}, \ldots, E\}$. 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 $\frac{E}{p}$. Indeed, the control operates one cell at once.

4.2 Active fault diagnosis for a 2-cells converter

Without loss of generality, we consider the case $p = 2$ in order to simplify notations. Anyway, the proposed approach can be easily applied for any p.

4.2.1 2-cells converter modeling

Fig. 6 depicts the topology of the 2-cells converter associated to an inductive load and its corresponding MM for the nominal modes where, the control signals S_1S_2 represent the input events and the discrete values, associated to V_s, are the output set.

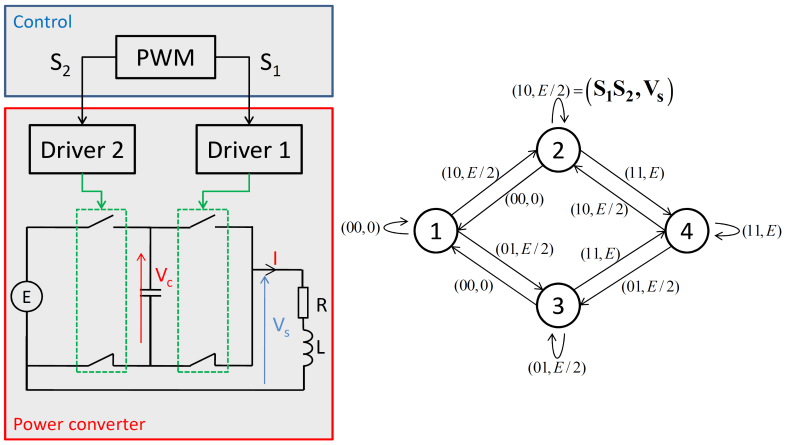


Fig. 6 Topology of a 2-cells converter with a PWM based control and the corresponding MM in its nominal behavior.

The model of the 2-cells converter involves that the reference voltage of the capacitor is such that $V_c = \frac{E}{2}$ and the output voltage is defined as $V_s \in \{0, \frac{E}{2}, E\}$ when the transient is ignored.

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 $\bar{f}_2$.

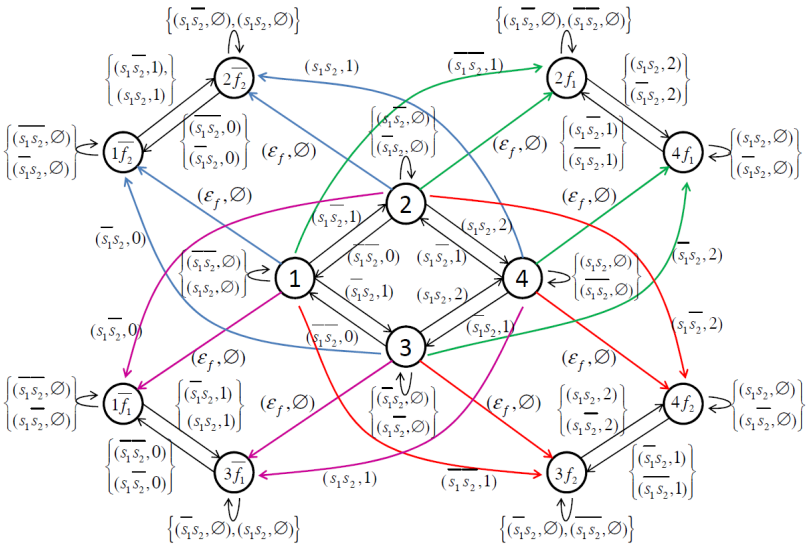


Fig. 7 MM modeling for the 2-cells converter considering $((S_2, S_1), V_s$ *variation*) as the observable quantity.

Fig. 7 shows the MM representation of the 2-cells converter. The output set is $O = \{\emptyset, 0, 1, 2\}$ and corresponds to Table 1. The output set represents the output voltage variations. The input set is $I = \{\varepsilon_f, s_1 s_2, \bar{s_1} s_2, s_1 \bar{s_2}, \bar{s_1} \bar{s_2}\}$ 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 pair $(\varepsilon_f, \emptyset)$.

Remark 4. The MM of the converter (given in Fig. 7) contains observable faults based on physical considerations of the system between the input and output (linked to the output value V_s). An expert can associate these faults with the different fault classes. Observable faults represented by the events associated with their fault classes are given in Table 2.

Table 1 Output voltage variations and the output set for the 2-cells converter.

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

Table 2 Observable faults associated with the fault classes.

Fault events	*Classes*
$(\bar{s_1}s_2, 2)$	f_1
$(s_1\bar{s_2}, 2)$	f_2
$(\bar{s_1}\bar{s_2}, 1)$	f_1, f_2
$(s_1s_2, 1)$	$\bar{f_1}, \bar{f_2}$
$(\bar{s_1}s_2, 0)$	$\bar{f_2}$
$(s_1\bar{s_2}, 0)$	$\bar{f_1}$

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

4.2.2 Algorithm associated with the 2-cells converter

Fig. 8 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, γ_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, $(2\bar{f_2}, 3\bar{f_1})$ and $(2f_1, 3f_2)$. Indeed, if the state of the system is, for instance 1 (or 4), a fault event $(\bar{s_1}\bar{s_2}, 1)$ (or $(s_1s_2, 1)$) 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 $(\bar{s_1}s_2, 0)$, $(s_1\bar{s_2}, 0)$, $(\bar{s_1}s_2, 2)$ and $(s_1\bar{s_2}, 2)$ (see Fig. 8). By a classical approach [20], 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.

Associated to the MM diagnoser, a fault isolating sequence can be computed, using $Function\ HomingSequence$, to eliminate the uncertainty between states $(2\bar{f_2}, 3\bar{f_1})$ and $(2f_1, 3f_2)$ (see Fig. 9). The input event $(\bar{s_1}s_2) \in I_c^*$ satisfying condition (5) can be a fault isolating sequence for the system (the input event $(s_1\bar{s_2}) \in I_c^*$ can be also used).

Remark 5. The diagnoser given in Fig. 8 cannot isolate a fault if the initial state x_0 is unknown. Here, it is considered that the initial conditions of the system are known and the initial mode is without fault. The initial mode corresponds to the mode without control (all $S_j = 0$) (see Fig. 5) and will be defined with mode 1.

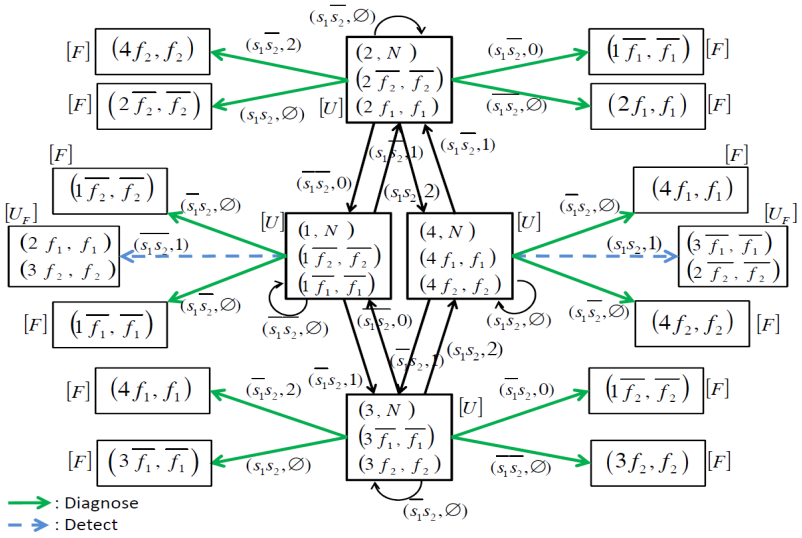


Fig. 8 Part of the diagnoser associated to the 2-cells converter, considering that the control is broken off if a fault can be detected.

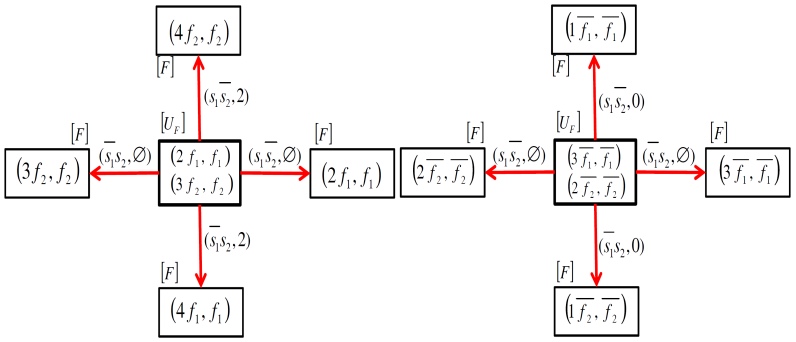


Fig. 9 Homing sequences allowing faults isolation (i.e., $(s_1\bar{s}_2)$ and $(\bar{s}_1 s_2)$ with $\|\alpha\| = 1$).

4.2.3 Simulation results

In this section, some simulations are carried out to show the effectiveness of the proposed approach. Equations (6)-(7) are written using Matlab/Simulink, a PWM module controls the 2-cells converter and a Stateflow module is used to model the DFA. The parameters used in the simulation are as follows:

$$E = 60V,\ c = 400\mu F,\ R = 200\Omega,\ L = 0.1H$$

Fig. 10(a) depicts the evolution of faults. In order to highlight the efficiency of the diagnoser, the simulation takes into account all kind of faults $\{f_1, f_2, \bar{f}_1, \bar{f}_2\}$. Fig. 10(b) highlights the fault detection and Fig. 10(c) illustrates the fault diagnosis using the proposed strategy. Indeed, a reset of the system is realized between each fault. The state is re-initialized at $x_0 = [V_{cref}, I_{ref}]^t = [30, 0.2]^t$ and the mode is 1. Fig. 11 shows the evolution of the mode of the DFA.

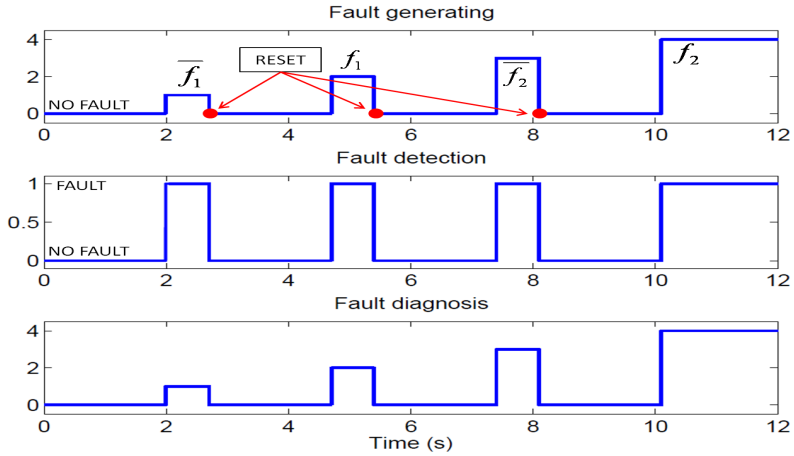


Fig. 10 Fault detection and isolation, using the proposed active diagnosis algorithm. (a) Fault evolution. (b) Fault detection using the proposed diagnoser. (c) Isolation using the diagnoser and the homing sequences given in Figs. 8-9.

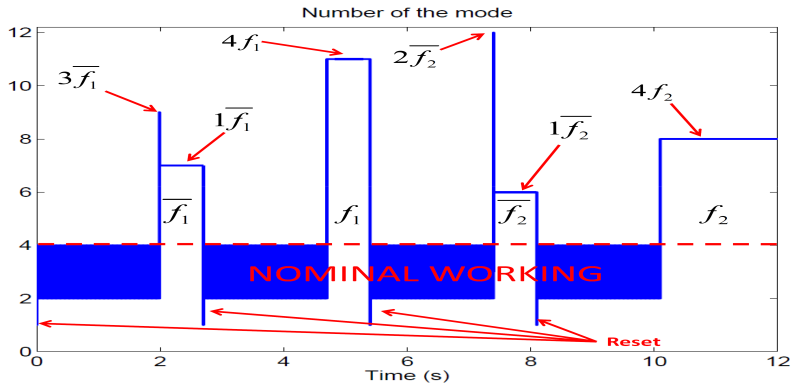


Fig. 11 Mode commutations (nominal and faulty).

One can see, in Fig. 10, that the diagnoser, using the MM representation, fulfils the objective, i.e., the faulty modes are well detected and isolated. In Fig. 11, one can note that faults $\bar{f}_1$ and $\bar{f}_2$ 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. 9, i.e., $(s_1\bar{s}_2)$ or $(\bar{s}_1 s_2)$. This sequence depends on the uncertain state of the diagnoser. It enables to eliminate the uncertain states and isolate the corresponding fault.

4.3 Active fault diagnosis for a 3-cells converter

In order to highlight the performance of the proposed active diagnosis, we have also performed some experimental validations.

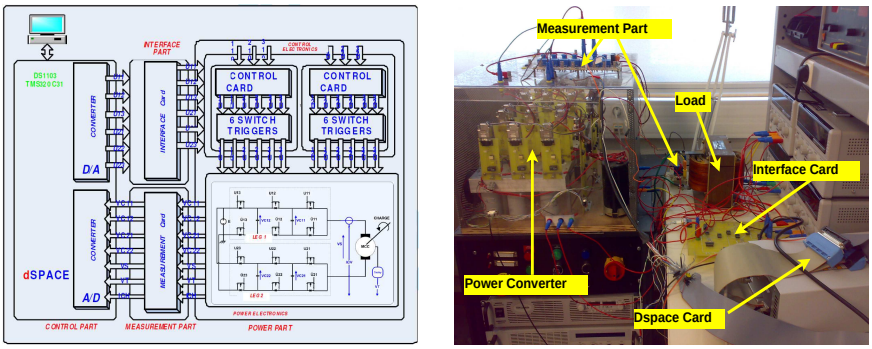
4.3.1 Experimental setup

To demonstrate the effectiveness of the proposed strategy, experimental investigations have been realized on a test bench which consists of a 3-cells converter. The schematic view of the overall platform is shown in Fig. 12(a). The experimental setup (see Fig. 12(b)) is described as follows:

- The power block is composed of a 3-cells converter with three legs. The nominal bench characteristics, obtained after identification, are: $c_1 = 40.10^{-6}F,\ c_2 = 40.10^{-6}F,\ E = 60V$.
- The measurement part is composed of voltage sensors to measure the voltage across the floating capacitors and a current transductor to measure the load current. A low pass filter has been added.
- The computer is equipped with Mathworks softwares and an interface Dspace card DSP1103, based on a floating point DSP (TMS320C31) with ControlDesk software in order to visualize the state during the experiment. In order to obtain the best resolution, the minimum sampling period for the Dspace has been chosen, i.e. $T_{ech} = 7.10^{-5}s$.
- The three control inputs, designed by the proposed scheme, are computed and delivered by the interface Dspace card. An interface card allows to protect, by insulation, the DSP of the power electronics.
- The load is composed of an inductance and a resistance: $R = 200\Omega,\ L = 1H$.

4.3.2 3-cells converter modeling

Fig. 13 depicts the MM of the 3-cells converter associated to an inductive load for the nominal modes.



a. b.

Fig. 12 Schematic view of the overall platform (a.). A photography of the experimental setup (b.).

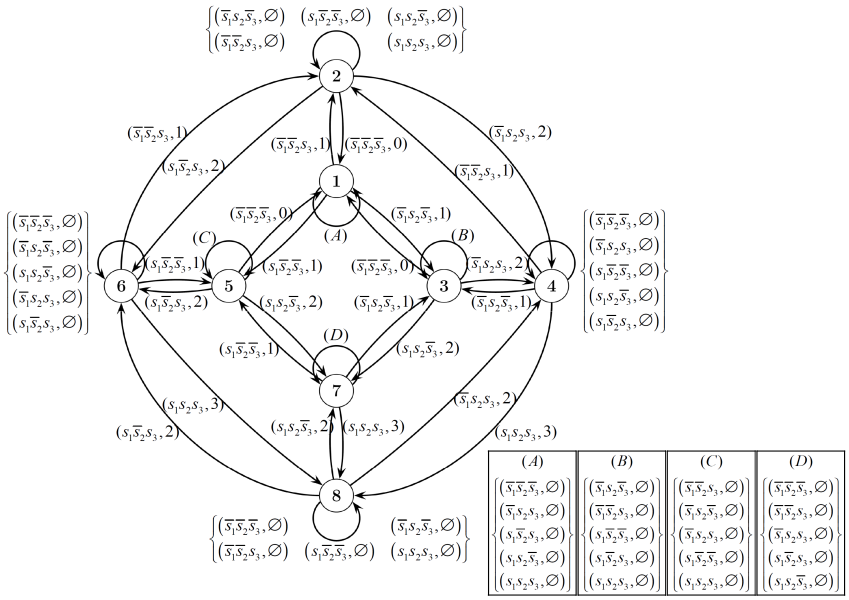


Fig. 13 Nominal MM of the 3-cells converter (without faults).

The model of the 3-cells converter involves that the reference voltages of the capacitors are such that $V_{c_1 ref} = \frac{E}{3}$ and $V_{c_2 ref} = \frac{2E}{3}$. The output voltage is defined as $V_s \in \{0, \frac{E}{3}, \frac{2E}{3}, E\}$ (considering the system in the steady state). Similarly with the model of the 2-cells converter, the fault event set may be defined with 6 fault classes $\Sigma_f = f_1 \cup f_2 \cup f_3 \cup \bar{f}_1 \cup \bar{f}_2 \cup \bar{f}_3$ (associated to each cells of the converter). The output set is $O = \{\emptyset, 0, 1, 2, 3\}$ and corresponds to Table 3. The input set is $I = \{\varepsilon_f, s_1 s_2 s_3, \bar{s_1} s_2 s_3, s_1 \bar{s_2} s_3, \bar{s_1} \bar{s_2} s_3, s_1 s_2 \bar{s_3}, \bar{s_1} s_2 \bar{s_3}, s_1 \bar{s_2} \bar{s_3}, \bar{s_1} \bar{s_2} \bar{s_3}\}$. The initial condi-

tions of the system are defined by $x_0 = [V_{c_1}, V_{c_2}, I]^T = [0,0,0]^T$ and the initial mode is 1.

Table 3 Output voltage variations and the output set for the 3-cells converter.

$O = \{\emptyset, 0, 1, 2, 3\}$	V_s *variation*
$\emptyset$	*no variation*
0	$E/3$ *to* 0
1	0 *or* $2E/3$ *to* $E/3$
2	$E/3$ *or* E *to* $2E/3$
3	$2E/3$ *to* E

Remark 6. If the fault $\bar{f}_1$ or $\bar{f}_2$ or $\bar{f}_3$ occurs, then $V_s \in \{0, \frac{E}{3}, \frac{2E}{3}\}$. If the fault f_1 or f_2 or f_3 occurs then $V_s \in \{\frac{E}{3}, \frac{2E}{3}, E\}$. When a fault occurs (when a cell is blocked), the system becomes similar to the 2-cells converter (4 modes).

Remark 7. This work considers the system in steady state. During the experimentation, there is a transient period to fulfil the control objective $x_{ref} = [V_{c_1 ref}, V_{c_2 ref}, I_{ref}]^T = [20,40,0,17]^T$. Therefore, after each reset, the system is re-initialized at x_0 and a delay, corresponding to its transient time, is considered on the active diagnosis procedure.

In this paper, the diagnoser, associated to the 3-cells converter, is not detailed in order to simplify notations. The diagnosis algorithm follows the same procedure than the 2-cells converter. Some experimental results are carried out to show that the approach can be generalized for this class of systems and applied in real time.

4.3.3 Experimental results

Fig. 14(a) depicts the evolution of faults. In order to highlight the efficiency of the approach in real time, the experimentation takes into account all kind of faults $\{f_1, f_2, f_3, \bar{f}_1, \bar{f}_2, \bar{f}_3\}$. The faults are manually generated in order to interact with the control. A reset of the system is realized between each fault (see Fig. 15(b)). Figs. 15 and 16 show respectively the evolution of the actual mode of the DFA and the state evolution of the converter. For each fault class, the diagnoser is initialized and the control ensures the state regulation. In Fig. 16, the nominal working of the converter between each generated fault is illustrated. When a fault is detected, the control is broken off and a fault isolating sequence can be applied in order to isolate it.

One can see, in Fig. 14, that the diagnoser, using the MM representation, fulfils the objective, i.e., the faulty modes are well detected and isolated. In Fig. 15, one can note that faults are identified by the same approach as the 2-cells converter and using the fault isolating sequences.

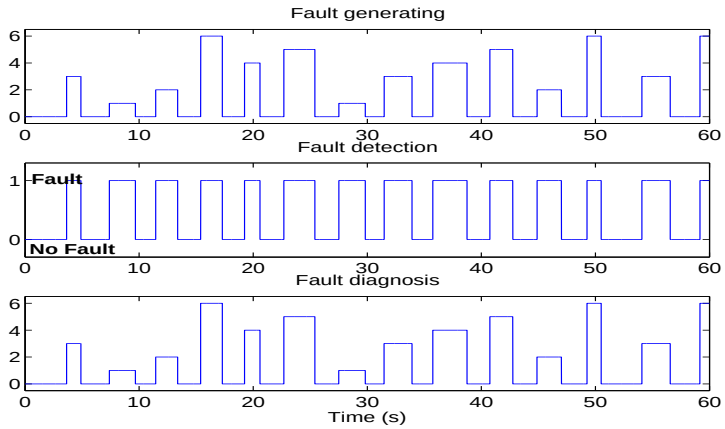


Fig. 14 Fault detection and isolation, using the proposed active diagnosis algorithm for the 3-cells converter. (a) Fault evolution. (b) Fault detection using the proposed diagnoser. (c) Isolation using the diagnoser and the homing sequences.

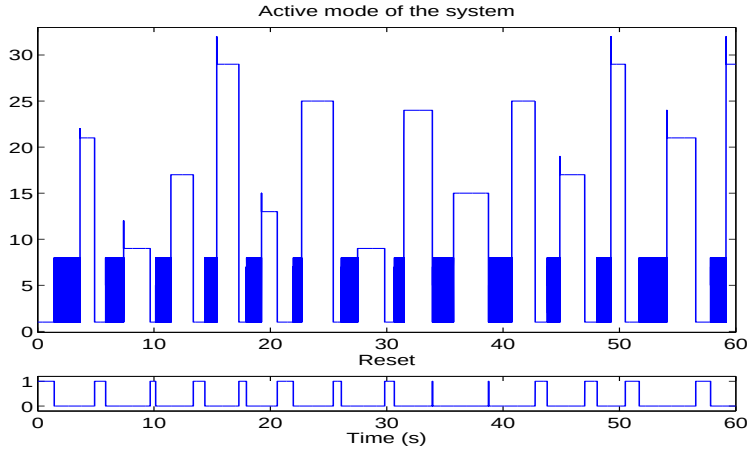


Fig. 15 Mode commutations (nominal and faulty) for the 3-cells converter.

5 Conclusion

An active diagnosis for a class of switched systems which may not satisfy the diagnosability conditions 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 satisfies 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

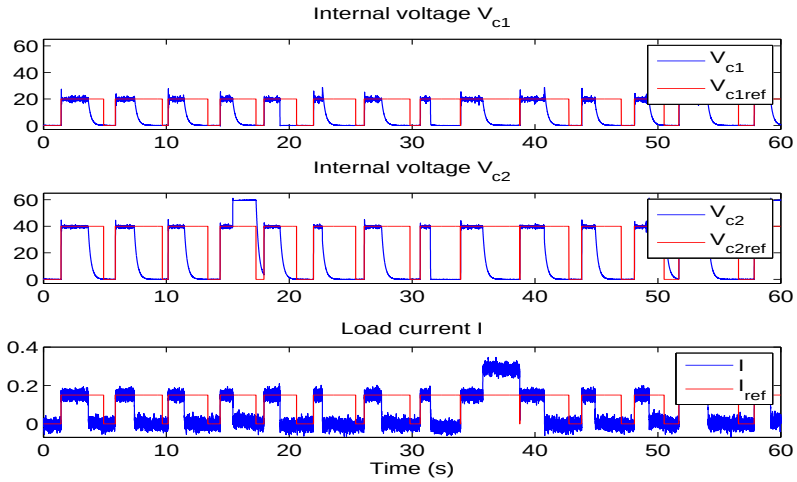


Fig. 16 Evolution of the state and the reference for the 3-cells converter.

cascade multicellular converter is carried out to detect and isolate faulty cells. Simulation results, on the 2-cells converter, are detailed and highlight the effectiveness of the proposed algorithm. Experimental results, on the 3-cells converter, show that the approach can be generalized for this class of switched system and applied in real time.

References

1. Bayoudh M. and Travé-Massuyès L. (2009), 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.
2. Branicky M. S. (1998), Multiple Lyapunov functions and other analysis tools for switched and hybrid systems, IEEE Trans. Aut. Cont., **43**(4):475–482.
3. Broy M., Jonsson B., Katoen J.-P. (2005), Leucker M. and Pretschner A. (Eds.), Model-Based Testing of Reactive Systems, Lecture Notes in Computer Science, Vol. 3472, Springer.
4. Cabasino M.P., Giua A., Lafortune S. and Seatzu C. (2012), A New Approach for Diagnosability Analysis of Petri Nets Using Verifier Nets, IEEE Trans. Aut. Cont., **57**(12):3104–3117.
5. Cabasino M.P., Giua A. and Seatzu C. (2013), Diagnosis using labeled Petri nets with silent or undistinguishable fault events, IEEE Trans. Syst. Man & Cybernetics, Part A, **43**(2):345–355.
6. Daigle M. and Biswas G. (2009), Improving diagnosability of hybrid systems through active diagnosis, Safeprocess09, pp. 217–222.
7. Defoort M., Van Gorp J., Djemaï M. and Veluvolu K. (2012), Hybrid Observer for Switched Linear Systems with Unknown Inputs, IEEE Conf. Ind. Elect. and App., pp. 594–599.
8. Franck P.M. (1990), Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy-a survey and some new results, Automatica, **26**(3):459–474.
9. Gertler, J. (1997), Fault detection and isolation using parity relations, Cont. Eng. Pract., **5**(5):653–661.

10. Guo Q., Hierons R. M., Harman M. and Derderian K. (2007), Heuristics for fault diagnosing when testing from finite state machines, The J. of Software Testing, Verification and Reliability, **17**(1):41–57.
11. Hwang I., Kim S., Kim Y. and Seah C. E. (2010), A survey of fault detection, isolation, and reconfiguration methods, IEEE Trans. Cont. Syst. Tech., **18**(3):636–653.
12. Isermann R. (2006), Fault diagnosis of technical process-applications, Springer, Heidelberg.
13. Kang W., Barbot J.P. and Xu L. (2009), On the Observability of Nonlinear and Switched Systems, Lecture Notes in Control and Information Sciences, Springer Berlin.
14. Liberzon D. (2003), Switching in Systems and Control, Systems and Control: Foundations and Applications, Birkhuser, Boston, MA.
15. Lin H. and Antsaklis P.J. (2009), Stability and stabilizability of switched linear systems: A survey of recent results, IEEE Trans. Aut. Cont., **54**(2):308–322.
16. Maharjan L., Yamagishi T., Akagi H. and Asakura J. (2010), Fault-Tolerant Operation of a Battery-Energy-Storage System Based on a Multilevel Cascade PWM Converter With Star Configuration, IEEE Trans. Power Elect., **25**(9):2386–2396.
17. Medjaher K., Andrews J. (Eds.), Bérenguer CH. (Eds.) and Jackson L. (Eds.) (2011), A bond graph model-based fault detection and isolation, Maintenance Modelling and Applications. Chapter 6 : Fault Diagnostics. Det Norske Veritas (DNV), pp. 503–512.
18. Pettersson S. and Lennartson B. (2002), Hybrid System Stability and Robustness Verification using Linear Matrix Inequalities, Int. J. Control, **75**(16/17):1335–1355.
19. Pocci M., Demongodin I., Giambiasi N. and Giua A. (2014), Testing experiments on synchronized Petri nets, IEEE Trans. Aut. Sc. and Eng., **11**(1):125–138.
20. Sampath M., Lafortune S. and Teneketzis D. (1998), Active diagnosis of discrete-event systems, IEEE Trans. Auto. Cont., **43**(7):908–929.
21. Sampath M., Sengupta R., Lafortune S., Sinnamohideen K. and Teneketzis D.C. (1996), Failure diagnosis using discrete-event models, IEEE Trans. Cont. Syst. Tech., **4**(2):105–124.
22. Schmidt M. and Lunze J. (2013), Active Diagnosis of Deterministic I/O Automata, 4th IFAC Workshop on Dependable Cont. of Dis. Syst., **4**(1), pp. 79–84.
23. Song W. and Huang A.Q. (2010), Fault-Tolerant Design and Control Strategy for Cascaded H-Bridge Multilevel Converter-Based STATCOM, IEEE Trans. Ind. Elect., **57**(8):2700–2708.
24. Tanwani A. and Liberzon D. (2010), Invertibility of switched nonlinear systems, Automatica, **46**(12):1962–1973.
25. Van Gorp J., Defoort M., Djemai M. and Manamanni N. (2012), Hybrid observer for the multicellular converter, Proceedings IFAC ADHS 12, pp. 259–264.
26. Van Gorp J., Defoort M., Djemai M. and Veluvolu K. (2015), Fault detection based on higher-order sliding mode observer for a class of switched linear systems, IET Cont. Th. Appl., **9**(15):2249–2256.
27. Van Gorp J., Defoort M., Veluvolu K. and Djemai M. (2014), Hybrid sliding mode observer for switched linear systems with unknown inputs, J. Franklin Inst., **351**(7):3987–4008.
28. Van Gorp J., Giua A., Defoort M. and Djemai M. (2013), Active diagnosis for a class of switched systems, IEEE Conf. on Decis. Cont., pp. 5003–5008.
29. Yoon S., Kim S., Bae J., Kim Y. and Kim E. (2011), Experimental evaluation of fault diagnosis in a skew-configured UAV sensor system, Cont. Eng. Pract., **19**(2):158–173.